

SnapDrive™ 3.2 for Windows®

Installation and Administration Guide

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number 215-01274_A0
July 2005

Copyright and trademark information

Copyright information

Copyright © 1994—2005 Network Appliance, 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 Network Appliance material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETWORK APPLIANCE “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NETWORK APPLIANCE 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.

Network Appliance reserves the right to change any products described herein at any time, and without notice. Network Appliance assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Network Appliance. 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 Network Appliance.

The product described in this manual may be protected by one or more U.S. 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

NetApp, the Network Appliance logo, the bolt design, NetApp—the Network Appliance Company, DataFabric, FAServer, FilerView, MultiStore, NearStore, NetCache, SecureShare, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapVault, SyncMirror, and WAFL are registered trademarks of Network Appliance, Inc. in the United States, and/or other countries. Data ONTAP, gFiler, Network Appliance, SnapCopy, Snapshot, and The Evolution of Storage are trademarks of Network Appliance, Inc. in the United States and/or other countries and registered trademarks in some other countries. ApplianceWatch, BareMetal, Camera-to-Viewer, ComplianceClock, ComplianceJournal, ContentDirector, ContentFabric, EdgeFiler, FlexClone, FlexVol, FPolicy, HyperSAN, InfoFabric, LockVault, Manage ONTAP, NOW, NetApp on the Web, ONTAPI, RAID-DP, RoboCache, RoboFiler, SecureAdmin, Serving Data by Design, SharedStorage, Simulate ONTAP, Smart SAN, SnapCache, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapMigrator, SnapSuite, SnapValidator, SohoFiler, vFiler, VFM, Virtual File Manager, VPolicy, and Web Filer are trademarks of Network Appliance, Inc. in the United States and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of Network Appliance, Inc. in the United States. Spinnaker Networks, the Spinnaker Networks logo, SpinAccess, SpinCluster, SpinFS,

SpinHA, SpinMove, and SpinServer are registered trademarks of Spinnaker Networks, LLC in the United States and/or other countries. SpinAV, SpinManager, SpinMirror, SpinRestore, SpinShot, and SpinStor are trademarks of Spinnaker Networks, LLC in the United States and/or other countries.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

Network Appliance NetCache is certified RealSystem compatible.

Preface	xiii
How to use this Help	xiii
 Chapter 1	
Overview of SnapDrive	1
SnapDrive licensable modules	2
About SnapDrive licensable modules	2
Feature availability	2
What to read	2
Managing SnapDrive module licenses from the MMC	3
SnapDrive-specific terms and technologies	4
block pointers	4
Cluster Service—Microsoft Cluster Service (MSCS)	4
failover	4
filer	5
file system	5
host	5
Host Bus Adapter (HBA)	5
initiator	5
Logical Unit Number (LUN).	5
LUN-type virtual disk	6
network interface card (NIC).	6
snapshot	6
Storage Area Network (SAN)	6
target	6
virtual disk	6
VLD-type virtual disk	6
volume	7
Windows Server cluster	7
How SnapDrive works	8
What SnapDrive does	8
What SnapDrive does not do.	8
SnapDrive virtual boot disk (SAN booting) support.	9
SnapDrive cluster support	9
About the SnapDrive components	9
How virtual disks work	12
How the filer interacts with a virtual disk (LUN)	12
How Windows hosts interact with a virtual disk (LUN).	12
Virtual disk capabilities and limitations	12
Protocols to access virtual disks (LUNs).	13
Overview of how data is accessed from virtual disks	13
Planning disk allocation	14
Configuring RAID groups	14

Hot spare disks	14
Understanding volume size	15
What a volume stores	15
Volume-size rules	15
Requirements for space-related filer settings	16
What space reservation provides	16
Disk space usage with space reservation	16
 Chapter 2	
Preparing to Install SnapDrive	21
What to read	22
Selecting a SnapDrive configuration	23
Recommendations for choosing a configuration	23
Understanding feature availability	24
iSCSI configurations	26
Single host direct-attached to a single filer	26
Single host attached to a single filer through a GbE switch	27
Single host attached to a single filer through a dedicated switch	28
Windows cluster connected to a filer cluster through a dedicated GbE switch	28
FCP configurations	30
Single host direct-attached to a single filer	30
Single host attached to a single filer through a FCP switch	31
Windows cluster attached to a filer cluster through an FCP switch	31
MPIO configurations	33
Single host direct-attached to single filer	33
Windows cluster attached to filer cluster through a switch	34
Preparing hosts	36
Verifying minimum requirements	36
Determining what components are installed	38
Preparing filers	40
Verifying minimum filer requirements	40
Checking filer licenses	41
Starting FCP and iSCSI services	41
Volume and filer options set by SnapDrive	41
SnapDrive-specific limitations	42
Cautions and recommendations	43
Preparing a volume for SnapDrive	43
Creating a filer volume	45
Configuring pass-through authentication for SnapDrive	51
Reasons for configuring pass-through authentication	51

Configuring pass-through authentication	51
Preparing the SnapDrive service account.	54
Types of access to establish	54
SnapDrive user interfaces.	56
SnapDrive user interface capabilities	57

Chapter 3

Installing or Upgrading SnapDrive	59
Upgrading to SnapDrive 3.2	60
Upgrading to SnapDrive 3.2 and Microsoft Windows Server 2003	62
Upgrade process	63
Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks	64
Upgrade and conversion process	64
Preparing for the upgrade and VLD conversion	67
Upgrading a single system to SnapDrive 3.2 and converting VLD-type virtual disks	69
SnapDrive 3.2 upgrade and conversion process	70
Stopping Microsoft Exchange services for VLD conversion	74
Stopping Microsoft SQL Server services for VLD conversion	75
Stopping Domino services for VLD conversion	75
Stopping all other applications for VLD conversion.	76
VLD-to-LUN conversion.	77
Converting a connected VLD-type virtual disk	77
Converting an unconnected VLD-type virtual disk	80
Converting VLD-type virtual disks for MSCS.	82
Converting VLDs in a cluster group	85
Converting a VLD-type quorum disk	86
Upgrading a server cluster to SnapDrive 3.2 if you have no VLD-type virtual disks	88
Upgrade process	88
Preparing for the upgrade	90
Upgrading a single system to SnapDrive 3.2 if you have no VLD-type virtual disks	92
Upgrade process	92
Installing SnapDrive for the first time	93
Installation process	93
Installing the FCP or iSCSI components	94
Installing the iSCSI Software Initiator	96

Upgrading the iSCSI Software Initiator	97
Upgrading the filer	100
Installing the new SnapDrive components	101
Setting a preferred IP address for filer hostname resolution	105
Stopping and starting the SnapDrive service.	105
Installing SnapDrive on SnapManager verification servers	106
Uninstalling old components	107
Uninstalling the VLD driver	107
Uninstalling SnapDrive and MPIO drivers	108
Uninstalling the FCP driver	108
Uninstalling the iSCSI Software Initiator	109

Chapter 4

Managing iSCSI Sessions	111
Tasks for managing iSCSI sessions	112
Establishing an iSCSI session to a target.	113
iSCSI software initiator node naming standards	113
Establishing an iSCSI session to a target.	113
Understanding CHAP authentication	115
Disconnecting an iSCSI target from a Windows host	116
Disconnecting a session to an iSCSI target.	117
Examining details of iSCSI sessions	119
Examining details of iSCSI sessions.	119

Chapter 5

Creating Virtual Disks	121
About virtual disk management	122
Creating a virtual disk	123
Rules for creating a virtual disk	123
Creating a virtual disk	123
Creating a shared virtual disk on a Windows cluster.	128
Creating a virtual disk as a quorum disk on a new Windows cluster.	129
Creating a virtual disk as a quorum disk on a new Windows 2000 Server cluster.	131
Creating a virtual disk as a quorum disk on a new Windows Server 2003 cluster.	133
Creating a shared non-quorum virtual disk on a Windows cluster.	139

Chapter 6	Managing Virtual Disks.	.141
	Connecting virtual disks	.142
	Connecting a virtual disk.	.142
	Disconnecting virtual disks.	.146
	Disconnecting a virtual disk	.146
	Forcing a disconnect	.147
	Deleting a virtual disk	.149
	Expanding virtual disks.	.150
	Expanding a virtual disk	.151
	Expanding a quorum disk	.152
	Managing LUNs not created in SnapDrive.	.155
	Prerequisites for SnapDrive to manage LUNs not created in SnapDrive	155
	Preparing LUNs not created in SnapDrive in a stand-alone Windows	
	configuration	.155
	Preparing LUNs not created in SnapDrive in a clustered Windows	
	configuration	.156
	Examining and modifying the Monitor Time Interval	.158
	Administering SnapDrive remotely	.160
	Enabling SnapDrive notification	.161
 Chapter 7	 SnapDrive Snapshots	 .163
	How snapshots work	.164
	Example: How snapshots work	.164
	Creating snapshots	.166
	Creating a snapshot.	.168
	Scheduling snapshots.	.169
	Connecting to LUNs in a snapshot	.172
	Connecting to a virtual disk (LUN) in a snapshot	.173
	Restoring virtual disks from snapshots	.176
	Restoring a virtual disk from a snapshot	.176
	Deleting snapshots	.178
	Deleting a snapshot.	.178
	Problems deleting snapshots due to busy snapshot error	.179
	Overview of archiving and restoring snapshots	.180

Chapter 8	Overview of the Volume Shadow Copy Service	.181
	What Volume Shadow Copy Service is	.181
	VSS requirements	.181
	Overview of VSS.	.181
	Typical VSS backup process.	.183
	Troubleshooting the NetApp VSS Hardware Provider.	.184
	NetApp VSS Hardware Provider requirement.	.184
	Multiple providers installed	.184
	Viewing installed VSS providers	.184
	Troubleshooting when a snapshot is not taken on the filer	.185
	Verifying that NetApp VSS Hardware Provider was used successfully .185	
	Verifying your NetApp VSS configuration	.186
 Chapter 9	 Multipathing.	 .189
	Feature availability.	.189
	Multipathing overview	.190
	SnapDrive MPIO features and requirements.	.191
	MPIO setup	.193
	Supported MPIO topologies	.193
	MPIO path management	.198
	Creating an MPIO path.	.199
	Understanding MPIO path states.	.200
	Changing MPIO path states	.201
	Removing MPIO on a Microsoft cluster	.202
 Chapter 10	 Overview of SAN Booting.	 .205
	What SAN booting is.	.205
	How SnapDrive supports SAN booting	.205
	Configuring bootable virtual disks	.206
 Chapter 11	 Using SnapMirror with SnapDrive	 .207
	SnapMirror overview.	.208
	Understanding replication	.208
	Requirements for using SnapMirror with SnapDrive	.208
	SnapMirror replication	.211
	Initiating replication	.213
	Connecting to a virtual disk on a destination volume	.215
	Reason for connecting to destination volumes.	.215

Requirements for connecting to a virtual disk on a destination volume .	215
Using SnapDrive to meet the requirements for connecting to a destination volume	215
Connecting to a mirrored destination volume	215
Recovering a cluster from shared virtual disks on a SnapMirror destination .	218
Connecting to shared virtual disks on a SnapMirror destination. . . .	218

Appendix A

SnapDrive Command-Line Reference	223
Using sdcli commands	224
Executing sdcli commands	224
Common command switches.	225
Command-specific switches	227
SnapDrive configuration commands	228
SnapDrive license commands	229
SnapDrive preferred IP address commands	230
iSCSI connection commands	231
iSCSI initiator commands	232
Virtual disk commands	234
Multipathing commands	238
Snapshot commands	242

Appendix B

SnapDrive Requirements and Recommendations.	247
Index	249

Preface

How to use this Help

These Help topics describe how to install, configure, and operate the SnapDrive™ 3.2 software. They do not cover basic system or network administration, such as IP addressing, routing, and network topology.

The following topics provide information on using the SnapDrive Help:

- ◆ “[Audience](#)” on page xiii
- ◆ “[About filer command execution](#)” on page xiii
- ◆ “[Interface conventions](#)” on page xiv
- ◆ “[Typographic conventions](#)” on page xiv
- ◆ “[Special messages](#)” on page xv

Audience: This Help is for system administrators who possess a working knowledge of Network Appliance™ storage appliances, such as filers.

This Help assumes that you are familiar with the following topics:

- ◆ The Network File System (NFS) and CIFS protocols, as applicable to file sharing and file transfers
- ◆ Fibre Channel Protocol (FCP)
- ◆ Internet SCSI (iSCSI) protocol
- ◆ Basic network functions and operations
- ◆ Windows® 2000 server and Windows Server 2003 management
- ◆ Windows security
- ◆ Data storage array administration concepts
- ◆ Network Appliance filer management

About filer command execution: You can manage filers in the following three ways:

- ◆ Through the Web-based FilerView® utility
- ◆ From the filer console
- ◆ From any computer on the network that can access the filer through a Telnet session

Note

The previous three management methods are specific to filer management only, not for SnapDrive operation.

Interface conventions: Throughout this Help, all examples involving commands and procedures assume a host running Windows 2000 Server or Windows Server 2003.

For procedures that use the Windows graphical user interface, the term “select” means that you should click, double-click, or right-click the control element, as appropriate. In many instances, you can press a corresponding key to achieve the same result. For example, if that element is a radio button, a dot appears in the associated circle; if it is a check box, an “x” appears in the box; if it is an item in a drop-down list, that item becomes highlighted; if it is a button control, a command is usually executed, and so on.

Menus, toolbars, and icons: When referring to graphical interface navigation within FilerView, Windows 2000 Server or Windows Server 2003, the greater-than symbol (>) points to the next element leading to your final destination. For example, My Computer > Manage > System Tools > Device Manager > SCSI and RAID controllers > Network Appliance VLD means to right-click the My Computer icon on the desktop of the system you are configuring, click Manage on the drop-down menu, double-click System Tools, double-click Device Manager, double-click SCSI and RAID controllers, then double-click Network Appliance VLD.

Keystrokes: When describing key combinations, this Help uses a hyphen (-) to separate individual keys. For example, “Ctrl-D” means “press the ‘Control’ and ‘D’ keys simultaneously.” Also, this guide uses the term “Enter” to refer to the key that generates a carriage return, although the key is labeled “Return” on some keyboards.

Visual Elements: In describing what to look for when executing SnapDrive-related operations, this document uses the term “screen” synonymously with “application window” whenever discussing the Windows environment. “Panel” refers either to a pop-up message or to a tabbed display, as in a property sheet or a procedural wizard. “Pane” refers to a portion of the application window, usually containing a list of items and having its own set of scroll bars.

Typographic conventions: The following table describes the typographic conventions used in this guide.

Convention	Type of information
<i>Italic type</i>	Words or characters that require special attention. Placeholders for information you must supply. For example, if the guide refers to <i>share name</i> , you must enter the actual share name. Book titles in cross-references.

Convention	Type of information
Monospaced font	Command and daemon names. Information displayed on the system console or other computer monitors. The contents of files.
Bold monospaced font	Words or characters you type at the system console or some other computer console. What you type is always shown in lowercase letters, unless you must type it in uppercase letters.

Special messages: This Help uses the following conventions to indicate special messages:

Note

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

Caution

A caution contains instructions you must follow to avoid damage to equipment, a system crash, or the loss of data.

This overview covers the following topics:

- ◆ “[SnapDrive licensable modules](#)” on page 2
- ◆ “[SnapDrive-specific terms and technologies](#)” on page 4
- ◆ “[How SnapDrive works](#)” on page 8
- ◆ “[How virtual disks work](#)” on page 12
- ◆ “[Planning disk allocation](#)” on page 14
- ◆ “[Understanding volume size](#)” on page 15

SnapDrive licensable modules

About SnapDrive licensable modules

SnapDrive 3.2 enables you to install NetApp® Multipath I/O (MPIO) with Path Management and LUN Provisioning and Snapshot™ Management software as separately licensed modules. With separately licensed modules you can choose to purchase licenses for and to install the following:

- ◆ MPIO only
- ◆ LUN Provisioning and Snapshot Management only
- ◆ MPIO and LUN Provisioning and Snapshot Management

Feature availability

If you do not license a particular module in SnapDrive, that module will not be installed and you will not have access to the features that module provides. For example, if you license only the MPIO module, you will not have access to the features in the LUN Provisioning and Snapshot Management module, such as LUN creation in SnapDrive. If the MPIO module is not licensed and installed, path management with SnapDrive is not available. Additionally, if you remove a license for a module that was previously licensed, features for that module will no longer be available.

What to read

If you licensed only the MPIO module, read the following sections for more information:

- ◆ Chapter 2, “[Preparing to Install SnapDrive](#),” on page 21
- ◆ Chapter 3, “[Installing or Upgrading SnapDrive](#),” on page 59
- ◆ Chapter 9, “[Multipathing](#),” on page 189

If you licensed LUN Provisioning and Snapshot Management without MPIO, disregard the multipathing section. Refer to all other sections for additional information about this module.

If you licensed both LUN Provisioning and Snapshot Management and MPIO, read all sections for more information.

Managing SnapDrive module licenses from the MMC

To view, add or delete licenses for MPIO or LUN Provisioning and Snapshot Management after either module has been installed, from the Microsoft Management Console (MMC), complete the following steps.

Note

You can only use the MMC to add or delete the SnapDrive 3.2 module licenses if the module has already been installed. Even if you choose to only license and install MPIO, the LUN Provisioning and Snapshot module is always installed, for disk enumeration purposes. However; many of the features that LUN Provisioning and Snapshot Management provides are not available until you supply a license. This can be done in the MMC, even if you originally chose an MPIO-only installation.

Step	Action
1	Expand the Storage option in the left pane of the MMC window, if it is not already expanded.
2	Select SnapDrive, then right-click SnapDrive and select SnapDrive Licenses. Result: The SnapDrive Licenses window is displayed.
3	View, add or remove (delete) the license(s) for MPIO and LUN Provisioning and Snapshot Management, as needed.

SnapDrive-specific terms and technologies

This section defines the terms and technologies that you come across while reading this document. The section defines the terms in a *SnapDrive-specific* context. Go to any of the following topics for more information.

- ◆ “[block pointers](#)” on page 4
- ◆ “[Cluster Service—Microsoft Cluster Service \(MSCS\)](#)” on page 4
- ◆ “[failover](#)” on page 4
- ◆ “[filer](#)” on page 5
- ◆ “[file system](#)” on page 5
- ◆ “[host](#)” on page 5
- ◆ “[Host Bus Adapter \(HBA\)](#)” on page 5
- ◆ “[initiator](#)” on page 5
- ◆ “[Logical Unit Number \(LUN\)](#)” on page 5
- ◆ “[LUN-type virtual disk](#)” on page 6
- ◆ “[network interface card \(NIC\)](#)” on page 6
- ◆ “[snapshot](#)” on page 6
- ◆ “[Storage Area Network \(SAN\)](#)” on page 6
- ◆ “[target](#)” on page 6
- ◆ “[virtual disk](#)” on page 6
- ◆ “[VLD-type virtual disk](#)” on page 6
- ◆ “[volume](#)” on page 7
- ◆ “[Windows Server cluster](#)” on page 7

block pointers

Block pointers are used by a filer to locate the physical disk block on which data is stored.

Cluster Service— Microsoft Cluster Service (MSCS)

The Microsoft Cluster Service (also known as MSCS) is a service that runs on hosts in a Windows Server cluster and enables the clustering functionality on those hosts. *See also* Windows Server cluster.

failover

Failover refers to situations where a system component fails, and another component takes over its functions while the system continues to operate.

filer	A filer is a NetApp® storage appliance that supports the FCP (Fibre Channel Protocol), iSCSI (Internet SCSI), and GbE (Gigabit Ethernet) protocols.
file system	A file system refers to NTFS, the native Windows 2000 Server and Windows Server 2003 file system supported by SnapDrive. (NetApp filers use the Write Anywhere File Layout (WAFL®) file system internally, but SnapDrive makes WAFL transparent to virtual disk users, who interact with data stored on the filer using Windows procedures only.)
host	A host is a computer system that accesses storage on a filer. For this document, the host must be running the following software: ◆ One of the following Windows servers: ❖ Windows 2000 Server ❖ Windows 2000 Advanced Server (for Windows-cluster configurations) ❖ Windows Server 2003 (Standard Edition or Enterprise Edition) ◆ SnapDrive 3.2
Host Bus Adapter (HBA)	A Host Bus Adapter (HBA) refers to the adapters used to connect hosts and filers in a NetApp Storage Area Network (SAN) so that hosts can access Logical Unit Numbers (LUNs) on the filers using FCP. <i>See also</i> Logical Unit Number (LUN).
initiator	An initiator is used to send SCSI I/O commands to a target. FCP initiator: An FCP initiator refers to a port on an HBA on a host. iSCSI initiator: An iSCSI initiator refers to a port on a NIC on a host. <i>See also</i> target.
Logical Unit Number (LUN)	A Logical Unit Number (LUN) is a SCSI identifier of a logical unit of storage on a target. This manual often refers to LUNs as virtual disks, and vice versa. <i>See also</i> virtual disks.

LUN-type virtual disk	A LUN-type virtual disk is a type of virtual disk that is used to store data using the Fibre Channel Protocol (FCP) or iSCSI protocol.
network interface card (NIC)	A network interface card (NIC) refers to a Gigabit (commonly known as GbE) or a Fast Ethernet card that is compliant with the IEEE 802.3 standards. These cards can provide the following connectivity functions: ◆ Connect hosts and filers to a local area network (LAN) ◆ Connect hosts and filers to data-center switching fabrics, specifically, enable hosts to connect to LUNs on filers using iSCSI
snapshot	A snapshot refers to the NetApp Snapshot technology, which facilitates recovery after accidental deletion or modification of the data stored on a filer by referencing a point-in-time image of that data.
Storage Area Network (SAN)	A Storage Area Network (SAN) is a storage setup composed of one or more filers and connected to one or more hosts in an FCP or an iSCSI environment. To a Windows host running SnapDrive, a connected SAN is just another target storage device within which SnapDrive can create and manage virtual disks (LUNs). <i>See also</i> target and virtual disk.
target	A target is used to receive the SCSI I/O commands that an initiator sends. For NetApp SANs, a target is a NetApp filer. <i>See also</i> initiator.
virtual disk	A virtual disk is a functional unit of filer storage that, for all practical purposes, behaves like a locally attached disk on a Windows host. This manual often refers to virtual disks as Logical Unit Numbers (LUNs), and vice versa.
VLD-type virtual disk	A Virtual Local Disk-type (VLD) virtual disk is a type of virtual disk created and supported by SnapDrive 2.1 and earlier versions to store data in GbE environments. VLD-type virtual disks are legacy in SnapDrive 3.2 or later versions.

volume

A volume is a functional unit of filer storage comprising a collection of physical disks. A volume can be composed of one or more redundant array of independent disks (RAID) groups to ensure data integrity and availability if multiple disks fail simultaneously within the same volume. For more information about filer volumes, see the *Data ONTAP Storage Management Guide*.

Windows Server cluster

A Windows Server cluster refers to a two-node to a four-node host cluster. The number of nodes in a cluster depends on the software running on the host nodes. The host nodes in a Server cluster must be running one of the following software packages:

- ◆ Windows 2000 Advanced Server (for a 2-node cluster)
- ◆ Windows Server 2003 Enterprise Edition (for up to a 4-node cluster)

How SnapDrive works

This section explains briefly what SnapDrive does and does not do and describes its components. Go to any of the following topics for more information.

- ◆ [“What SnapDrive does”](#) on page 8
- ◆ [“What SnapDrive does not do”](#) on page 8
- ◆ [“SnapDrive cluster support”](#) on page 9
- ◆ [“About the SnapDrive components”](#) on page 9

What SnapDrive does

SnapDrive software integrates with the Windows Volume Manager so that NetApp filers can serve as virtual storage devices for application data in Windows 2000 Server and Windows Server 2003 environments.

SnapDrive is dependent on the Virtual Disk Service. The Virtual Disk Service must be started on the host prior to installing SnapDrive.

SnapDrive manages virtual disks (LUNs) on a NetApp filer, making these virtual disks available as local disks on Windows hosts. This allows Windows hosts to interact with the virtual disks just as if they belonged to a directly attached redundant array of independent disks (RAID).

SnapDrive provides the following additional features:

- ◆ It enables online storage configuration, virtual disk expansion, and streamlined management.
- ◆ It integrates NetApp Snapshot technology, which creates point-in-time images of data stored on virtual disks.
- ◆ It works in conjunction with SnapMirror® software to facilitate disaster recovery from either asynchronously or synchronously mirrored destination volumes.

What SnapDrive does not do

SnapDrive does not support the following uses:

- ◆ A virtual disk managed by SnapDrive cannot be configured as a “dynamic” disk (a storage device that is divided into volumes rather than partitions); it can serve only as a “basic” disk (a storage device for host-side application data).
- ◆ A virtual disk as an extended partition. SnapDrive supports only a single, primary partition on a virtual disk.

- ◆ In the case of a filer that uses the optional MultiStore® feature of Data ONTAP™ software to create virtual filers (vFiler™ units), SnapDrive can create, connect to, and manage virtual disks (LUNs) only on the “hosting” filer (the physical filer), not on the vFilers.
For more information, see the *Data ONTAP MultiStore Management Guide*.
- ◆ Virtual disks created in FilerView or at the filer command line cannot be managed unless certain steps are taken to prepare these disks for SnapDrive. For more information, see “[Managing LUNs not created in SnapDrive](#)” on page 155.

SnapDrive virtual boot disk (SAN booting) support

SnapDrive supports both bootable virtual disks (SAN booting) and nonbootable virtual disks and differentiates between the two in the Microsoft Management Console (MMC) by representing each virtual disk type with a unique icon.

SnapDrive cluster support

SnapDrive can be deployed in a nonclustered configuration (a single host connected to a single filer) as well as in topologies involving the following cluster technologies:

- ◆ Windows clusters (MSCS)
To protect against node failure, Windows clustering fails over applications from the host node to the surviving node.
- ◆ NetApp cluster failover
If a filer fails, the partner filer takes over the functions of the failed filer, thus protecting data and ensuring continued storage availability.

About the SnapDrive components

Some of the software components of SnapDrive are integrated in the SnapDrive software; others are available on the NetApp on the Web™ (NOW™) site at <http://now.netapp.com/>.

Caution

All SnapDrive components, and their respective software and firmware, must be installed on the filer and Windows host before you can successfully use the software.

Integrated components: The following SnapDrive components are integrated in the software and are automatically installed during the SnapDrive installation process:

- ◆ SnapDrive “snap-in”

This software module integrates with the Microsoft Management Console (MMC) to provide a graphical interface for managing virtual disks on the filer. The module does the following:

- ❖ Resides in the Windows 2000 Server and Windows Server 2003 computer management storage tree
- ❖ Provides a native MMC snap-in user interface for configuring and managing virtual disks
- ❖ Supports Remote Administration so that you can manage SnapDrive on another host
- ❖ Provides SnapMirror® integration
- ❖ Provides AutoSupport integration, including event notification
- ◆ SnapDrive command-line interface

The sdcli.exe utility enables you to manage virtual disks from the command prompt of the Windows host. You can do the following tasks with the sdcli.exe utility:

 - ❖ Enter individual commands
 - ❖ Run management scripts
- ◆ Underlying SnapDrive service

This software interacts with software on the filer to facilitate virtual disk management for the following:

 - ❖ A host
 - ❖ Applications running on a host
- ◆ MPIO path management and drivers (if licensed)

This module provides a set of drivers that protects against path failure by enabling redundant paths from the host (initiator) to a LUN (target storage device) on the filer. The module has the following features:

 - ❖ It includes one NetApp module and three Microsoft drivers.
 - ❖ It is installed as a separately licensed module during SnapDrive installation.
 - ❖ It supports the use of redundant FCP or iSCSI paths to LUNs.
 - ❖ It requires, for FCP, the pair of HBAs supplied in the NetApp Dual HBA FCP Attach Kit for Windows, or, for iSCSI, the Microsoft iSCSI Software Initiator or the QLogic 4010 iSCSI HBAs. For an up-to-date list of supported initiators, see the SnapDrive Compatibility Matrix on NOW at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/snapdrive.shtml.

- ◆ NetApp Volume Shadow Copy Service (VSS) Hardware Provider on Windows 2003 hosts

The NetApp VSS Hardware Provider is a VSS hardware provider, which is a module of the Microsoft VSS framework. The NetApp VSS Hardware Provider enables VSS snapshot technology on NetApp filers when SnapDrive is installed on Windows 2003 hosts.

NOW site components: The following SnapDrive components are available at the NOW site:

- ◆ iSCSI initiator

The iSCSI initiator enables SCSI I/O operations using the iSCSI protocol between a host and a filer. The initiator has the following features:

- ❖ It includes an iSCSI driver that supports iSCSI connections between a host and a filer.
- ❖ It is installed like a SCSI/RAID controller on a host.
- ❖ It includes either an HBA hardware component or the software initiator only, through which the iSCSI driver enables the host's standard Ethernet NIC (preferably GbE) to be used for the SCSI operations.

The necessary software for the iSCSI software initiator is in the iSCSI Host Support Kit for Windows. The necessary software and firmware for the iSCSI hardware driver is in the iSCSI Host Attach Kit. Both can be downloaded at <http://now.netapp.com/NOW/cgi-bin/software/>.

- ◆ FCP initiator

The FCP initiator enables SCSI I/O operations using the FCP protocol between a host and a filer. The initiator has the following features:

- ❖ It includes an FCP driver that supports FCP connections between a host and a filer.
- ❖ It is a SCSI/RAID controller on the host.
- ❖ It includes an HBA hardware component.

The necessary software and firmware for the FCP driver is in the SAN Host Attach Kit for Fibre Channel Protocol on Windows at <http://now.netapp.com/NOW/cgi-bin/software/>.

How virtual disks work

This sections explains how virtual disks work. Go to any of the following topics for more information.

- ◆ [“How the filer interacts with a virtual disk \(LUN\)”](#) on page 12
- ◆ [“How Windows hosts interact with a virtual disk \(LUN\)”](#) on page 12
- ◆ [“Virtual disk capabilities and limitations”](#) on page 12
- ◆ [“Protocols to access virtual disks \(LUNs\)”](#) on page 13
- ◆ [“Overview of how data is accessed from virtual disks”](#) on page 13

How the filer interacts with a virtual disk (LUN)

To the filer, a virtual disk (LUN) is a logical representation of a physical unit of storage. Therefore, the filer handles each virtual disk as a single storage object. The size of this virtual disk (LUN) is slightly larger than the raw disk size reported to the Windows host. SnapDrive must be used to expand the virtual disk in order for the Windows host to recognize the newly created disk space.

Note

You can expand a virtual disk, but you cannot reduce it in size.

How Windows hosts interact with a virtual disk (LUN)

You manage virtual disks (LUNs) on the filer just as you manage other Windows disks that store application data. Similarly, the virtual disks on the filers are automatically formatted by SnapDrive the same way that you format other Windows disks. Moreover, a Windows host interacts with all user data files on the virtual disk as if they were NTFS files distributed among the disks of a locally attached RAID array.

You do not need to be aware that your data files actually are part of a single virtual disk file that is stored on the filer; the intricacies of WAFL file management remain completely transparent to you as you manage SnapDrive virtual disks from the Windows host.

Virtual disk capabilities and limitations

A virtual disk managed by SnapDrive can be used for data storage and can be a boot disk. A virtual disk cannot be a dynamic disk.

SnapDrive can also take snapshots of virtual disks when they are used for data storage, and it can work with SnapMirror at the volume level for disaster recovery.

When a virtual disk is a boot disk, the following actions are disabled or unavailable in SnapDrive:

- ◆ Snapshots
- ◆ Disconnect
- ◆ Delete
- ◆ Expand

Protocols to access virtual disks (LUNs)

You can access the SnapDrive-created virtual disks (LUNs) using one or both of the following two protocols:

- ◆ Fibre Channel Protocol (FCP)
- ◆ iSCSI

You must have the appropriate hardware and firmware, if any, and software installed on your host and the filer before you can use these protocols to access virtual disks.

Note

SnapDrive 3.2 supports both FCP and iSCSI on the same Windows host connected to different LUNs. SnapDrive 3.2 does not support FCP and iSCSI on the same Windows host connecting to the same LUN. It is possible, however, to have different nodes in a cluster, each using a different protocol, connecting to the same LUN.

Overview of how data is accessed from virtual disks

In a NetApp SAN environment, an initiator (on the Windows host) initiates a SCSI I/O operation to a target (filer). The operation can be initiated using either the FCP or the iSCSI protocol, depending on the type of initiator installed on your Windows host and the setup on the target. A target can receive SCSI requests using FCP if a supported HBA is installed and FCP is licensed. Similarly, a target can receive SCSI requests using iSCSI, if iSCSI is licensed.

After a target receives a SCSI I/O request, the appropriate operation is performed by writing data to or fetching data from the virtual disk (LUN).

Planning disk allocation

This section explains the considerations involved in planning how to allocate disks on the filer. Go to any of the following topics for more information.

- ◆ [“Configuring RAID groups”](#) on page 14
- ◆ [“Hot spare disks”](#) on page 14

Configuring RAID groups

You can assign more than one RAID group to a single filer volume, especially if the volume contains more than 14 disks. This ensures data integrity and availability if multiple disks fail simultaneously within the same volume.

The number of disks in each RAID group on a volume should be balanced to allow maximum performance.

For more information about RAID groups, see the *Data ONTAP Storage Management Guide* for your version of Data ONTAP.

Hot spare disks

Hot spare disks are disks held in reserve globally in case an active disk fails.

Hot spare disks in a filer do not belong to any particular volume. In fact, any disk in the filer that has not yet been assigned to a volume (and has not been marked bad) is treated as a hot spare.

If the filer has multiple volumes, any available spare can replace a failed disk on any volume, as long as the following conditions are true:

- ◆ The spare is as large or larger than the disk it replaces.
- ◆ The replacement disk resides on the same filer as the failed disk.

Network Appliance recommends that you always keep at least one hot spare disk in the filer. This ensures that a spare disk is available at all times. As soon as an active disk fails, the filer automatically reconstructs the failed disk by using the hot spare. You don't have to intervene manually—except to replace the failed disk after the reconstruction is complete.

Note

To receive proactive alerts about the status of disks in your filer, enable the Data ONTAP AutoSupport feature.

Understanding volume size

This section explains filer volumes and how to manage space reservation. Go to any of the following topics for more information.

- ◆ [“What a volume stores”](#) on page 15
- ◆ [“Volume-size rules”](#) on page 15
- ◆ [“Requirements for space-related filer settings”](#) on page 16
- ◆ [“What space reservation provides”](#) on page 16
- ◆ [“Disk space usage with space reservation”](#) on page 16

What a volume stores

The space on a volume is used to store the following:

- ◆ The virtual disks (LUNs), which in turn contain the host data
- ◆ Data that changes between snapshots (Even if all the data on the virtual disks changes following the most recent snapshot, and none is committed to disk, everything can still be written to disk.)
- ◆ The active file system of the virtual disk
- ◆ Metadata

Volume-size rules

The following factors govern the appropriate minimum size for a volume that will hold a virtual disk:

- ◆ The volume must be more than twice the combined size of all the virtual disks on the volume if snapshots of the volume will be created. This enables the volume to hold the virtual disks and a special reserved space, so that no matter how much the contents of the virtual disks change between snapshots, the entire contents of the disks can be written to the volume. See [“How snapshots work”](#) on page 164 for more information.
- ◆ The volume must also provide enough additional space to hold the number of snapshots you intend to keep online. The amount of space consumed by a snapshot depends on the amount of data that changes after the snapshot is taken. The maximum number of snapshots is 255 per filer volume.

Requirements for space-related filer settings

The following space-related settings must be configured on your filer for SnapDrive to operate as expected:

- ◆ The space reservation option must be set to On for each virtual disk.
Upon virtual disk creation or connection, SnapDrive automatically sets space reservation to On for each virtual disk.

Caution

To avoid interfering with SnapDrive operation, you must never set space reservation to Off.

- ◆ The snap reserve option must be reset to 0 percent for all volumes holding SnapDrive virtual disks.
Data ONTAP can reserve a certain percentage of raw volume capacity exclusively for snapshot creation. By default, the snap reserve percentage on the filer volume is 20 percent, and SnapDrive does not automatically change this. Therefore, you must manually reset the percentage to 0 percent. For details, see [“Resetting the snap reserve option”](#) on page 49.

What space reservation provides

Space reservation ensures that write operations to a virtual disk always have enough space. Space reservation prevents snapshot creation whenever the filer volume storing the virtual disk might not have enough free space to accommodate all future write operations to virtual disks on that volume. This prevents situations where all writable blocks on the volume are locked by snapshots, and no blocks are available for writing new data.

Disk space usage with space reservation

When you first create a virtual disk (LUN) with space reservation enabled, it is granted a space reservation equal to its size. This reserved space is subtracted from the total available disk space on the filer volume where the virtual disk resides. As data is written to the virtual disk, the space occupied by that data is subtracted from the remaining available volume space and added to the used volume space.

When you create a snapshot of the filer volume holding the virtual disk, that snapshot locks down all the disk blocks occupied by live data.

By monitoring the remaining available space in the filer volume, space reservations determine whether snapshot creation is allowed. When the amount of available space on the filer volume falls to zero, snapshot creation is blocked.

Example: The following sequence illustrates the effect of various virtual disk operations upon free space for a virtual disk for which space reservation has been enabled.

Note

The metrics in the Results column correspond to the Used, Reserved, Available, and Total metrics provided by the filer command `df -r`.

Action	Results	Comment
Create a 100-GB volume.	Used: 0 GB Reserved: 0 GB Available: 100 GB Volume Total: 100 GB	
Create a 40-GB virtual disk on that volume.	Used: 0 GB Reserved: 40 GB Available: 60 GB Volume Total: 100 GB Snapshot creation is allowed.	If the virtual disk size was limited to accommodate at least one snapshot when it was created, then virtual disk size will always be less than one half of the volume size.
Write 40 GB of data to the virtual disk.	Used: 40 GB Reserved: 40 GB Available: 60 GB Volume Total: 100 GB Snapshot creation is allowed.	When you write data to the virtual disk, it counts against the running Used total. The sum of Used, Reserved, and Available always equals Volume Total.
Create a snapshot of the virtual disk.	Used: 40 GB Reserved: 40 GB Available: 20 GB Volume Total: 100 GB Snapshot succeeds.	The snapshot locks all the data on the virtual disk so that even if that data is later deleted, it remains in the snapshot until the snapshot is deleted. After a snapshot is created, the reserved space must now be large enough to ensure that any future writes to the disk succeed.

Action	Results	Comment
Overwrite all 40 GB of data on the virtual disk with entirely new data.	Used: 60 GB Reserved: 40 GB Available: 0 GB Volume Total: 100 GB Snapshot creation is blocked.	The amount of space used on the volume increases, because the original 40 GB of data belongs to the snapshot and therefore continues to count against the Used total. Reserved space must be equal to the size of the LUN (40 GB), and reserved and used space together cannot exceed the size of the volume, so used space is displayed as 60 GB rather than the expected 80 GB. However, all data is preserved. You cannot take a snapshot now, because no space is available. That is, all space is used by data or held in reserve so that any and all changes to the content of the virtual disk can be written to the volume.
Expand the volume by 100 GB.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation is allowed.	After you expand the volume, free space becomes available again. Therefore, snapshot creation is no longer blocked. In addition, the Used and Available totals are adjusted to reflect the fact that reserved space is no longer being used to hold disk data.
Overwrite all 40 GB of data on the virtual disk with entirely new data.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation is allowed.	Because none of the overwritten data belongs to a snapshot, it disappears when the new data replaces it, so the Used total remains unchanged.
Create a snapshot of the virtual disk.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation is allowed.	The snapshot locks all 40 GB of data currently on the virtual disk. A total of 80 GB of data now belongs to the two snapshots of the virtual disk. Reserved space remains equal to the size of the LUN, or 40 GB.

Action	Results	Comment
Overwrite all 40 GB of data on the virtual disk with entirely new data.	Used: 120 GB Reserved: 40 GB Available: 40 GB Volume Total: 200 GB Snapshot creation is allowed.	Because the data being replaced belongs to a snapshot, it remains on the volume.
Expand the virtual disk by 40 GB.	Used: 120 GB Reserved: 80 GB Available: 0 GB Volume Total: 200 GB Snapshot creation is blocked.	The amount of reserved space increases to match the expanded size of the virtual disk. This guarantees that the entire contents of the virtual disk can be written to the volume. Because the available space is now 0, snapshot creation is blocked.
Delete both snapshots.	Used: 40 GB Reserved: 40 GB Available: 120 GB Volume Total: 200 GB Snapshot creation is allowed.	The 80 GB of data locked by the two snapshots disappears from the Used total when the snapshots are deleted. Because there are no more snapshots of this virtual disk, the reserved space goes to 40 GB, enough to guarantee any future write operations. Snapshot creation is once again allowed.
Delete the virtual disk.	Used: 0 GB Reserved: 0 GB Available: 200 GB Volume Total: 200 GB	Because no snapshots exist for this volume, deletion of the virtual disk causes the used space to go to 0 MB.

The topics that follow explain the tasks you must complete before installing the SnapDrive application software. These tasks include:

- ◆ Determining your SnapDrive configuration and what it requires in terms of hardware, software, settings, and background reading
- ◆ Configuring your hosts
- ◆ Configuring your filers
- ◆ Cabling your SnapDrive configuration
- ◆ Setting up your SnapDrive service account
- ◆ Verifying your configuration and domain settings

Note

The requirements discussed in these topics apply to *each* filer and host you connect in the various configurations supported by SnapDrive.

Go to any of the following topics for more information:

- ◆ [“What to read”](#) on page 22
- ◆ [“Selecting a SnapDrive configuration”](#) on page 23
- ◆ [“iSCSI configurations”](#) on page 26
- ◆ [“FCP configurations”](#) on page 30
- ◆ [“MPIO configurations”](#) on page 33
- ◆ [“Preparing hosts”](#) on page 36
- ◆ [“Preparing filers”](#) on page 40
- ◆ [“Configuring pass-through authentication for SnapDrive”](#) on page 51
- ◆ [“Preparing the SnapDrive service account”](#) on page 54

What to read

SnapDrive installation requirements and procedures vary according to the protocols you use to create virtual disks. Use the following table to determine which NetApp documents you should read.

Note

You can obtain the documents listed below at <http://now.netapp.com/>.

To create...	Read...
iSCSI-accessed virtual disks	◆ This document ◆ If you are using the Microsoft iSCSI Software Initiator, the Microsoft iSCSI Software Initiator documentation, available at the Microsoft site. For the most up-to-date list of supported initiators, see the SnapDrive Compatibility Matrix at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/snapdrive.shtml. ◆ If you are using NetApp's iSCSI Host Attach Kit for Windows, the <i>iSCSI Host Attach Kit for Windows Installation and Setup Guide</i>, or, if you are not, the vendor documentation for your Windows Hardware Quality Lab (WHQL) signed iSCSI HBA. ◆ Data ONTAP <i>Block Access Management Guide for iSCSI</i>, which shipped with your filer
FCP-accessed virtual disks	◆ This document ◆ <i>SAN Host Attach Kit for Fibre Channel Protocol on Windows Installation and Setup Guide</i>, which shipped with your NetApp Windows Attach Kit For the most up-to-date list of supported initiators, see the SnapDrive Compatibility Matrix at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/snapdrive.shtml. ◆ Data ONTAP <i>Block Access Management Guide for FCP</i>, which shipped with your filer

Selecting a SnapDrive configuration

SnapDrive supports a variety of configurations. The following factors can help you decide which configuration to deploy:

- ◆ LUN access protocol—iSCSI, FCP, or both
- ◆ Host operating system—Windows 2000 Server (or Advanced Server for Windows cluster configurations) or Windows Server 2003 (Standard Edition or Enterprise Edition)
- ◆ Host operating system Service Pack level
 - ❖ For Windows 2000 Server: SP4
 - ❖ For Windows Server 2003: no Service Pack required
- ◆ Host operating system hotfix level (various combinations of mandatory and optional hotfixes, which are determined by host operating system, Service Pack level, and special SnapDrive options. See [“Understanding feature availability”](#) on page 24.)
- ◆ Special options (Windows clustering, filer cluster failover, MPIO)

Go to any of the following topics for more information.

- ◆ [“Recommendations for choosing a configuration”](#) on page 23
- ◆ [“Understanding feature availability”](#) on page 24

Recommendations for choosing a configuration

Network Appliance recommends the following:

- ◆ For all configurations:
 - ❖ Place the host and filer in the same broadcast domain, so that virtual disk I/O commands do not need to traverse router hops.
- ◆ For Windows cluster configurations:
 - ❖ Segregate internal cluster traffic from both host-filer traffic and data-center traffic whenever possible.

Do not permit internal cluster traffic on a GbE network used for transferring data from host to filer. Instead, use a Fast Ethernet connection for all cluster traffic. This ensures that a single network error cannot affect both the connection for internal cluster traffic and the connection to the quorum disk.

To determine the feasibility of SnapDrive configurations not described in the following sections, consult your NetApp Sales Engineer.

Related topics:

- ◆ [“Preparing hosts”](#) on page 36
- ◆ [“Preparing filers”](#) on page 40

Understanding feature availability

The following table lists the SnapDrive features supported on the Windows host operating systems for each virtual disk type, as well as any hotfixes required on the specific operating systems.

	Feature availability by virtual disk type	
Host operating system	iSCSI	FCP
Windows 2000 Server or Advanced Server with...		
SP4 with the following hotfixes: ◆ 293778 ◆ 815198 ◆ 822831, only if you encounter the problem described in Microsoft’s Knowledge Base article 822831. ◆ 867818 ◆ 885294	Standard features, Windows cluster, MPIO Note ————— MPIO is not supported with iSCSI on Windows 2000 clustered systems. —————	Standard features, Windows cluster, MPIO

Windows Server 2003 Standard Edition or Enterprise Edition with...		
	Feature availability by virtual disk type	
Host operating system	iSCSI	FCP
The following hotfixes: ◆ 824354, for Windows cluster only ◆ 833167 ◆ 867818 ◆ 886652 ◆ 886800, for Windows cluster only ◆ 887532 ◆ 896592 ◆ 898706 Note_____ For more information about a specific hotfix listed here, see the Microsoft Knowledge Base article of the same number at http://support.microsoft.com/. _____ No Service Packs are required at this time.	Standard features, Windows cluster up to four hosts, MPIO	Standard features, Windows cluster up to four hosts, MPIO
Windows Server 2003 Enterprise Edition with...		
SP1 No hotfixes are required at this time.	Standard features, Windows cluster up to four hosts, MPIO	Standard features, Windows cluster up to four hosts, MPIO
Note_____ For a list of the latest service packs and hotfixes required by SnapDrive, see the SnapDrive 3.2 Description Page at http://now.netapp.com/NOW/cgi-bin/software/. _____		

iSCSI configurations

This section describes the supported iSCSI configurations. Go to any of the following topics for details.

- ◆ [“Single host direct-attached to a single filer”](#) on page 26
- ◆ [“Single host attached to a single filer through a GbE switch”](#) on page 27
- ◆ [“Single host attached to a single filer through a dedicated switch”](#) on page 28
- ◆ [“Windows cluster connected to a filer cluster through a dedicated GbE switch”](#) on page 28

Related topics:

- ◆ [“FCP configurations”](#) on page 30
- ◆ [“MPIO configurations”](#) on page 33
- ◆ [“Understanding feature availability”](#) on page 24

Single host direct-attached to a single filer

The configuration in the following illustration uses a GbE crossover cable to attach the host directly to the filer. Such an arrangement minimizes latency and eliminates unwanted network broadcasts.

The host and filer in this configuration each use the following connection hardware:

- ◆ 1 GbE NIC dedicated to host-filer data transfer
- ◆ 1 Fast Ethernet (or GbE) NIC to connect to the data-center fabric

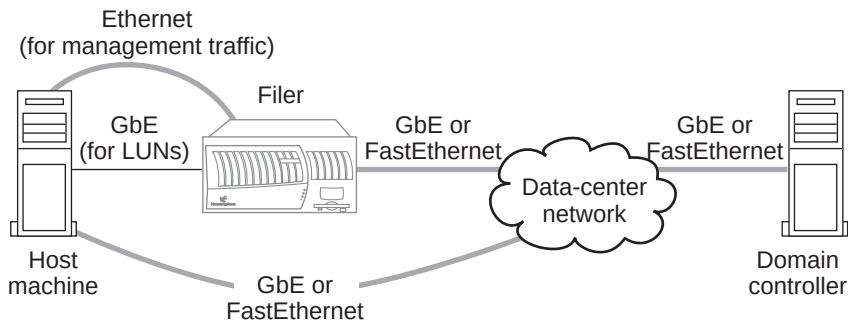
Note

Both the filer and the host *must* be within the same broadcast domain.

Note

LUN traffic and management traffic in an iSCSI configuration can be performed over a single GbE connection; however, NetApp recommends separating the traffic as shown in the following illustration.

Windows requirements: For Windows OS and hotfix requirements for iSCSI, see [“Understanding feature availability”](#) on page 24.



Single host attached to a single filer through a GbE switch

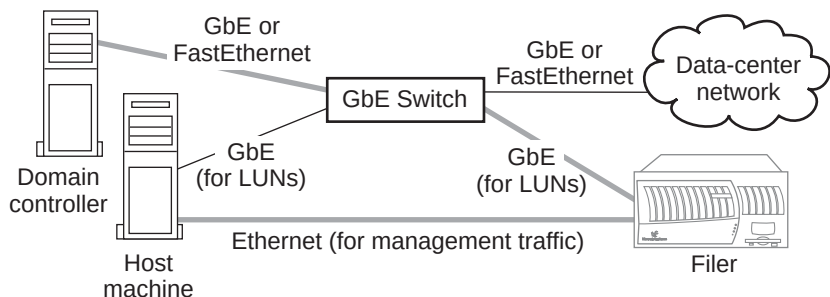
The following illustration depicts a single-homed configuration that places a network switch between the filer and the host. Such an arrangement provides good performance and also segregates host-filer traffic by directing it through a single pair of switch ports.

Because the switch connects to the data-center fabric, the host and filer in this configuration each use a single GbE NIC both for host-filer data transfers and for connecting to the data-center fabric.

Note

LUN traffic and management traffic in an iSCSI configuration can be performed over a single GbE connection; however, NetApp recommends separating the traffic as shown in the following illustration.

Windows requirements: For Windows OS and hotfix requirements for iSCSI, see “[Understanding feature availability](#)” on page 24.



Single host attached to a single filer through a dedicated switch

The following illustration depicts a multihomed configuration that employs a GbE switch between the filer and the host. In addition to providing good performance and segregating host-filer traffic to the dedicated switch, this arrangement minimizes disruptions in situations where network routing configuration changes frequently.

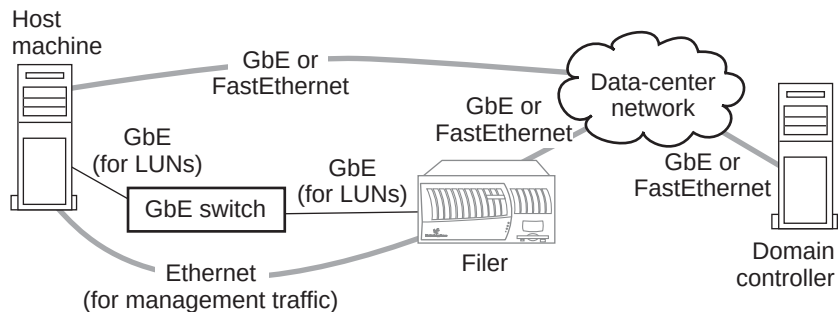
The host and filer in this configuration each use the following hardware for the connection:

- ◆ 1 GbE NIC dedicated to host-filer data transfer
- ◆ 1 Fast Ethernet (or GbE) NIC to connect to the data-center fabric

Note

LUN traffic and management traffic in an iSCSI configuration can be performed over a single GbE connection; however, NetApp recommends separating the traffic as shown in the following illustration.

Windows requirements: For Windows OS and hotfix requirements for iSCSI, see “[Understanding feature availability](#)” on page 24.



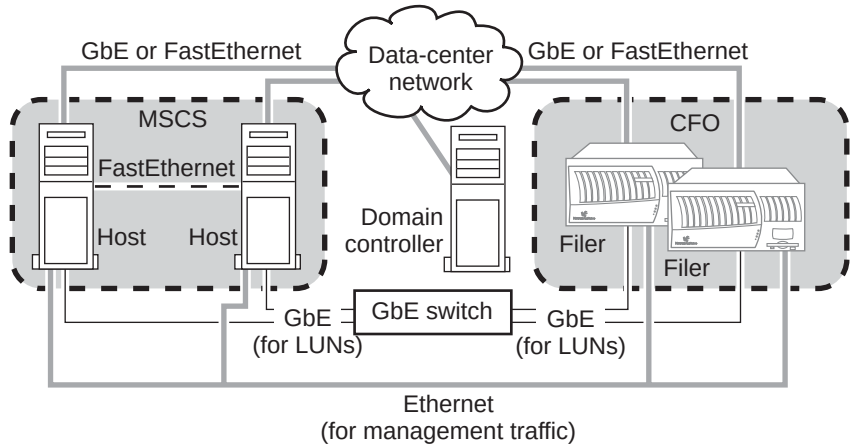
Windows cluster connected to a filer cluster through a dedicated GbE switch

The configuration in the following illustration employs both a Windows cluster and a filer cluster. The diagram also pictures an optional, but recommended “private” network that handles internal cluster traffic (rather than host-filer data traffic).

You can also create configurations that connect the host cluster to multiple filers or filer clusters, and you can connect a filer or filer cluster to multiple hosts.

Note

LUN traffic and management traffic in an iSCSI configuration can be performed over a single GbE connection; however, NetApp recommends separating the traffic as shown in the following illustration.



Windows requirements: For Windows OS and hotfix requirements for iSCSI, see “[Understanding feature availability](#)” on page 24.

FCP configurations

This section describes the supported FCP configurations. Go to any of the following topics for details.

- ◆ [“Single host direct-attached to a single filer”](#) on page 30
- ◆ [“Single host attached to a single filer through a FCP switch”](#) on page 31
- ◆ [“Windows cluster attached to a filer cluster through an FCP switch”](#) on page 31

Related topics:

- ◆ [“iSCSI configurations”](#) on page 26
- ◆ [“MPIO configurations”](#) on page 33
- ◆ [“Understanding feature availability”](#) on page 24

Single host direct-attached to a single filer

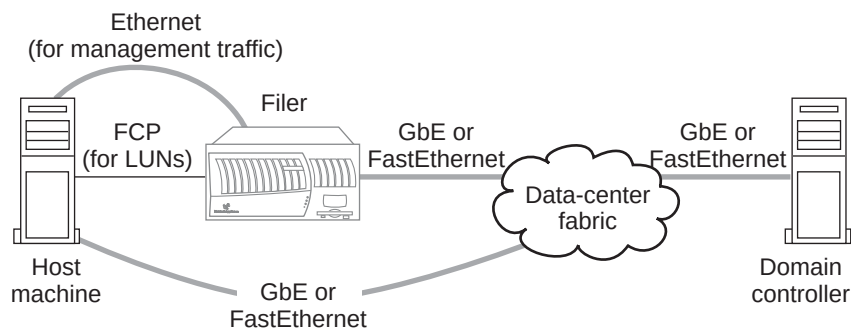
The following illustration shows a configuration that uses a crossover FCP cable to attach the host directly to the filer.

The host and filer in this configuration each use the following connection hardware:

- ◆ 1 HBA to transfer LUN data between filer and host
- ◆ 1 FastEthernet or GbE NIC to connect to the data-center fabric

Caution

For this configuration, both the filer and the host must be within the same broadcast domain.



Windows requirements: For Windows OS and hotfix requirements for FCP, see [“Understanding feature availability”](#) on page 24.

Single host attached to a single filer through a FCP switch

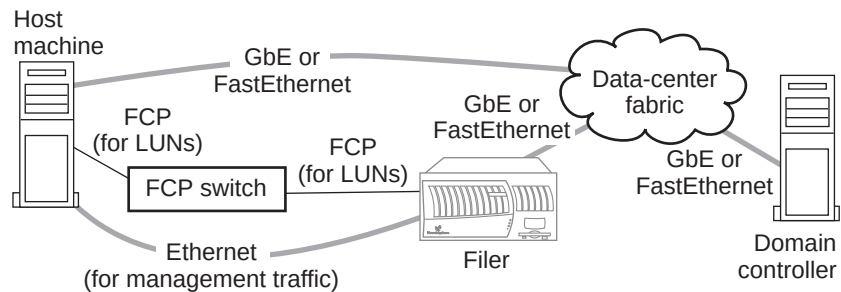
The configuration in the following illustration uses a dedicated FCP switch to handle all host-filer data traffic for LUNs.

The host and filer in this configuration each use the following hardware:

- ◆ 1 HBA to transfer LUN data between filer and host
- ◆ 1 Fast Ethernet or GbE NIC to connect to the data-center fabric

Note

LUN traffic and management traffic in an FCP configuration can be performed over a single GbE connection, however, Network Appliance recommends separating the traffic as shown in the following illustration.

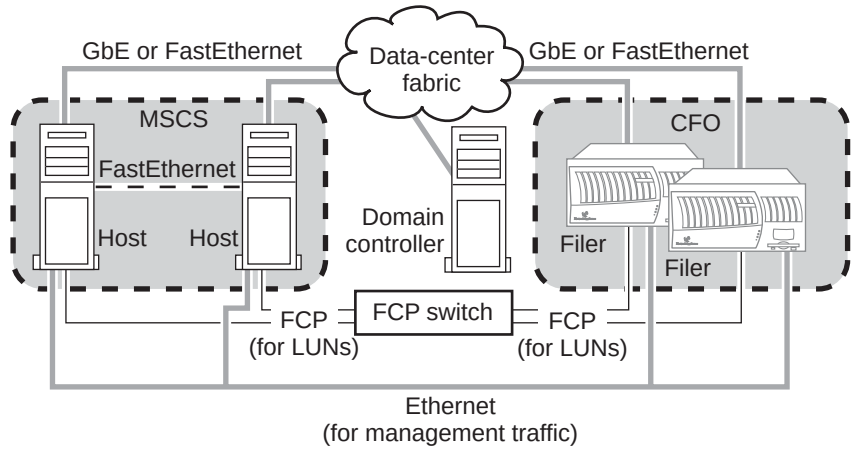


Windows requirements: For Windows OS and hotfix requirements for FCP, see [“Understanding feature availability”](#) on page 24.

Windows cluster attached to a filer cluster through an FCP switch

The following illustration depicts a configuration that employs both a Windows cluster and a filer cluster connected through an FCP switch. It also pictures an optional, but recommended dedicated network for internal cluster traffic.

You can create similar configurations that connect the Windows cluster to multiple filers or filer clusters.



Windows requirements: For Windows OS and hotfix requirements for FCP, see “[Understanding feature availability](#)” on page 24.

MPIO configurations

This section describes the supported MPIO configurations. Go to any of the following topics for more information.

- ◆ [“Single host direct-attached to single filer”](#) on page 33
- ◆ [“Windows cluster attached to filer cluster through a switch”](#) on page 34

Related topics: ◆

- ◆ [“iSCSI configurations”](#) on page 26
- ◆ [“FCP configurations”](#) on page 30
- ◆ [“Understanding feature availability”](#) on page 24
- ◆ [“MPIO setup”](#) on page 193

Single host direct-attached to single filer

FCP configuration: This configuration uses two or more FCP HBAs to support MPIO between a host and a filer. The host has at least two HBAs, and the filer has at least two FCP adapters.

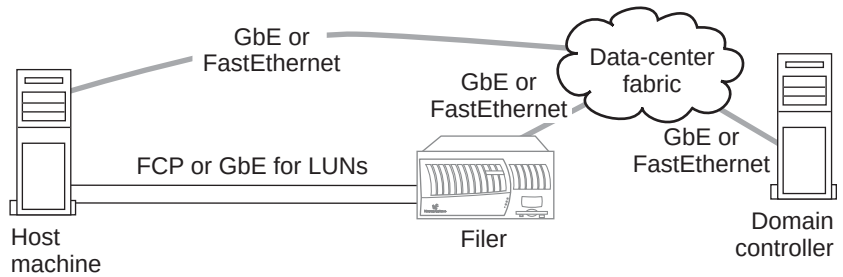
The host and filer in this configuration each use the following connection hardware:

- ◆ 2 FCP HBAs to transfer multipathed LUN data between filer and host
- ◆ Fast Ethernet (or GbE) NIC to connect to the data-center fabric

iSCSI configuration: This configuration uses iSCSI HBAs or the Microsoft iSCSI Software Initiator to support MPIO between a host and a filer. The filer has two GbE network adapters, and the host has one of the following configurations:

- ◆ Two or more iSCSI HBAs
- ◆ The Microsoft iSCSI Software Initiator and two GbE NICs

The following illustration depicts a single host direct-attached to a single filer using either FCP or iSCSI over MPIO.



Windows requirements: For Windows OS and hotfix requirements for MPIO, see “[Understanding feature availability](#)” on page 24.

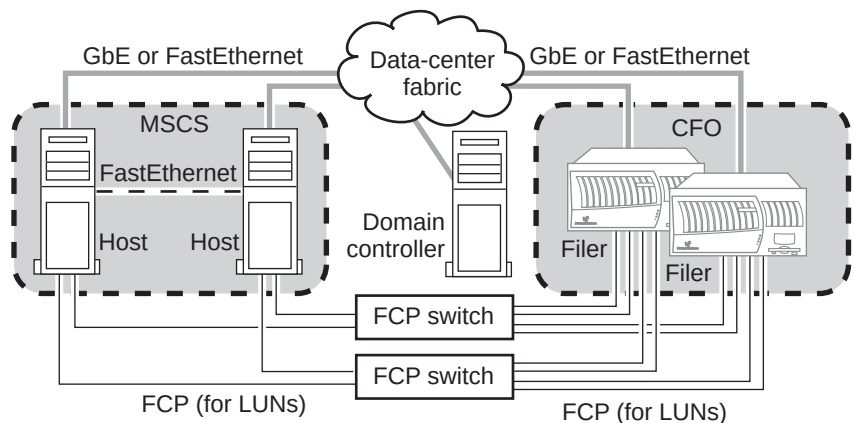
Windows cluster attached to filer cluster through a switch

FCP configuration: The configuration in the following diagram employs both a Windows cluster and a filer cluster connected through an FCP switch. The diagram also pictures an optional, but recommended dedicated network for all internal cluster traffic.

Each host in this configuration uses the following connection hardware:

- ◆ 2 HBAs to transfer multipathed LUN data between filer and host
- ◆ 1 GbE (or Fast Ethernet) NIC to connect to the data-center fabric
- ◆ 1 optional Fast Ethernet, GbE or 10/100 NIC for internal cluster traffic

Each filer in this configuration requires 2 dual-port FCP adapters and a GbE (or Fast Ethernet) NIC to connect to the data-center fabric. (See your Data ONTAP *Block Access Management Guide for FCP* for details.)

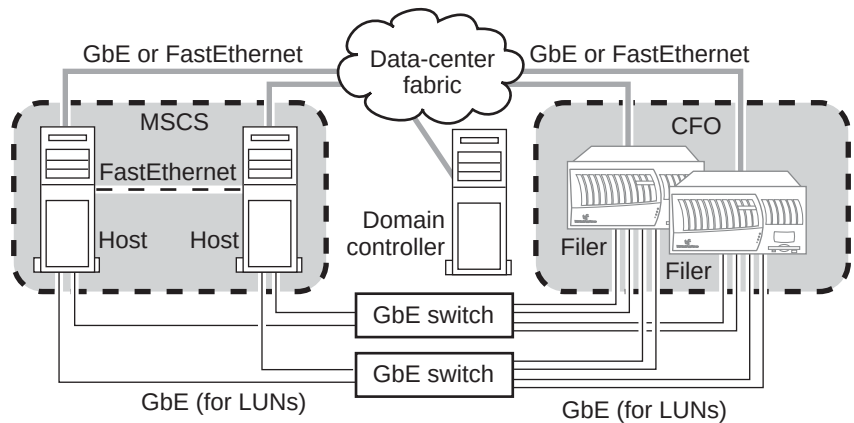


iSCSI configuration: The configuration in the following diagram employs both a Windows cluster and a filer cluster connected through a GbE switch. The diagram also pictures an optional, but recommended dedicated network for all internal cluster traffic.

Each host in this configuration uses the following connection hardware:

- ◆ Two GbE (or two iSCSI HBAs) to transfer multipathed LUN data between filer and host
- ◆ 1 GbE (or Fast Ethernet) NIC to connect to the data-center fabric
- ◆ 1 optional Fast Ethernet, GbE or 10/100 NIC for internal cluster traffic

Each filer configuration requires at least two GbE (or Fast Ethernet) NICs to connect to the data-center fabric. (See your Data ONTAP *Block Access Management Guide for iSCSI* for details.)



Windows requirements: For Windows OS and hotfix requirements for MPIO, see “[Understanding feature availability](#)” on page 24.

Preparing hosts

Before installing SnapDrive, you need to prepare your Windows hosts by performing the following tasks:

- ◆ Verify that each host meets the requirements summarized in the table that follows.
- ◆ Install on each host the proper connection hardware or software for your SnapDrive configuration.
- ◆ Install on each host the proper operating system edition, Service Pack, and hotfixes for your SnapDrive configuration.

See “[Verifying minimum requirements](#)” on page 36 for more information.

Related topics:

- ◆ “[Preparing filers](#)” on page 40
- ◆ “[Preparing the SnapDrive service account](#)” on page 54

Verifying minimum requirements

Each host in your SnapDrive configuration must meet the following requirements.

Component	Requirement
CPU	500 MHz Pentium® III or compatible
Memory	256 MB RAM
Note The requirements above are the minimums for installing SnapDrive; however, NetApp recommends a host configuration consisting of at least a Pentium III with a minimum of 512 MB RAM or a Pentium IV with at least 1 GB RAM.	

Component	Requirement
HBAs and software initiators	For FCP, see the SAN Host Attach Kit Fibre Channel Protocol on Windows at http://now.netapp.com/NOW/cgi-bin/software/. For iSCSI HBA, see the iSCSI Host Attach Kit for Windows http://now.netapp.com/NOW/cgi-bin/software/. For a list of the latest compatible software for SnapDrive 3.2, see the SnapDrive Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/. For the Microsoft iSCSI Software Initiator, see the Microsoft site at http://www.microsoft.com/downloads/.
Operating system	For Windows OS, Service Pack, and hotfix requirements, see “ Understanding feature availability ” on page 24.

To determine the exact number and type of HBAs and NICs required by each host in your SnapDrive configuration, consult “[Selecting a SnapDrive configuration](#)” on page 23.

Interface drivers: To ensure high network bandwidth and ease of configuration, make sure you have the latest firmware and drivers for the HBAs and NICs you are using.

- ◆ The NIC you use to facilitate data transfer for the Microsoft iSCSI Initiator can come from any vendor, but must have the appropriate LOGO certification: “Designed for Windows Server 2003” or “Designed for Windows 2000.”
- ◆ The latest FCP driver and firmware is available on NOW at <http://now.netapp.com/NOW/cgi-bin/software/>. From this gateway, navigate to the SAN Host Attach Kit for Fibre Channel Protocol on Windows download page.
- ◆ The Microsoft iSCSI Software Initiator must be downloaded from the Microsoft site. For directions and links, see the NOW site: <http://now.netapp.com/NOW/cgi-bin/software/>.

- ◆ The latest iSCSI driver and firmware is available on NOW <http://now.netapp.com/NOW/cgi-bin/software/>. From this gateway, navigate to the iSCSI Host Attach Kit for Windows download page.

Determining what components are installed

Before you begin installing SnapDrive or any of the required HBAs and initiators, you can check if these components are already installed to determine whether you need to perform a new installation or whether an upgrade is necessary.

Determining whether the iSCSI Software Initiator is installed: To determine whether the iSCSI Software Initiator is installed on your Windows host, complete the following steps.

Step	Action
1	Double-click Add/Remove Programs in the Windows Control Panel.
2	In the list of currently installed programs, determine whether Microsoft iSCSI Software Initiator is listed.
3	If the Microsoft iSCSI Software Initiator is not listed and you want to install it, see “ Installing the iSCSI Software Initiator ” on page 96.

Determining whether FCP or iSCSI HBA or MPIO components are installed: To determine whether FCP or iSCSI HBA or MPIO components are installed, complete the following steps.

Step	Action
1	In the left pane of the MMC, select Device Manager.
2	In the right pane of the MMC, double-click SCSI and RAID controllers.

Step	Action	
3	If...	Then...
	An FCP or iSCSI HBA is not listed and you want to install one or both	See “ Installing the FCP or iSCSI components ” on page 94 for more information.
	Multipath support is not listed	See “ Installing the new SnapDrive components ” on page 101 for more information.

Determining whether SnapDrive is installed: To determine whether SnapDrive is installed on your Windows host, complete the following steps.

Step	Action
1	Double-click Add/Remove Programs in the Windows Control Panel.
2	In the Currently installed programs list, determine whether SnapDrive is listed.
3	If SnapDrive is not listed, see Chapter 3, “ Installing or Upgrading SnapDrive ,” on page 59.

Preparing filers

Before installing SnapDrive, you must prepare the filers in your SnapDrive configuration to meet the following conditions:

- ◆ The filers are online.
- ◆ The filers are running at least Data ONTAP 6.5.4.

Note _____
VSS requires Data ONTAP 6.5 or later.

- ◆ The HBAs and NICs in your filers meet the requirements for your particular host-target SnapDrive configuration.

Note _____
For the latest SnapDrive file requirements, see the NetApp on the Web (NOW) site at <http://now.netapp.com/NOW/cgi-bin/software/>.

For detailed information about filer administration, see your Data ONTAP *Storage Management Guide*.

Go to any of the following topics for more information.

- ◆ “[Verifying minimum filer requirements](#)” on page 40
- ◆ “[Checking filer licenses](#)” on page 41
- ◆ “[Volume and filer options set by SnapDrive](#)” on page 41
- ◆ “[SnapDrive-specific limitations](#)” on page 42
- ◆ “[Cautions and recommendations](#)” on page 43
- ◆ “[Preparing a volume for SnapDrive](#)” on page 43

Related topics:

- ◆ “[Preparing hosts](#)” on page 36
- ◆ “[Preparing the SnapDrive service account](#)” on page 54

Verifying minimum filer requirements

Each filer in your SnapDrive configuration must meet the requirements in the following table.

Component	Minimum Requirement
Operating system	Data ONTAP 6.5.4

Component	Minimum Requirement
Licenses	◆ iSCSI, if you plan to use iSCSI-accessed virtual disks ◆ FCP, if you plan to use FCP-accessed virtual disks ◆ SnapRestore® license, which is required only for restoring virtual disks from snapshots ◆ SnapMirror license, if you plan to use the SnapMirror option

Note

The iSCSI and FCP licenses supplied with SnapDrive enable all the CIFS functionality necessary for using SnapDrive. If you also want *full-featured, direct CIFS access* to a particular filer, you must install a separate CIFS license on that filer.

Checking filer licenses

You can determine what licenses are enabled on your filer (and enable additional licenses) by opening FilerView in your Web browser, then navigating to Filer > Licenses > Manage. Alternatively, you can connect to the filer through a Telnet session and issue the `license` command at the filer prompt. Use the `license add code` command to enable a license at the filer command line. See your Data ONTAP documentation for details.

Starting FCP and iSCSI services

After you verify that licenses for FCP, iSCSI, or both are enabled on your filer, you must start the services by entering the `fcf start` command or the `iscsi start` command at the filer command line. See the *Block Access Management Guide for FCP* and the *Block Access Management Guide for iSCSI* for more information.

Volume and filer options set by SnapDrive

SnapDrive checks (and resets) various filer and volume options at key points:

- ◆ When you start SnapDrive
- ◆ When you create a virtual disk
- ◆ When you connect a host to a virtual disk

The following table shows the defaults reset by SnapDrive, and when those resets take place.

Caution

NetApp *strongly recommends* that you do not change these values.

Option type	Parameter	SnapDrive setting	When
Volume	Space reservation	File-based space reservation reset to On	◆ SnapDrive start ◆ Disk creation ◆ Disk connection (as long as the connected virtual disk is not a virtual disk backed by a snapshot) ◆ Snapshot creation (see Note)
Volume	create_ucose	On	◆ Disk creation ◆ Disk connection
Volume	convert_ucose	On	◆ Disk creation ◆ Disk connection
Volume	nosnapdir	Off	◆ Disk creation ◆ Disk connection
Filer	Snapshot schedule	Off	◆ Disk creation ◆ Disk connection

Note

SnapDrive checks the space-reservation setting for the target LUN at snapshot creation time. If space reservation is disabled, SnapDrive attempts to enable it; if the attempt fails, no snapshot is created.

SnapDrive-specific limitations

SnapDrive has the following limitations:

- ◆ SnapDrive supports qtrees, but you cannot manage quotas from SnapDrive.

LUNs can be created within a qtree and quota limits for that qtree will be enforced; therefore, you will not be able to create a LUN or expand an existing LUN beyond the quota limit set for that qtree.

- ◆ SnapDrive supports the use of SnapMirror to replicate volumes, but it does not support the use of SnapMirror to replicate individual qtrees.
- ◆ SnapDrive does not support the use of LUN cloning.
- ◆ A Windows host running SnapDrive can connect directly to the “hosting” filer (vfiler0) created by the optional Data ONTAP MultiStore feature, but it cannot connect to any virtual filers you create.

Cautions and recommendations

Network Appliance strongly recommends that you heed the following cautions whenever you use SnapDrive:

- ◆ Use SnapDrive to create and manage all the virtual disks on your filer.
- ◆ *Never* disable the space reservation setting for any virtual disk managed by SnapDrive.
- ◆ *Do* set the snap reserve setting on the filer to 0 percent.
- ◆ Place all virtual disks connected to the same host on a dedicated volume accessible by just that host.
- ◆ Unless you can be sure that name resolution publishes only the filer interface you intend, configure each network interface by *IP address*, rather than by name.
- ◆ If you use snapshots, you cannot use the entire space on a filer volume to store your virtual disk.

The filer volume hosting the virtual disk should be at least twice the combined size of all the virtual disks on the volume.

- ◆ Do not create any LUNs in /vol/vol0.

This volume is used by Data ONTAP to administer the filer and should not be used to contain any LUNs.

Preparing a volume for SnapDrive

You need to perform the following tasks to create a volume that can hold the SnapDrive virtual disks attached to a single host:

- ◆ Create a filer volume.
- ◆ Create a qtree (only necessary if you plan to store virtual disks at a qtree root, rather than at the dedicated volume root).
- ◆ Create a CIFS share so that your host can access the volume or qtree holding the virtual disks attached to that host.

Note

The iSCSI and FCP licenses supplied with SnapDrive enable all the CIFS functionality necessary for using SnapDrive, including CIFS share creation. If you also want *full-featured, direct CIFS access* to a particular filer, you must install a separate CIFS license on that filer.

- ◆ Reset the snap reserve option to 0 percent on the volume holding all the virtual disks attached to the host (optional, but highly recommended).

Note

You can use either the graphical user interface (GUI)-based FilerView utility or the command-line prompt on the filer (through a Telnet session, for example) to create a volume dedicated to SnapDrive virtual disks.

For more information about the following procedures, see the *Data ONTAP Block Access Management Guide for FCP* or *Block Access Management Guide for iSCSI*.

Guidelines for creating filer volumes: When you create a filer volume to hold virtual disks, keep the following in mind:

- ◆ You can create multiple virtual disks on a filer volume.
- ◆ A virtual disk must reside at either the root of a volume or the root of a qtree.

Note

Network Appliance recommends that you do not create virtual disks on the root volume.

Recommendations and requirements for configuring filer volumes:

You can optimize your filer volumes in the following ways:

- ◆ When multiple hosts share the same filer, each host should have its own dedicated volume on that filer to hold all the virtual disks connected to that host.

For more information about this recommendation, see “[Reasons for creating snapshots using SnapDrive](#)” on page 166.

- ◆ When multiple virtual disks exist on a filer volume, the dedicated volume on which the virtual disks reside must contain the virtual disks for just one host—and must *not* contain any other files or directories. Creating virtual disks on different dedicated volumes is necessary to ensure that snapshots are consistent and to avoid the possibility of busy snapshots.

Creating a filer volume

To create a volume on the filer, complete the following steps.

Step	Action
1	Using your Web browser, open a FilerView session to the filer where you are creating the volume. Example: Enter <code>http://accounting-filer2/na_admin/</code> in the Address field of your Web browser.
2	From the main FilerView menu, navigate to Volumes > Add.
3	Complete the FilerView transaction to add the volume. See the FilerView Help and the <i>Data ONTAP Storage Management Guide</i> for information about the fields.
4	Create a CIFS share to the root of the volume you created in Step 3 , making sure that no other shares exist for this volume. (See “ Creating a CIFS share ” on page 46.) Network Appliance recommends that you reset the snap reserve option for this dedicated virtual disk-storage volume to 0 percent. (See “ Resetting the snap reserve option ” on page 49.)

You can also create a filer volume by opening a Telnet session and issuing the `vol create vol_name` command at the filer prompt. See the *Data ONTAP Storage Management Guide* for details.

Creating a qtree: To create a qtree on the filer to host multiple LUNs, complete the following steps.

Note

You can create virtual disks at the root of a qtree, but virtual disks do not support the filer’s qtree *quota* capability.

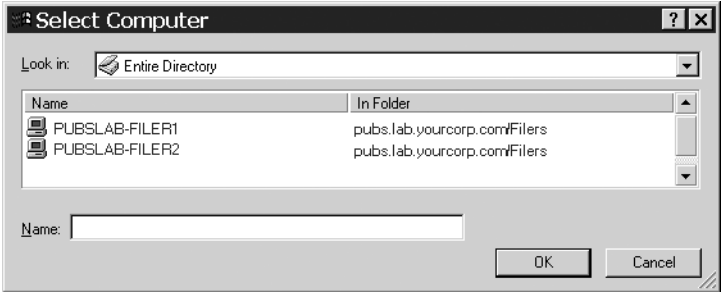
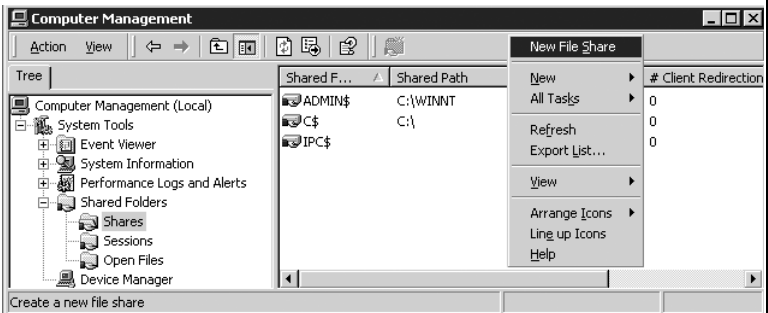
Step	Action
1	Using your Web browser, open a FilerView session to the filer where you are creating the volume. Example: Enter <code>http://accting-filer2/na_admin/</code> in the Address field of your Web browser.

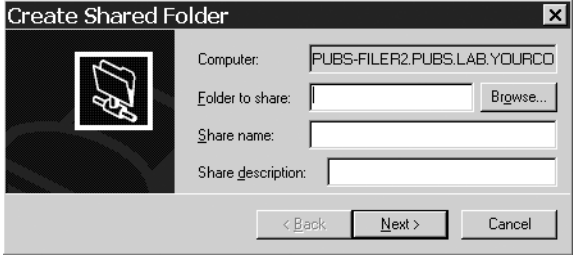
Step	Action
2	From the main FilerView menu, navigate to Volumes > Qtrees > Add.
3	Complete the FilerView transaction to add the qtree. See the FilerView Help and the <i>Data ONTAP Storage Management Guide</i> for information about the fields.

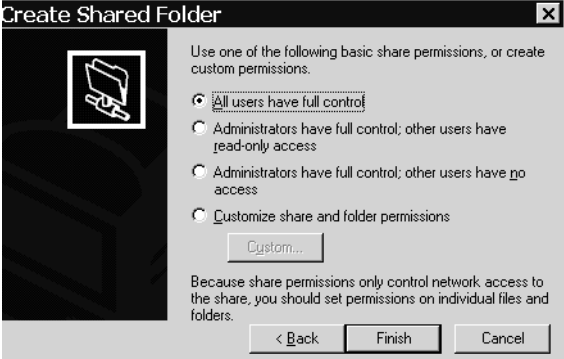
You can also create a qtree by opening a Telnet session and issuing the `qtree create path` command at the filer prompt. See the *Data ONTAP Storage Management Guide* for details.

Creating a CIFS share: To establish a CIFS share for a volume that will contain virtual disks, complete the following steps.

Step	Action
1	Make sure CIFS is enabled and configured (through the <code>cifs setup</code> command) on the filer. For SnapDrive to operate properly, the filer's CIFS (NetBIOS) name must exactly match the filer listed (UNIX host name). For more information about running CIFS setup, see your <i>Data ONTAP File Access Management Guide</i> .
2	From the Start Menu on the Windows host, select Programs > Admin Tools > Computer Management.
3	In the Computer Management window, select Action > Connect to another computer.

Step	Action
4	In the Select Computer window, select the filer you want to connect to your share. When the computer appears in the Name box, click OK. 
5	Double-click System Tools.
6	Double-click Shared Folders.
7	Click Shares.
8	Right-click the right pane of the window, then select New File Share. 

Step	Action
9	In the “Folder to share” field of the Create Shared Folder panel, type the following: <pre>c:\vol\volname\</pre> <i>volname</i> is the name of the volume. 
10	In the “Share name” field, type the name of the share. Note_____ For the “Share name” and “Share description” fields, choose easy-to-remember alphanumeric character strings that begin with a letter, a number, or the underscore character. _____
11	In the “Share description” field, type a description of the share, then click Next.

Step	Action
12	Select the appropriate permissions, then click Finish.  Note This share must have permissions set so that the Administrators Local Group has full control.

As an alternative to the preceding Windows-initiated procedure, you can use the Web-based FilerView utility to create a CIFS share for a filer volume or qtree; see the Data ONTAP *File Access Management Guide* and the FilerView Help for more information.

Resetting the snap reserve option: By default, the snap reserve option for Data ONTAP 6.5.4 and later is 20 percent. Network Appliance strongly recommends that you reset the snap reserve option to 0 percent on all volumes holding SnapDrive virtual disks. To reset the snap reserve option, complete the following steps.

Step	Action
1	Open a FilerView session to the filer holding the volume whose snap reserve setting is to be changed.
2	From the main FilerView menu, navigate to Volumes > Snapshots > Configure.
3	In the Volume field, select the volume whose snap reserve setting is to be changed

Step	Action
4	In the space reservation field, enter 0.
5	Click Apply at the bottom of the panel.

You can also reset the snap reserve option by opening a Telnet session and issuing the `snap reserve vol_name 0` command at the filer prompt. See the *Data ONTAP Storage Management Guide* for details.

Configuring pass-through authentication for SnapDrive

This section explains pass-through authentication and how to configure it. Go to the following topics for more information.

- ◆ [“Reasons for configuring pass-through authentication”](#) on page 51
- ◆ [“Configuring pass-through authentication”](#) on page 51

Reasons for configuring pass-through authentication

You can use pass-through authentication between a Windows host and a filer. You might want to use pass-through authentication for any of the following reasons:

- ◆ You do not have a domain controller available.
- ◆ You want to install your Windows host as a standalone server without any dependency on another system for authentication, even if there is a domain controller available.
- ◆ Your Windows host and the filer are in two different domains.
- ◆ Your Windows host is in a domain and you want to keep the filer on a separate private network with no direct access by user or domain controller.

Related topics:

- ◆ [“Preparing hosts”](#) on page 36
- ◆ [“Preparing filers”](#) on page 40

Configuring pass-through authentication

To configure pass-through authentication between a Windows host and a filer for SnapDrive, complete the following steps.

Note

You must have root privileges on the filer and administrator privileges on the Windows hosts to perform the following operations.

Step	Action
On the filer	
1	Enter the following command to create a user account: <pre>useradmin useradd user_name</pre> <i>user_name</i> is the name of the SnapDrive user. Note_____ You will need to provide this user name in a later step in this procedure. Therefore, make a note of the user name, including the case—lower or upper—of each character in the user name. _____
2	Enter a password when prompted to do so for the user account you are creating. You are prompted to enter the password twice. Note_____ You will need to provide the exact password in a later step in this procedure. Therefore, make a note of the password, including the case. _____
3	Check to ensure that the user account you just created belongs to the local administrator's group on the filer. For information about how to assign a user account to a specific filer group, see the section about creating local groups on the filer in the <i>Data ONTAP File Access Management Guide</i>.
4	Create a CIFS share on the filer, as described in “Creating a CIFS share” on page 46.
On each Windows host that needs access to the filer	

Step	Action
5	Create a local user account, using the same user name and password that you specified in Step 1 and Step 2. Tip: You should set up the local user account so that the password for the account never expires. For detailed instructions about how to create local user accounts, see your Windows documentation.
6	Log in to each Windows host as the local user you created in Step 5, and install SnapDrive by following the procedure described in “Installing SnapDrive for the first time” on page 93. Note_____ If you are configuring pass-through authentication for Windows hosts that are clustered, you must use a domain account to run the cluster service. All nodes of the cluster must be in the same domain; however, the filer can be in a different domain or workgroup. _____

Preparing the SnapDrive service account

Before installing SnapDrive, you must establish a SnapDrive service account. You must log in to this account whenever you need to perform SnapDrive-related functions on either a host or a filer. See [“Types of access to establish”](#) on page 54 for more information.

Related topics:

- ◆ [“Preparing hosts”](#) on page 36
- ◆ [“Preparing filers”](#) on page 40

Types of access to establish

You must establish the following types of access for the SnapDrive service account:

- ◆ You must be able to log in to the host using the service account.

Note

If at any time you change the password for this account (for example, from the Windows login panel), remember that you must make the same change to the password the SnapDrive service uses to log in. You can do this from the Start Menu: choose Settings > Control Panel > Administrative Tools > Services > SnapDrive > Log On.

- ◆ The service account must have administrator privileges on both the filer and host.
- ◆ If you do not have pass-through authentication configured, the service account must be a domain account.
- ◆ If you do not have pass-through authentication configured, the host and filer must belong to the same domain as the service account, or they must belong to domains that have direct or indirect trust relationships with the domain to which the service account belongs.
- ◆ The service account must have administrator access to the filer. It must belong to the BUILTIN\administrators group on the filer.

You can accomplish this in several ways, including connecting a Remote Administration session to the filer from the host. For instance, right-click the Local Machine icon in the Computer Management window, select Connect to Another Computer from the drop-down menu, then select the filer from the list of machines.

Next, add the service account to the Administrators group. (One way to do this is by clicking My Computer, right-clicking Manage on the drop-down

menu, then navigating to System Tools > Local Users and Groups > Groups > Administrators.)

- ◆ The host must have access to the filer volumes on which virtual disks are stored.

You enable such access by creating a share on the filer for each volume or qtree you want the host to access. This can be done only after you create the volumes or qtrees. For more information about this procedure, see “[Creating a CIFS share](#)” on page 46.

SnapDrive user interfaces

The following list covers the different interfaces you can use to execute the various SnapDrive-related commands:

- ◆ *FilerView* refers to the Web-based Data ONTAP filer management utility.
- ◆ *Filer console* refers to the command-line prompt of a console attached directly to the filer.
- ◆ *Telnet session* refers to the command-line prompt of a Telnet session connected to the filer.
- ◆ *Host console* refers to a console attached directly to the host. It displays console session 0, which receives all SnapDrive error messages and notifications. (A Terminal Service session does not receive these messages.)

Note

When you create or manage virtual disks using the host console, Remote Administration, or Terminal Service (which is an allowed, but not recommended method), you can choose between the following user interfaces:

- ❖ The GUI interface of the SnapDrive plug-in
 - ❖ `sdcli.exe` commands in the Windows command-line environment
-
- ◆ *Remote Administration* refers to a connection initiated by selecting Action > “Connect to another computer” in the Computer Management Console of a Windows computer on the same network as the SnapDrive host. This type of session enables you to manage the host as if you were using a console directly attached to the host.
 - ◆ *Terminal Service* refers to the optional Windows component that allows remote desktop administration.

Note

Do not use the Terminal Service if you can avoid it. Use the system console or a remote administration session instead.

Terminal Service sessions have the following drawbacks:

- ❖ Not all the error messages visible on the host console (session 0) are visible within a Terminal Service session.
- ❖ Virtual disks (LUNs) created through a Terminal Service session are not visible in the SnapDrive plug-in or in Windows Explorer.
- ❖ The list of available drive letters might not be up-to-date when you map a newly created virtual disk in the SnapDrive Create Disk wizard,

making it seem that you can map the virtual disk to a drive letter that is in fact already mapped.

If you encounter these problems, log off the Terminal Service session and then log on again.

Note

You must actually log off the system and log back on; just closing the terminal session is not sufficient.

The newly created or disconnected disks should now appear in their proper states.

SnapDrive user interface capabilities

Not all user interfaces are appropriate for all SnapDrive-related operations. The following table lists some of the methods appropriate for performing some common SnapDrive-related operations.

SnapDrive-related operation	Recommended interfaces
Creating a CIFS share	◆ FilerView ◆ Filer console ◆ Telnet session to the filer ◆ Remote Management session to the filer
Creating and managing volumes and qtrees	◆ FilerView ◆ Filer console ◆ Telnet session to the filer
SnapDrive-related SnapMirror operations	◆ FilerView ◆ Filer console ◆ Telnet session to the filer
Creating and managing virtual disks	◆ Host console ◆ Remote Management session to the host

The following topics explain the procedures you must follow to install or upgrade to SnapDrive 3.2, or to uninstall SnapDrive. Go to any of these topics for more information.

Use one of the following procedures, depending on what is currently installed on your system.

- ◆ If an earlier version of SnapDrive is currently installed, follow the instructions in the section “[Upgrading to SnapDrive 3.2](#)” on page 60.
- ◆ If no version of SnapDrive is installed, follow the instructions in the section “[Installing SnapDrive for the first time](#)” on page 93.

Upgrading to SnapDrive 3.2

When to use this section: Use this section if a previous version of SnapDrive is installed on your system.

Which releases you can upgrade to 3.2: You can upgrade to SnapDrive 3.2 from SnapDrive 3.1, 3.0, 2.1, or 2.0.1. If you are using an earlier release (or the VLD Manager application) you must first upgrade to 2.0.1 or 2.1, then upgrade to 3.2.

You can confirm what version of SnapDrive your system is using by selecting SnapDrive in the Microsoft Management Console (MMC), and selecting SnapDrive Info from the Action menu.

If you are using VLD-type virtual disks: VLD-type virtual disks cannot be restored using SnapDrive 3.2. If you are using VLDs, upgrade from 2.0.1 or 2.1 using the upgrade-and-conversion process described in [“Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks”](#) on page 64 or [“Upgrading a single system to SnapDrive 3.2 and converting VLD-type virtual disks”](#) on page 69. If the conversion process fails, you can reinstall a previous version of SnapDrive to restore the VLD-type virtual disk from snapshot.

Which procedure to follow: How you upgrade to SnapDrive 3.2 depends on the components of SnapDrive you are currently using and on your Windows configuration.

To upgrade...	Follow procedures under...
A single system with VLD-type virtual disks connected	“Upgrading a single system to SnapDrive 3.2 and converting VLD-type virtual disks” on page 69
A single system with only LUN-type virtual disks connected	“Upgrading a single system to SnapDrive 3.2 if you have no VLD-type virtual disks” on page 92
A Microsoft Windows server cluster with VLD-type virtual disks connected	“Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks” on page 64
A Microsoft Windows server cluster with only LUN-type virtual disks connected	“Upgrading a server cluster to SnapDrive 3.2 if you have no VLD-type virtual disks” on page 88

To upgrade...	Follow procedures under...
A single system or server cluster to SnapDrive 3.2 and Microsoft Server 2003 Edition	“Upgrading to SnapDrive 3.2 and Microsoft Windows Server 2003” on page 62

Upgrading to SnapDrive 3.2 and Microsoft Windows Server 2003

Use this section if you intend to upgrade a single Windows system or server cluster to SnapDrive 3.2 and Windows Server 2003.

Note

VLD-type virtual disks are not supported on Windows Server 2003. Upgrade VLD-type virtual disks to LUN-type disks before upgrading your Windows 2000 server to Windows Server 2003. For more information, see “[Upgrade process](#)” on page 63.

Caution

If you are running Microsoft Exchange 2000 and SnapManager for Exchange 2000, do not upgrade your Windows server or server cluster to Windows Server 2003 now. Neither Exchange 2000 nor SnapManager® for Exchange 2000 version 1.1 runs on Windows Server 2003. To view a list of compatible software for SnapDrive and SnapManager, see the SnapDrive and SnapManager Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/.

Upgrade process

To upgrade a Windows 2000 Server system or server cluster to SnapDrive 3.2 and Windows Server 2003, complete the following steps.

Note

Perform these actions in the order given.

Stage	Process
1	Upgrade to SnapDrive 3.2. Choose one of the following options. ◆ To upgrade a single system that has VLD-type virtual disks, see “Upgrading a single system to SnapDrive 3.2 and converting VLD-type virtual disks” on page 69. ◆ To upgrade a single system that has only LUN-type virtual disks, see “Upgrading a single system to SnapDrive 3.2 if you have no VLD-type virtual disks” on page 92. ◆ To upgrade a server cluster with VLD-type virtual disks connected, see “Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks” on page 64. ◆ To upgrade a server cluster with only LUN-type virtual disks connected, see “Upgrading a server cluster to SnapDrive 3.2 if you have no VLD-type virtual disks” on page 88.
2	Uninstall the VLD driver. See “Uninstalling old components” on page 107.
3	Upgrade to Windows Server 2003 Standard Edition or (for a server cluster) Windows Server 2003 Enterprise Edition. For information about this upgrade, see your Microsoft documentation.

Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks

Use this section if you are upgrading SnapDrive on a Microsoft server cluster with VLD-type virtual disks.

Upgrade and conversion process

To upgrade a server cluster with VLD-type virtual disks, complete the following steps.

Stage	Process
1	Plan and announce downtime. You will need to take offline the cluster groups that have VLD-type virtual disks as physical disk resources, thus stopping resources in that group that require the disk resource (see “Converting VLDs in a cluster group” on page 85). Note_____ Taking the cluster groups offline shuts down the applications that use them. To ensure a graceful shutdown of an application, make sure you take offline all the cluster groups that the application uses. For example, if a Microsoft Exchange installation consists of two Exchange virtual servers in two cluster groups, you will need to take both cluster groups offline. _____ You will also need to shut down the cluster nodes themselves if the cluster needs to be upgraded to the required Service Pack and hotfix level (see “Selecting a SnapDrive configuration” on page 23). Pick a time for the upgrade when loss of access will have the least effect on your users.
2	When the time you have set arrives, make sure that no users are using the system and no SnapDrive operations are running.
3	Check that the cluster is functioning properly. Make sure that the cluster groups are online and that you can do a “move group” back and forth between nodes.

Stage	Process
4	Prepare your cluster for the upgrade and VLD conversion. See “Preparing for the upgrade and VLD conversion” on page 67.
5	If necessary, upgrade Data ONTAP on the filer. If an upgrade is necessary, you will have to reboot the filer. See “Upgrading the filer” on page 100.
6	Install the components you need for FCP or iSCSI (see “Selecting a SnapDrive configuration” on page 23 for supported configurations). Choose one of the following options: ◆ If you will be creating and managing LUNs using the iSCSI Software Initiator, download and install the Microsoft iSCSI Software Initiator on both nodes. ❖ For download instructions, see Microsoft download site. ❖ For detailed installation instructions, see “Installing the iSCSI Software Initiator” on page 96. ◆ If you will be creating and managing LUNs using the iSCSI protocol and HBA, install or upgrade the iSCSI components on both nodes. See the <i>iSCSI Host Attach Kit for Windows Installation and Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/). ◆ If you will be creating and managing LUNs using the FCP protocol, install or upgrade the FCP components on both nodes. See the <i>SAN Host Attach Kit for Fibre Channel Protocol on Windows Installation and Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/). For a list of the latest compatible software for SnapDrive 3.2, see the SnapDrive Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/.

Stage	Process
7	Install SnapDrive 3.2 on both nodes, starting with the node that does not own the SnapDrive resources. See “Installing the new SnapDrive components” on page 101. The upgrade could require a reboot on both nodes, depending on whether new versions of underlying drivers need to be installed. Note If you try to use the MMC after upgrading SnapDrive on the first node and before upgrading SnapDrive on the second node, you will get an error message indicating that the SnapDrive service is unavailable owing to an invalid tag. This message occurs because two versions of SnapDrive are temporarily present on the same cluster. No corrective action is needed; just upgrade SnapDrive on the other node. Note You will see messages warning you to convert VLD-type virtual disks. This is expected behavior at this point, because you have not yet done the conversion.
8	Convert the cluster’s VLD-type virtual disks. See “ Converting VLD-type virtual disks for MSCS ” on page 82.
9	Using the information you collected earlier (see “ Preparing for the upgrade and VLD conversion ” on page 67), verify that all converted virtual disks still have the same drive letter that they had before the upgrade.
10	When all the VLD-type virtual disks are converted to LUNs, make sure that the cluster is functional by doing several “move group” operations back and forth for each cluster group.
11	Back up your application data. If you use SnapManager, use SnapManager rather than SnapDrive to create the backup.
12	When all the VLD-type virtual disks are converted to LUNs, and you are satisfied that everything is working correctly, remove the VLD driver. See “ Uninstalling old components ” on page 107.

Preparing for the upgrade and VLD conversion

To prepare for the upgrade and VLD conversion, perform the following steps.

Step	Action
1	For each VLD-type virtual disk in your installation, record the drive letter and Universal Naming Convention (UNC) path to the virtual disk object on the filer. Use the SnapDrive MMC snap-in to get this information. Recording this information helps you ensure that no drive letters are changed by the conversion, so that all scripts and applications function correctly after the conversion.
2	If you use SnapManager® software, make sure that you have an up-to-date and valid SnapManager backup, and that no SnapManager backups are scheduled to occur while you are upgrading. If backups are scheduled, cancel them.
3	If necessary, upgrade the operating systems on the cluster nodes to the required Service Pack and hotfix level. See “Preparing hosts” on page 36. If you need to apply a new Service Pack or hotfix, you will have to reboot the cluster.
4	Network Appliance strongly recommends that you create a system backup and an Emergency Repair Disk for each node before upgrading to SnapDrive 3.2.

Step	Action
5	Using your current version of SnapDrive, take a snapshot of all VLD-type virtual disks. This creates a backup that can be restored by your current version of SnapDrive, in case the upgrade fails for any reason. Note _____ Taking a snapshot of a virtual disk creates a single, consistent snapshot of all the virtual disks that share this filer volume and are connected to this Windows host. (You can check this by clicking each virtual disk in turn in the left frame of the MMC window; the same snapshot shows up for each virtual disk that shares the filer volume.)

Upgrading a single system to SnapDrive 3.2 and converting VLD-type virtual disks

Because VLD-type virtual disks are not supported on Windows Server 2003 and are no longer fully supported in SnapDrive 3.2, the upgrade to SnapDrive 3.2 includes extra steps if you are currently using VLD-type virtual disks. Network Appliance recommends that you read over the upgrade process that follows before you start the upgrade, to familiarize yourself with the requirements and upgrade steps.

Note

For more information about the VLD-to-LUN conversion, see “[VLD-to-LUN conversion](#)” on page 77.

When you are ready to start, continue with the “[SnapDrive 3.2 upgrade and conversion process](#)” on page 70.

SnapDrive 3.2 upgrade and conversion process

To upgrade to SnapDrive 3.2 when your Windows host has VLD-type virtual disks connected, complete the following steps.

Step	Action
Prepare your system for the upgrade and VLD conversion	
1	For each VLD-type virtual disk in your installation, record the drive letter and the UNC path to the virtual disk object on the filer. Use the SnapDrive MMC snap-in to get this information. Recording this information helps you ensure that no drive letters are changed by the conversion, so that all scripts and applications function correctly after the conversion.
2	Bearing in mind that you will need to stop any application(s) that access VLD-type virtual disks, pick a time for the upgrade when loss of access to the virtual disks will have the least effect on your users.
3	If you use SnapManager, make sure that you have a valid SnapManager backup, and that no SnapManager backups are scheduled to occur while you are upgrading. If backups are scheduled, cancel them.
4	Network Appliance strongly recommends that you create a system backup and an Emergency Repair Disk before upgrading to SnapDrive 3.2.

Step	Action	
5	If your applications access VLD-type virtual disks, determine the correct application-specific instructions to use to stop your applications. If the VLD-type virtual disks are accessed by more than one application, make sure you follow the instructions for all applicable applications.	
	If you have VLD-type virtual disks that store data used by...	Then...
	Microsoft Exchange	Follow the instructions in “Stopping Microsoft Exchange services for VLD conversion” on page 74.
	Microsoft SQL Server	Follow the instructions in “Stopping Microsoft SQL Server services for VLD conversion” on page 75.
	Domino	Follow the instructions in “Stopping Domino services for VLD conversion” on page 75.
	SnapManager remote verification servers	Make sure that the server will not be doing a verification during the conversion process. Check for scheduled commands and processes both on the verification server and on the production server. (Remote verification is performed as an option during backups that are scheduled and executed on the production server.)
	All other applications	Follow the instructions “Stopping all other applications for VLD conversion” on page 76.

Step	Action
6	Using your current version of SnapDrive, take a snapshot of all VLD-type virtual disks. This creates a backup that your current version of SnapDrive can restore, in case the upgrade fails for any reason. Note _____ Taking a snapshot of a virtual disk creates a single, consistent snapshot of all the virtual disks that share this filer volume and are connected to this Windows host. (You can check this by clicking each virtual disk in turn in the left frame of the MMC window; the same snapshot shows up for each virtual disk that shares the filer volume.)
7	If necessary, upgrade Data ONTAP on the filer. If an upgrade is necessary, you will have to reboot the filer. See “Upgrading the filer” on page 100.

Step	Action
8	Install the components you need for FCP or iSCSI (For supported configurations, see “Selecting a SnapDrive configuration” on page 23). Choose one of the following options: ◆ If you will be creating and managing LUNs using the iSCSI Software Initiator, download and install the Microsoft iSCSI Software Initiator on both nodes. ❖ For download instructions, see Microsoft download site. ❖ For detailed installation instructions, see “Installing the iSCSI Software Initiator” on page 96. ◆ If you will be creating and managing LUNs using the iSCSI protocol and HBA, install or upgrade the iSCSI components on both nodes. See the <i>iSCSI Host Attach Kit for Windows Installation and Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/). ◆ If you will be creating and managing LUNs using the FCP protocol, install or upgrade the FCP components. See the <i>SAN Host Attach Kit for Fibre Channel Protocol on Windows Installation and Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/). For a list of the latest compatible software for SnapDrive 3.2, see the SnapDrive Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/.
Upgrade SnapDrive and convert your VLDs	
9	Upgrade to SnapDrive 3.2. See “Installing the new SnapDrive components” on page 101. Note— You will see messages warning you to convert VLD-type virtual disks. This is expected behavior at this point, since you have not yet done the conversion.

Step	Action
10	Create a small test LUN of about 100 MB and connect to it before attempting the conversion. Repeat this step for every filer containing VLDs. Caution——— If this step is unsuccessful, and you continue with the upgrade, you will not be able to access any of your converted LUNs. Do not proceed until you have found and fixed the problem,
11	Convert your VLD-type virtual disks to LUNs. See “ VLD-to-LUN conversion ” on page 77.
Validate upgrade and return system to production	
12	Using the information you collected in Step 1 , verify that all converted virtual disks still have the same drive letter that they had before the upgrade.
13	If you do not use SnapManager, use SnapDrive to take snapshots of all virtual disks. This creates a backup that SnapDrive 3.2 can restore.
14	If you stopped any applications, restart those applications.
15	If you use Microsoft Exchange, Microsoft SQL Server, or Lotus Domino, verify that all the application databases are mounted correctly after the application is restarted.
16	If you use SnapManager, create a valid SnapManager backup.
17	When all the VLD-type virtual disks are converted to LUNs, and you are satisfied that everything is working correctly, remove the VLD driver. See “ Uninstalling old components ” on page 107.

Stopping Microsoft Exchange services for VLD conversion

If Microsoft Exchange is accessing VLD-type virtual disks, you must stop Exchange before converting the VLD-type virtual disks to LUNs. To stop Microsoft Exchange for the VLD conversion, complete the following steps.

Note

This procedure is for single systems. For instructions pertaining to MSCS clusters, see [“Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks”](#) on page 64.

Step	Action
1	Close the SnapManager application, if it is open.
2	From the Start menu, select Administrative Tools > Computer Management to display the Computer Management MMC.
3	Under Services and Applications, select Services.
4	Select the Microsoft Exchange Information Store service and select Action > Stop to stop the service.

Stopping Microsoft SQL Server services for VLD conversion

To stop Microsoft SQL Server before the VLD conversion, complete the following steps.

Note

This procedure is for single systems. For instructions pertaining to MSCS clusters, see [“Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks”](#) on page 64.

Step	Action
1	Close the SnapManager application, if it is open.
2	From the Start menu, select Administrative Tools > Computer Management to display the Computer Management MMC.
3	Under Services and Applications, select Services.
4	Select the MSSQLSERVER service and select Action > Stop to stop the service.

Stopping Domino services for VLD conversion

To stop Domino before the VLD conversion, complete the following steps.

Note

This procedure is for single systems. For instructions pertaining to MSCS clusters, see [“Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks”](#) on page 64.

Step	Action
1	Close the SnapManager application if it is open.
2	At the Domino server console, type <code>quit</code> to stop the Domino server.
3	Wait for the server to completely shut down before proceeding. For more information about stopping Domino, see “Administering the Domino System” from the Domino documentation.

Stopping all other applications for VLD conversion

To stop applications other than Exchange, SQL Server, or Domino for the VLD conversion, complete the following steps.

Note

This procedure is for single systems. For instructions pertaining to MSCS clusters, see [“Upgrading a server cluster to SnapDrive 3.2 and converting VLD-type virtual disks”](#) on page 64.

Step	Action
1	Close the SnapManager application if it is open.
2	Stop all instances of any application that is accessing the VLD-type virtual disks to be converted.

VLD-to-LUN conversion

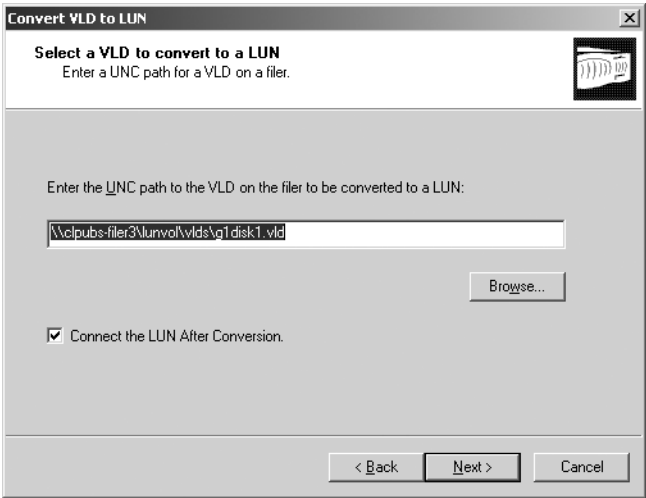
VLD-type virtual disks are not fully supported in SnapDrive 3.2. To manage the data on your VLD-type virtual disks, you must convert all VLD-type virtual disks to LUNs. SnapDrive 3.2 provides a Virtual Disk Conversion Wizard to assist you with this process. The following procedures describe how to perform the conversion.

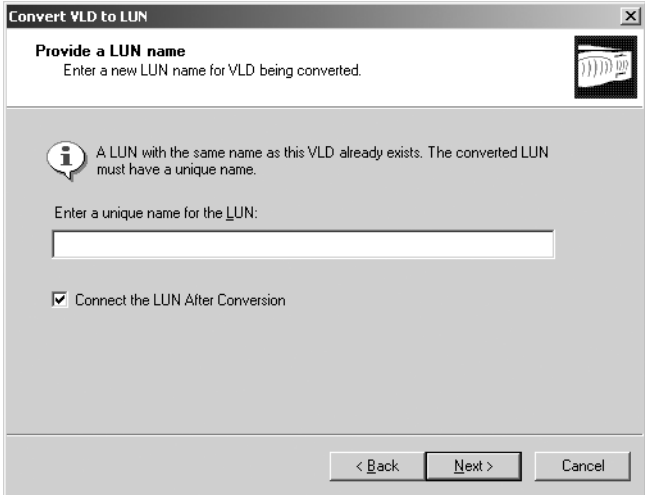
- ◆ “[Converting a connected VLD-type virtual disk](#)” on page 77
- ◆ “[Converting an unconnected VLD-type virtual disk](#)” on page 80
- ◆ “[Converting VLD-type virtual disks for MSCS](#)” on page 82
- ◆ “[Converting VLDs in a cluster group](#)” on page 85
- ◆ “[Converting a VLD-type quorum disk](#)” on page 86

Converting a connected VLD-type virtual disk

To convert a connected VLD-type virtual disk to a LUN, complete the following steps.

Step	Action
1	Make sure that your environment is prepared for the conversion and that no applications are accessing the VLD-type virtual disk to be converted. For more information, see “Upgrade and conversion process” on page 64. Note _____ The VLD-type virtual disk to be converted is disconnected during the conversion procedure. If applications are accessing the virtual disk when the disk is disconnected, the conversion fails.
2	Select Start > Programs > Administrative Tools > Computer Management to open the Computer Management window.
3	In the Computer Management window, select Storage > SnapDrive > Disks, and then select the VLD-type virtual disk you want to convert.
4	Right-click and select Convert VLD to LUN.

Step	Action
5	After the VLD-to-LUN Conversion Wizard appears, click Next. Result: The Select a VLD to Convert to a LUN panel is displayed, with the UNC path to the VLD-type virtual disk you selected already filled in. The converted LUN will have the same name as the VLD-type virtual disk you are converting. Example: \\clpubs-filer3\lunvol\vlds\g1disk1.vld becomes a LUN named g1disk1.lun. 
6	To automatically reconnect the LUN after it is converted, leave the Connect the LUN After Conversion check box selected (NetApp recommends leaving this check box selected). Click Next.

Step	Action						
7	If a LUN-type virtual disk exists with the same name as the VLD-type virtual disk you are converting, a panel is displayed prompting you to specify a different name for the converted disk. 						
8	If you did not leave the Connect the LUN After Conversion check box selected, skip to Step 14.						
9	In the Select a Virtual Disk Type panel, verify that the preselected virtual disk type is correct for your configuration. <table><tr><th>If...</th><th>Then...</th></tr><tr><td>The VLD-type virtual disk being converted will be connected to a single-host system</td><td>Select Dedicated, click Next, and then skip to Step 11.</td></tr><tr><td>The VLD-type virtual disk being converted is an MSCS cluster resource</td><td>Select Shared, and click Next.</td></tr></table>	If...	Then...	The VLD-type virtual disk being converted will be connected to a single-host system	Select Dedicated, click Next, and then skip to Step 11 .	The VLD-type virtual disk being converted is an MSCS cluster resource	Select Shared, and click Next.
If...	Then...						
The VLD-type virtual disk being converted will be connected to a single-host system	Select Dedicated, click Next, and then skip to Step 11 .						
The VLD-type virtual disk being converted is an MSCS cluster resource	Select Shared, and click Next.						
10	In the Information about Microsoft Cluster Services System panel, verify that you want the disk to be shared by the nodes listed, and then click Next.						

Step	Action
11	In the Select Virtual Disk Drive Letter panel, make sure that the drive letter for the converted LUN is the same as the drive letter previously used by the VLD-type virtual disk being converted, and then click Next.
12	Select the desired initiator, click the right arrow, and then click Next. Note_____ If you are using MSCS or MPIO, you must select an initiator for each path to the filer.
13	If you are connecting the converted LUN to an MSCS cluster, the Specify Microsoft Cluster Services Group screen is displayed. Verify that the disk will be connected to the correct cluster group. If you want to create a new cluster group and add the converted LUN to the new group, select Create a New Cluster Group. However, that results in a different cluster configuration than you had before the conversion.
14	In the Completing the VLD-to-LUN Conversion Wizard panel, check the settings you selected for your new LUN, and then click Finish to start the conversion.

Converting an unconnected VLD-type virtual disk

To convert an unconnected VLD-type virtual disk to a LUN, complete the following steps.

Step	Action
1	Make sure that your environment is prepared for the conversion.
2	Select Start > Programs > Administrative Tools > Computer Management to open the Computer Management window.
3	In the Computer Management window, select Storage > SnapDrive > Disks.
4	Right-click and select Convert VLD to LUN.

Step	Action						
5	After the VLD-to-LUN Conversion Wizard appears, click Next. Result: The Select a VLD to Convert to a LUN panel is displayed.						
6	Enter the UNC path or browse to the VLD-type virtual disk you want to convert. The converted LUN will have the same name as the VLD-type virtual disk you are converting. Example: \\clpubs-filer3\\lunvol\\vlds\\g1disk1.vld becomes a LUN named g1disk1.lun.						
7	To automatically connect the LUN after it is converted, select the Connect the LUN After Conversion check box. Click Next.						
8	If a LUN-type virtual disk exists with the same name as the VLD-type virtual disk you are converting, you are prompted to specify a different name for the converted disk.						
9	If you did not select the Connect the LUN After Conversion check box, skip to Step 15 .						
10	In the Select a Virtual Disk Type panel, verify that the preselected virtual disk type is correct for your configuration.						
	<table><tr><th>If...</th><th>Then...</th></tr><tr><td>The VLD-type virtual disk being converted will be connected to a single-host system</td><td>Select Dedicated, click Next, and then skip to Step 12.</td></tr><tr><td>The VLD-type virtual disk being converted is an MSCS cluster resource</td><td>Select Shared, and click Next.</td></tr></table>	If...	Then...	The VLD-type virtual disk being converted will be connected to a single-host system	Select Dedicated, click Next, and then skip to Step 12 .	The VLD-type virtual disk being converted is an MSCS cluster resource	Select Shared, and click Next.
	If...	Then...					
	The VLD-type virtual disk being converted will be connected to a single-host system	Select Dedicated, click Next, and then skip to Step 12 .					
The VLD-type virtual disk being converted is an MSCS cluster resource	Select Shared, and click Next.						
11	In the Information about Microsoft Cluster Services System panel, verify that you want the disk to be shared by the nodes listed, and then click Next.						
12	In the Select Virtual Disk Drive Letter panel, select the same drive letter for the converted LUN as the drive letter previously used by the VLD-type virtual disk being converted, and then click Next.						

Step	Action
13	Select the desired initiator, click the right arrow, and then click Next. Note_____ If you are using MSCS or MPIO, you must select an initiator for each path to the filer.
14	If you are connecting the converted LUN to an MSCS cluster, the Specify Microsoft Cluster Services Group screen is displayed. Select the cluster group that you want the newly converted LUN to be connected to. If you want to create a new cluster group and add the converted LUN to the new group, select Create a New Cluster Group.
15	In the Completing the VLD-to-LUN Conversion Wizard panel, check the settings you selected for your new LUN, and then click Finish to start the conversion.

Converting VLD-type virtual disks for MSCS

To convert all VLD-type virtual disks to LUN-type virtual disks in an MSCS configuration, complete the following steps.

Note_____

The following procedure assumes extensive knowledge of MSCS administration.

Step	Action
Prepare the cluster for conversion	
1	Determine the order in which you will convert your cluster groups. Each group should be completely converted before you move on to the next group. The main cluster group (the group that contains the quorum disk) should be converted last.

Step	Action
2	Create a new shared LUN for temporary use during the conversion. The size of this LUN should be at least 200 MB. Place the temporary LUN in the first cluster group to be converted. This temporary LUN will be used to shift resource dependencies and will function as a quorum disk while the current quorum disk is being converted. For more information, see “Creating a virtual disk” on page 123.
3	If you have only one cluster group, skip to Step 6 .
Convert cluster groups that do not contain the quorum disk	
4	For each cluster group that does not contain the quorum disk, if the group contains VLD-type virtual disks, perform the following steps: - Open Cluster Administrator on the node that owns the cluster group. - Right-click the cluster group and select Take Offline. - Right-click each physical disk resource in the cluster group and select Bring Online. - Using SnapDrive, create a snapshot of every VLD-type virtual disk in the cluster group. Name the snapshots using the name of the cluster group and the drive letter. For more information on creating snapshots, see “Creating snapshots” on page 166. - Right-click the cluster group and select Take Offline again to bring all of the disks back offline. - Convert each VLD-type virtual disk in the cluster group. See “Converting VLDs in a cluster group” on page 85.
Convert the main cluster group	
5	Open Cluster Administrator on the node that owns the main cluster group.

Step	Action
6	If your quorum disk is a VLD-type virtual disk, convert it to a LUN. See “Converting a VLD-type quorum disk” on page 86.
7	Using SnapDrive, create a snapshot of every VLD-type virtual disk in the main cluster group. Name the snapshots using the name of the main cluster group and the drive letter. For more information on creating snapshots, see “Creating snapshots” on page 166.
8	For each remaining VLD-type virtual disk in the main cluster group, right-click the resource in Cluster Administrator and select Take Offline.
9	Convert any remaining VLD-type virtual disks in the main cluster group. See “Converting VLDs in a cluster group” on page 85.
Delete the temporary LUN	
10	On the node that currently owns the cluster group containing the temporary LUN, open the Computer Management window and select SnapDrive > Disks.
11	Select the temporary LUN, right-click, and select Delete Disk to delete the temporary LUN. Note _____After deleting the temporary LUN, you may see an Unsafe Removal of Device notification on the other node. This is not a problem; click OK to dismiss the dialog box.

Converting VLDs in a cluster group

To convert all VLD-type virtual disks in a cluster group, complete the following steps.

Step	Action
1	For each resource in this cluster group, record all dependencies and remove any dependencies on VLD-type virtual disks. - Right-click the resource and select Properties. - Select the Dependencies tab. - Record all dependencies for the resource. - If the resource has a dependency on any VLD-type virtual disk, remove the dependency. - If you cannot remove the last dependency, move the dependency to the temporary LUN. Some services, for example Microsoft Exchange System Attendant, do not allow all physical disk dependencies to be removed.
2	After all dependencies on the VLD-type virtual disks are removed, convert every VLD-type virtual disk in this cluster group to a LUN-type virtual disk. For more information, see “Converting a connected VLD-type virtual disk” on page 77.
3	Using Cluster Administrator, reestablish the original dependencies on the newly converted LUNs, and remove any dependencies you placed on the temporary LUN.
4	Drag and drop the temporary LUN into the next cluster group to be converted.
5	Right-click the cluster group that you just converted and select Bring Online.

Step	Action
6	Verify the status of your cluster by performing a “move group” operation back and forth. - Right-click the cluster group that contains the quorum and select Move Group. - After the cluster group comes back online after the move group, repeat the move group operation to return the cluster group to its original owning node.
7	After all dependencies on the VLD-type virtual disks are removed, convert every VLD-type virtual disk in this cluster group to a LUN-type virtual disk. For more information, see “Converting a connected VLD-type virtual disk” on page 77.

Converting a VLD-type quorum disk

To convert a VLD-type virtual disk that is being used as a quorum disk, perform the following steps.

For more information, see Microsoft Knowledge Base Article 280353, “How to Change the Quorum Disk Designation.”

Step	Action
1	In Cluster Administrator, right-click the top-level cluster name and select Properties.
2	In the Properties dialog box, select the Quorum tab.
3	Select the temporary LUN from the list of available drives, and then click OK. Result: The temporary LUN is now the quorum disk.
4	Convert the original (VLD-type virtual disk) quorum disk to a LUN-type virtual disk. See “Converting a connected VLD-type virtual disk” on page 77.

Step	Action
5	Reopen the Properties dialog box for the cluster. This time, select the newly converted LUN to be the quorum disk. Result: The quorum disk has the same drive letter as before, but now it is a LUN-type virtual disk.
6	Verify the status of your cluster by performing a “move group” operation back and forth. a. Right-click the cluster group that contains the quorum and select Move Group. b. After the cluster group comes back online, repeat the move group operation to return the cluster group to its original owning node.

Upgrading a server cluster to SnapDrive 3.2 if you have no VLD-type virtual disks

Use this section only if your Microsoft server cluster is currently running an earlier version of SnapDrive and you are not using VLD-type virtual disks. If this is the case, continue with the “[Upgrade process](#)” on page 88.

Upgrade process

Follow this process to upgrade a server cluster that has no VLD-type virtual disks.

Stage	Process
1	Plan and announce downtime. You will need to shut down the cluster nodes if the cluster needs to be upgraded to the Service Pack and hotfix level required by SnapDrive 3.2 (see “Selecting a SnapDrive configuration” on page 23). Pick a time for the upgrade when loss of access will have the least effect on your users.
2	When the time you have set arrives, make sure no users are using the system and no SnapDrive operations are running.
3	Check that the cluster is functioning properly. Make sure that the Cluster Groups are online and that you can perform a “move group” operation back and forth between nodes.
4	Prepare your cluster for the upgrade. See “Preparing for the upgrade” on page 90.
5	If necessary, upgrade Data ONTAP on the filer. If an upgrade is necessary, you will have to reboot filer. See “Upgrading the filer” on page 100.
6	Stop the SnapDrive service and ensure the MMC is closed.

Stage	Process
7	Install the components you need for FCP or iSCSI (see “Selecting a SnapDrive configuration” on page 23 for supported configurations). Choose one of the following options. ◆ If you will be creating and managing LUNs using the iSCSI Software Initiator, download and install the Microsoft iSCSI Software Initiator on both nodes. ❖ For download instructions, see Microsoft download site. ❖ For detailed installation instructions, see “Installing the iSCSI Software Initiator” on page 96. ◆ If you will be creating and managing LUNs using the iSCSI protocol and HBA, install or upgrade the iSCSI components on both nodes. See the <i>iSCSI Host Attach Kit for Windows Installation and Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/). ◆ If you will be creating and managing LUNs using the FCP protocol, install or upgrade the FCP components on both nodes. See the <i>SAN Host Attach Kit for Fibre Channel Protocol on Windows Installation and Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/). For a list of the latest compatible software for SnapDrive 3.2, see the SnapDrive Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/.

Stage	Process
8	Install SnapDrive 3.2 on both nodes, starting with the node that does not own the SnapDrive resources. See “Installing the new SnapDrive components” on page 101. The upgrade could require a reboot on both nodes, depending on whether new versions of underlying drivers need to be installed. Note_____ If you try to use the MMC after upgrading SnapDrive on the first node and before upgrading SnapDrive on the second node, you will get an error message indicating that the SnapDrive service is unavailable due to an invalid tag. This message occurs because two versions of SnapDrive are temporarily present on the same cluster. No corrective action is needed; just upgrade SnapDrive on the other node.
9	Uninstall the VLD driver if necessary. (It could be on your system even if you have not used it recently.) See “Uninstalling old components” on page 107.
10	Back up your application data. If you use SnapManager, use SnapManager rather than SnapDrive to create the backup.

Preparing for the upgrade

To prepare for the upgrade, complete the following steps.

Step	Action
1	If you use SnapManager, make sure that you have a valid and up-to-date SnapManager backup, and that no SnapManager backups are scheduled to occur while you are upgrading. If there are backups scheduled, cancel them.

Step	Action
2	If necessary, upgrade the operating systems on the cluster nodes to the required Service Pack and hotfix level. See “Preparing hosts” on page 36. If you need to apply a new Service Pack or hotfix, you will have to reboot the cluster.
3	Network Appliance strongly recommends that you create a full backup, including system state, and create an Emergency Repair Disk for each node before upgrading to SnapDrive 3.2.

Upgrading a single system to SnapDrive 3.2 if you have no VLD-type virtual disks

Use this section only if you are currently running an earlier version of SnapDrive and you are not using VLD-type virtual disks. If this is the case, continue with the [“Upgrade process”](#) on page 92.

Upgrade process

To upgrade a system without VLD-type virtual disks to SnapDrive 3.2, you need to do the following.

Stage	Process
1	Install the required version of the iSCSI Software Initiator, iSCSI HBA driver, or FCP driver. See “Installing the FCP or iSCSI components” on page 94.
2	Network Appliance strongly recommends that you create a full backup, including system state, and create an Emergency Repair Disk before upgrading to SnapDrive 3.2.
3	If necessary, upgrade Data ONTAP on the filer. If an upgrade is necessary, you will have to reboot the filer. See “Upgrading the filer” on page 100.
4	Install SnapDrive 3.2. See “Installing the new SnapDrive components” on page 101.
5	Uninstall the VLD driver if necessary. (It could be on your system even if you have not used it recently.) See “Uninstalling old components” on page 107.

Installing SnapDrive for the first time

Use this section to install SnapDrive 3.2 if no previous version of SnapDrive or VLD Manager is installed on your system. In this case, continue with the [“Installation process”](#) on page 93.

Installation process To install SnapDrive 3.2, you need to do the following in the order given.

Stage	Process
6	If necessary, upgrade Data ONTAP on your filer.
7	Install the required version of the iSCSI Software Initiator, iSCSI HBA, or FCP components. See “Installing the FCP or iSCSI components” on page 94.
8	Install SnapDrive 3.2. See “Installing the new SnapDrive components” on page 101. In a server cluster, install SnapDrive on all nodes.

Installing the FCP or iSCSI components

Supported protocols: SnapDrive 3.2 supports two protocols for creating and managing virtual disks (LUNs): iSCSI and FCP.

Note

Both FCP and iSCSI protocols are supported on the same host, however, FCP and iSCSI connections from the same host to the same LUN are not supported.

What you need to do: Before you install SnapDrive 3.2, you need to do one of the following:

If...	Then...
You will be using the iSCSI protocol and software initiator to create and manage LUNs	Install the Microsoft iSCSI Software Initiator. See “ Installing the iSCSI Software Initiator ” on page 96.
You are currently using the iSCSI protocol and hardware initiator to create and manage LUNs, and will continue to use it	Upgrade the iSCSI driver and firmware. For a list of supported iSCSI initiators, see the iSCSI Solutions Support Matrix on the NOW site at http://now.netapp.com/NOW/knowledge/docs/san/fcp_iscsi_config/iscsi_support_matrix.shtml/ .

If...	Then...
You will be using the iSCSI protocol and hardware initiator to create and manage LUNs, and have not previously used it	Install the iSCSI Host Bus Adapter, driver, and firmware. For a list of supported iSCSI initiators, see the iSCSI Solutions Support Matrix on the NOW site at http://now.netapp.com/NOW/knowledge/docs/san/fcp_iscsi_config/iscsi_support_matrix.shtml/. Note If you are using the QLogic 4010/4010C iSCSI HBA, you must also install the Microsoft iSCSI Initiator Service. You can install this service from the Microsoft iSCSI Initiator installation package. See “Installing the iSCSI Software Initiator” on page 96.
You are currently using the FCP protocol to create and manage LUNs, and will continue to use it	Upgrade the FCP driver and firmware. See the <i>SAN Host Attach Kit for Fibre Channel Protocol on Windows Installation and Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/). Note The FCP upgrade stops the SnapDrive service. SnapDrive restarts when the system is rebooted. If you proceed without a reboot, restart the SnapDrive service manually.

If...	Then...
You will be using the FCP protocol to create and manage LUNs, and have not previously used it	Install the FCP Host Bus Adapter, driver, and firmware. See the <i>SAN Host Attach Kit for Fibre Channel Protocol on Windows Installation and Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/).
For a list of the latest compatible software for SnapDrive 3.2, see the SnapDrive Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/.	

Installing the iSCSI Software Initiator

To install the Microsoft iSCSI Software Initiator, complete the following steps.

Step	Action
1	Download the Microsoft iSCSI Software Initiator from the Microsoft site.
2	Click the Microsoft iSCSI Initiator Installer Package icon.

Step	Action
3	In the iSCSI Installation Options screen: If you are going to be using the iSCSI Initiator to create and manage LUNs, make sure that the check boxes are selected for the Initiator Service and the Software Initiator. If you are going to be using the QLogic 4010/4010C HBA, clear the check box for the iSCSI Software Initiator; you need only the Initiator Service. Note_____ Installation of the Microsoft MPIO Multipathing Support for iSCSI is not required because the same MPIO version will be installed with SnapDrive 3.2 if you choose to license and install the SnapDrive MPIO feature. _____ Note_____ The Virtual Port Driver option is grayed out and will always be installed during the Microsoft iSCSI Initiator installation and upgrade. _____
4	Follow the directions in the installer wizard to install the Microsoft iSCSI Initiator.

Upgrading the iSCSI Software Initiator

Upgrading a single, non-clustered Windows host: To upgrade the Microsoft iSCSI Software Initiator on a stand-alone Windows host, complete the following steps.

Step	Action
1	Stop the SnapDrive service. See “ Stopping and starting the SnapDrive service ” on page 105.

Step	Action
2	If you are running SnapManager for Exchange, stop the application-specific services, (for example, Microsoft Exchange System Attendant) which have iSCSI dependencies. Note— You can also remove iSCSI dependencies using SnapManager for Exchange Configuration Wizard, however, this option is not recommended and should only be used if you are unable to stop the application-specific services.
3	Install the new iSCSI software initiator. For more information, see “Installing the iSCSI Software Initiator” on page 96.
4	From the MMC, open SnapDrive. Note— Opening the SnapDrive snap-in restarts the SnapDrive service.

Upgrading the iSCSI Software Initiator on clustered Windows

hosts: To upgrade the Microsoft iSCSI Software Initiator on a two-node Windows cluster, complete the following steps.

Step	Action
1	If you are running SnapManager for Exchange, stop the application-specific services, (for example, Microsoft Exchange System Attendant) which have iSCSI dependencies. Note— You can also remove iSCSI dependencies using SnapManager for Exchange Configuration Wizard, however, this option is not recommended and should only be used if you are unable to stop the application-specific services.
2	Close the MMC.
3	Install the new iSCSI software package. For more information, see “Installing the iSCSI Software Initiator” on page 96.

4	From the MMC, open SnapDrive. Note _____ Opening the SnapDrive snap-in restarts the SnapDrive service. _____
5	Perform a Move Group to the node you just upgraded (node 2). Result: Node 2 now owns the cluster resources.
6	From node 1, repeat Step 1 through Step 4, then perform a Move Group to return ownership of the cluster to node 1.
7	To upgrade the iSCSI Software Initiator in a multi-node Windows cluster, perform Step 1 through Step 4 on each non-owning node.

Upgrading the filer

Note

If a filer upgrade is necessary, upgrade the filer before installing SnapDrive. For more information, see “[Preparing filers](#)” on page 40.

SnapDrive 3.2 requires at least Data ONTAP 6.5.4 on the filer. For a list of the latest compatible software for SnapDrive 3.2, see the SnapDrive Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/. To upgrade the filer, complete the following steps.

Step	Action
1	Upgrade the filer to at least Data ONTAP 6.5.4. See the Data ONTAP <i>Upgrade Guide</i> for details.
2	When the filer upgrade is complete, install SnapDrive on your Windows system. In a server cluster, install SnapDrive on each node in the cluster.

Installing the new SnapDrive components

To install the new SnapDrive components, complete the following steps.

Note
In a cluster, install SnapDrive 3.2 on all nodes, one at a time. If you are upgrading SnapDrive in a cluster, start with the node that does not own the SnapDrive resources.

Note
If you are upgrading or installing SnapDrive to support a SnapManager installation, see “[Stopping and starting the SnapDrive service](#)” on page 105.

Caution
Perform this procedure from the system console, and not from a Terminal Service client.

Step	Action
1	Make sure that you have installed the required FCP or iSCSI components. See “Installing the FCP or iSCSI components” on page 94. Note If you will be using the iSCSI initiator, you may see a message after the SnapDrive installation has completed stating that SnapDrive will modify the <code>MaxRequestHoldTime</code> parameter. This setting modifies the timeout value to ensure proper cluster failover operation. NetApp recommends rebooting your system after installing all your SnapDrive components.
2	Stop the SnapDrive service, if necessary, and close the Microsoft Management Console (MMC) window. See “Stopping and starting the SnapDrive service” on page 105.
3	Browse to the location of the SnapDrive installation package and double-click <code>SnapDrive3.2.exe</code>.
4	Click Next on the “Welcome to the InstallShield Wizard for SnapDrive” screen.

Step	Action	
5	If this is a new SnapDrive installation, accept the license agreement and click Next.	
6	If you are upgrading SnapDrive, the Program Maintenance panel appears. Click Modify/Upgrade, and then click Next.	
7	On the SnapDrive Modules to Install panel, select the modules you want to install. You can select either MPIO Path Management, LUN Provisioning and Snapshot Management, or both, depending on your needs. Then click Next. If you are upgrading SnapDrive, the license information will be displayed for the modules you previously installed and licensed.	
8	If...	Then...
	The Installed Version shown on the SnapDrive Driver Installation screen is the same as, or later than, the Minimum Required Version for the type of virtual disk protocol you will be using (FCP or iSCSI)	Click Next and proceed to the next step.
	The Installed Version is earlier than the Minimum Required Version	Update the driver (see “Installing the FCP or iSCSI components” on page 94), and then restart the SnapDrive InstallShield Wizard.
9	If...	Then...
	The Driver Installed shown on the MPIO Driver Installation screen is not installed or is earlier than the minimum required version	Click Next to install the current driver and proceed to the next step.

Step	Action	
10	If...	Then...
	You are upgrading from SnapDrive 2.0.1 or later	Skip to Step 14 .
	This is a new SnapDrive installation	Continue with the next step.
11	In the Customer Information panel, type your user name and organization name, and then click Next.	
12	The Destination Folder panel prompts you for a directory in which to install SnapDrive on the host. By default, this is C:\Program Files\SnapDrive. To accept the default, click Next, and then proceed to Step 13. To specify a different location, click the Change button. In the Change Current Destination Folder panel, either type the path to the target directory in the Folder Name text box, or navigate to the folder you prefer and select it. When the correct target location appears in the Folder Name text box, click OK to return to the Destination Folder panel, and then click Next.	
13	On the SnapDrive Service Credentials screen, click Add and select Administrator from the drop-down list. Type the account password in both the Password and Confirm Password text boxes, then click Next.	

Step	Action
14	On the “Ready to” panel, click Install. Result: The Installing SnapDrive screen appears, informing you that installation might take several minutes to complete. Note_____ If you are upgrading from an earlier version of SnapDrive and you have VLD-type virtual disks, a message warns you to convert the VLDs to LUNs. See “VLD-to-LUN conversion” on page 77. _____ Note_____ If you are running SnapDrive 3.0 and you previously installed NetApp VSS Hardware Provider 1.0, a message informs you that the previous installation will be removed from your system. During the SnapDrive 3.2 installation, an updated NetApp VSS hardware provider will be installed. _____
15	When the InstallShield Wizard Complete screen appears, click Finish.
16	If you are installing or upgrading the MPIO drivers, the SnapDrive Installer Information pop-up screen appears. Click Yes to reboot the machine.
17	When the reboot process is complete, SnapDrive is successfully installed on your host. Note_____ If you are upgrading a server cluster and you try to use the MMC after upgrading SnapDrive on the first node and before upgrading SnapDrive on the second node, you get an error message indicating that the SnapDrive service is unavailable owing to an invalid tag. This message is the result of the temporary presence of two versions of SnapDrive on the same cluster. No corrective action is needed; just upgrade SnapDrive on the other node. _____
18	If you will be creating and managing LUNs using the iSCSI protocol, establish an iSCSI connection to the filer. See “Establishing an iSCSI session to a target” on page 113.

Setting a preferred IP address for filer hostname resolution

You can configure SnapDrive to use a preferred IP address for filers having more than one IP address. Setting a preferred IP address enables SnapDrive to properly resolve filer host names.

To set the preferred IP address for a filer in SnapDrive, complete the following steps.

Step	Action
1	Perform the following actions: a. Expand the Storage option in the left panel of the MMC, if it is not already expanded. b. Double-click SnapDrive, then select Disks. c. Right-click Disks and select Properties from the menu.
2	In the Disks Properties window, select the Preferred Filer IP Addresses tab.
3	Enter the filer name and preferred IP address for that filer in the spaces provided.
4	Click Apply.
5	Repeat Step 3 and Step 4 for each filer for which you want to set a preferred IP address.
6	Click OK.

Stopping and starting the SnapDrive service

When you upgrade SnapDrive or add new SnapDrive components, it is sometimes necessary to stop or restart the SnapDrive service.

To stop or start the SnapDrive service, complete the following steps.

Step	Action
1	In the left MMC pane, expand the Services and Applications option and select Services.
2	In the right MMC pane, scroll down the list of service and locate the SnapDrive service.

Step	Action
3	Double-click SnapDrive. Result: The SnapDrive Properties window is displayed.
4	Under Service status, click Stop or Start, then click OK to exit the SnapDrive Properties window.

Installing SnapDrive on SnapManager verification servers

If you are upgrading or installing SnapDrive to support a SnapManager installation, and you use verification servers, remember to install SnapDrive 3.2 on the verification servers as well as on the production systems. Both the verification server and the production servers must be using the same version of SnapDrive.

If a verification server will be connecting to LUNs over an iSCSI session, make sure you also install the Microsoft iSCSI Software Initiator on the verification server (see “[Installing the iSCSI Software Initiator](#)” on page 96) and establish a session from the verification server to the iSCSI target on the filer where the database to be verified resides. This connection enables the verification server to connect to the snapshot LUN that contains the database, and you must create it explicitly before the verification server attempts to connect to the LUN.

For instructions for establishing an iSCSI session, see “[Establishing an iSCSI session to a target](#)” on page 113.

Note

For this purpose, create only an iSCSI session; do not use the Create Disk wizard, which would create a new LUN as well.

Uninstalling old components

Go to any of the following topics for more information.

- ◆ “[Uninstalling the VLD driver](#)” on page 107
- ◆ “[Uninstalling SnapDrive and MPIIO drivers](#)” on page 108
- ◆ “[Uninstalling the FCP driver](#)” on page 108
- ◆ “[Uninstalling the iSCSI Software Initiator](#)” on page 109

Uninstalling the VLD driver

After you have converted all VLD-type virtual disks to LUNs (see “[VLD-to-LUN conversion](#)” on page 77) and have made a backup and checked that all your applications are running properly, you should remove any version of the VLD driver that is on your system. This driver could have been installed as part of a previous version of SnapDrive or the VLD Manager application, and could still be on your system even if you have not recently used VLD-type virtual disks.

To check for and remove the VLD driver if necessary, complete the following steps.

Step	Action
1	Make sure that no VLD-type virtual disks are connected to your Windows host. You can confirm this by selecting SnapDrive in the MMC and opening the Disks folder. VLDs are flagged with a “v” in the upper-left part of the disk icon and have a .vld suffix in the details list.
2	On the Windows host, navigate to the Microsoft Device Manager by right-clicking My Computer, and then selecting Properties > Hardware > Device Manager.
3	Open SCSI and RAID Controllers.
4	If there is an entry for VLD Driver, pull down the Action menu and select Uninstall, and then click OK in the dialog box to confirm that you want to uninstall the VLD driver.

Uninstalling SnapDrive and MPIO drivers

Perform the following steps if, for some reason, you need to do any of the following:

- ◆ Uninstall SnapDrive
- ◆ Uninstall the MPIO drivers

Step	Action
1	Navigate to the folder containing the SnapDrive installation package from which you did the installation (or the CD directory).
2	Launch the SnapDrive executable, which guides you through the uninstall procedure.

Note

Do not attempt to uninstall the MPIO drivers using the Device Manager, or the Add/Remove Programs utility. You must use the SnapDrive InstallShield wizard to remove the MPIO drivers.

Caution

To avoid data corruption, make sure all LUNs are using a single path before uninstalling MPIO.

Uninstalling the FCP driver

To remove the FCP driver, complete the following steps.

Step	Action
1	Make sure that no virtual disks are connected to your Windows host over an FCP connection.
2	On the Windows host, navigate to the Microsoft Device Manager by right-clicking My Computer, then choosing Properties > Hardware > Device Manager.
3	Open SCSI and RAID Controllers.
4	Select the entry for the Fibre Channel HBA, pull down the Action menu and select Uninstall, and then click OK in the dialog box to confirm that you want to uninstall the FCP driver.
5	Remove the HBA (the physical card) from the system.

Uninstalling the iSCSI Software Initiator

To uninstall the Microsoft iSCSI Software Initiator, complete the following steps.

Step	Action
1	Make sure that no virtual disks are connected to your host by means of the iSCSI protocol.
2	If you are uninstalling from hosts in a cluster, and you plan to convert your quorum disk from iSCSI to FCP, complete the following steps, otherwise, skip to Step 3. a. Create a temporary shared FCP LUN. In Cluster Administrator, right-click the top-level cluster name and select Properties. b. In the Properties dialog, select the Quorum tab. c. Select the temporary shared LUN from the list of available drives, and then click OK. The temporary LUN is now the quorum disk. d. From SnapDrive, disconnect the quorum disk, then reconnect using FCP. e. In Cluster Administrator, redirect the cluster back to the original quorum disk. f. Delete the temporary shared LUN.
3	Stop the SnapDrive service. See “ Stopping and starting the SnapDrive service ” on page 105.

Step	Action
4	If you are running SnapManager for Exchange, stop the application-specific services, (for example, Microsoft Exchange System Attendant) which have iSCSI dependencies. Note You can also remove iSCSI dependencies using SnapManager for Exchange Configuration Wizard, however, this option is not recommended and should only be used if you are unable to stop the application-specific services.
5	From the Windows Control Panel, select Add or Remove Programs and remove the Microsoft iSCSI Initiator.
6	To reinstall the Microsoft iSCSI Initiator, relaunch the Microsoft iSCSI Software Initiator executable or, if you are installing a new version of the iSCSI software initiator, download the new version, then follow the procedure “ Installing the iSCSI Software Initiator ” on page 96.
7	Restart the SnapDrive service.
8	If you are uninstalling from hosts in a cluster, restart the cluster service.

The topics that follow explain how to manage iSCSI sessions that you use to access virtual disks on the targets (filers).

Go to any of the following topics for more information.

- ◆ [“Tasks for managing iSCSI sessions”](#) on page 112
- ◆ [“Establishing an iSCSI session to a target”](#) on page 113
- ◆ [“Disconnecting an iSCSI target from a Windows host”](#) on page 116
- ◆ [“Disconnecting a session to an iSCSI target”](#) on page 117
- ◆ [“Examining details of iSCSI sessions”](#) on page 119

Tasks for managing iSCSI sessions

Ways to establish iSCSI sessions: You can establish iSCSI sessions to targets on which your virtual disks will exist in the following two ways:

- ◆ Establish iSCSI sessions prior to creating virtual disks
For detailed information, see “[Establishing an iSCSI session to a target](#)” on page 113.
- ◆ Establish iSCSI sessions during the creation of a virtual disk
If an iSCSI session does not exist to a target on which you create a virtual disk, SnapDrive collects the pertinent information about the session when you use the Create Disk Wizard and establishes the session.
For detailed information, see “[Establishing an iSCSI session to a target](#)” on page 113.

Other iSCSI management tasks: In addition to the preceding iSCSI management tasks, you can perform the following iSCSI-specific tasks:

- ◆ Disconnect an iSCSI target from the Windows host
For detailed information, see “[Disconnecting an iSCSI target from a Windows host](#)” on page 116.
- ◆ Examine details about iSCSI sessions
For detailed information, see “[Examining details of iSCSI sessions](#)” on page 119.

Establishing an iSCSI session to a target

You need to have an iSCSI session to a target on which you create a virtual disk. You establish this session prior to creating a virtual disk.

Note— If you do not establish an iSCSI session to a target prior to creating a virtual disk on it, SnapDrive prompts you for information it needs to establish the session during the course of virtual disk creation. After you supply the information, the iSCSI session is established during the virtual disk creation process. For detailed information, see “[Creating a virtual disk](#)” on page 123.

iSCSI software initiator node naming standards

When you install the Microsoft iSCSI Software Initiator, an applet is installed that enables you to rename the initiator node to something other than the standard iSCSI qualified name (IQN) or IEEE EUI-64 (EUI) formats. Data ONTAP, however, does not recognize non-standard initiator node names and will return an error when you attempt to create a virtual disk using a node name that does not use the IQN or EUI formats.

The following are the formats for standard initiator node names.

IQN-type node name uses the following format:

`iqn.yyyy-mm.reverse_domain_name:any`

For example:

`iqn.1991-05.com.microsoft:winclient1`

The EUI-type node name format consists of the “eui.” prefix, followed by 16 ASCII-encoded hexadecimal characters. For example:

`eui.02004567A425678D`

Establishing an iSCSI session to a target

To establish an iSCSI session to a target, complete the following steps.

Step	Action
1	Verify that the iSCSI service is started.

Step	Action
2	Perform the following actions to launch the Create iSCSI Session wizard: a. Expand the Storage option in the left panel of the MMC, if it is not expanded already. b. Double-click SnapDrive. c. Select iSCSI Management. d. Click Action (from the menu choices on top of the MMC). e. Select Establish New Session from the drop-down menu.
3	In the Create iSCSI Session wizard, click Next. Result: The Provide Filer Identification panel is displayed.
4	In the Provide Filer Identification panel, enter the NetBIOS name or IP address of the target (filer) you want to establish the iSCSI session with, and then click Next. Result: The Provide iSCSI HBA panel is displayed.
5	In the upper pane of the Provide iSCSI HBA panel, click the radio button next to the iSCSI HBA you want to use.
6	In the lower pane of the Provide iSCSI HBA panel, perform the following actions: a. Select the target portal to which SnapDrive will establish the iSCSI session by clicking the button next to the IP address of the target portal you want to use. b. If your target requires authentication, select Use CHAP, and then enter the user name and password that SnapDrive will use to authenticate the initiator to the target. For more information about CHAP, see “Understanding CHAP authentication” on page 115. c. Click Next. Result: The Completing the iSCSI Session Wizard panel is displayed.

Step	Action
7	In the Completing the iSCSI Session Wizard, perform the following actions: a. Review the information to make sure it is accurate. b. If the information is not accurate, use Back to go back to previous panels of the wizard to modify information. c. Click Finish. Result: An iSCSI session to the target is established.

Understanding CHAP authentication

The Challenge Handshake Authentication Protocol (CHAP) enables authenticated communication between iSCSI initiators and targets. When you use CHAP authentication, you define the CHAP user names and passwords on the initiator and the filer.

During the initial stage of the iSCSI session, the initiator sends a login request to the filer to begin the session. The login request includes the initiator's CHAP user name and algorithm. The filer responds with a CHAP challenge. The initiator provides a CHAP response. The filer verifies the response and authenticates the initiator. The CHAP password is used to compute the response.

Disconnecting an iSCSI target from a Windows host

To disconnect an iSCSI target from a Windows host, complete the following steps.

Step	Action
1	Perform the following actions to disconnect an iSCSI target: a. Expand the Storage option in the left panel of the MMC, if it is not expanded already. b. Double-click SnapDrive. c. Double-click iSCSI Management. d. Select the iSCSI session that you want to disconnect. e. Click Action (from the menu choices on top of the MMC). f. Select Disconnect Target from the drop-down menu. Result: A SnapDrive pop-up box is displayed prompting you to confirm your action. Additionally, if you have virtual disks (LUNs) connected to the iSCSI target, a warning pop-up box is displayed prompting you to confirm that all LUNs on the iSCSI target can be terminated.
2	Click Yes. Result: The selected iSCSI target is disconnected from the Windows host.

Disconnecting a session to an iSCSI target

You can disconnect an iSCSI session from an iSCSI target when you have more than one session and you do not want to disconnect the target or other sessions connected to that target. For example, when you are using MPIO, you can disconnect iSCSI sessions to create a single path to a LUN. For more information on MPIO, see Chapter 9, “[Multipathing](#),” on page 189.

To disconnect a session to an iSCSI target, complete the following steps.

Step	Action
1	Perform the following actions to disconnect a session to an iSCSI target: a. Expand the Storage option in the left panel of the MMC, if it is not expanded already. b. Double-click SnapDrive. c. Double-click iSCSI Management. d. Select the iSCSI target from which you want to disconnect a session.
2	In the right pane of the MMC, select the iSCSI session you want to disconnect.
3	Click Action (from the menu choices on top of the MMC), and select Disconnect Session. Result: A SnapDrive pop-up box is displayed prompting you to confirm your action. Additionally, if you disconnect the last session to the iSCSI target and you have virtual disks (LUNs) connected to the target, a warning pop-up box is displayed prompting you to confirm that all LUNs on the iSCSI target can be terminated. Note— If you have only one iSCSI session connected to the iSCSI target, performing this procedure will disconnect the iSCSI target from the Windows host.

Step	Action
4	Click Yes. Result: The selected iSCSI session is disconnected from the iSCSI target.

Examining details of iSCSI sessions

The following table describes the iSCSI session details you can examine using the Computer Management (MMC) window on your Windows host. For instructions, go to [“Examining details of iSCSI sessions”](#) on page 119.

Property	Description
For all iSCSI sessions	
iSCSI Target Name	iSCSI name of the target
Number of LUNs	Number of virtual disks (LUNs) to the target portal to which the Windows host is connected
For a specific iSCSI session	
Initiator HBA	Initiator HBA being used for the iSCSI session
Initiator IP	Initiator IP address
Target Portal IP	Target portal’s IP address to which the iSCSI session exists
Target Portal IP Port	Target portal’s port number on which the target is listening for iSCSI session requests

Examining details of iSCSI sessions

To examine the details of iSCSI sessions from your Windows host, complete the following steps.

Step	Action
1	Perform the following actions: a. b. c. Expand the Storage option in the left panel of the MMC, if it is not expanded already. Double-click SnapDrive. Select iSCSI Management.

Step	Action	
2	If you want to view...	Then...
	The details of all iSCSI targets connected on the Windows host	The details are displayed in the right panel of the MMC.
	The details of a specific iSCSI session connected from the Windows host to a particular target	a. Double-click iSCSI Management. b. Select the connected iSCSI target whose details you want to view. Result: The details are displayed in the right panel of the MMC.

Go to any of the following topics to learn about virtual disk management:

- ◆ [“About virtual disk management”](#) on page 122
- ◆ [“Creating a virtual disk”](#) on page 123
- ◆ [“Creating a shared virtual disk on a Windows cluster”](#) on page 128
- ◆ [“Creating a virtual disk as a quorum disk on a new Windows cluster”](#) on page 129
- ◆ [“Creating a shared non-quorum virtual disk on a Windows cluster”](#) on page 139

About virtual disk management

After you install SnapDrive to manage your virtual disks, keep the following in mind:

- ◆ You must never create, delete, or rename virtual disks from FilerView or the filer command line.
- ◆ You must perform all virtual disk management functions using SnapDrive from the host machine.

Note

Network Appliance recommends that you execute all SnapDrive operations from the console of your host machine, through a Remote Administration connection, or using the `sdcli.exe` command-line utility. Do not use Terminal Services because you might not be able to see all SnapDrive error messages, and the list of available drive letters will not be up-to-date.

Creating a virtual disk

Go to any of the following topics for information on creating virtual disks.

- ◆ [“Rules for creating a virtual disk”](#) on page 123
- ◆ [“Creating a virtual disk”](#) on page 123

Rules for creating a virtual disk

Keep the following rules in mind when creating a virtual disk:

- ◆ If you are adding the virtual disk to a cluster, make sure to perform the following procedure on whichever node owns that cluster’s physical disk resources.
- ◆ To ensure that snapshots can be taken, do not attempt to create a virtual disk on a filer volume that holds anything other than virtual disks. Conversely, do not put anything other than virtual disks on a filer volume that contains virtual disks.
- ◆ Virtual disk names must be created using ASCII characters only, even when using non-ASCII operating systems.

Creating a virtual disk

To create an FCP- or iSCSI-accessed virtual disk, complete the following steps.

Step	Action
1	Create the dedicated volumes to hold your virtual disks on the filer and create CIFS shares for those volumes. For more information on creating volumes, see “Creating a filer volume” on page 45. For more information about creating CIFS shares, see “Creating a CIFS share” on page 46, and also consult the <i>Data ONTAP File Access Management Guide</i> .
2	Verify that the FCP or iSCSI services have been started on the filer. For more information, see “Starting FCP and iSCSI services” on page 41.

Step	Action						
3	Perform the following actions to launch the Create Disk wizard: a. Expand the Storage option in the left panel of the MMC, if it is not expanded already. b. Double-click SnapDrive. c. Select Disks. d. Click Action (from the menu choices on top of the MMC). e. Select Create Disk from the drop-down menu. Result: The Create Disk wizard is launched. f. In the Create Disk wizard, click Next.						
4	In the Provide a Path and Name panel, perform the following actions: ◆ In the “Enter a Virtual Disk UNC Path to Filer Volume or Qtree” field, type the filer location for the virtual disk. Alternatively, click Browse and navigate to that location. ◆ In the “Enter a Name for the New Virtual Disk” field, type in a descriptive name for the virtual disk; for example, “corporate billing” or “sunnyvale gym.” ◆ The name you enter in this field is automatically made lowercase. Click Next. Result: The Select a Virtual Disk Type panel is displayed.						
5	In the Select a Virtual Disk Type panel, perform one of the following actions:						
	<table><tr><th>If...</th><th>Then...</th></tr><tr><td>The virtual disk will belong to a single-host system</td><td>Select Dedicated, click Next, and then skip to Step 7.</td></tr><tr><td>The virtual disk will be a Windows cluster resource</td><td>Select Shared, click Next, and then proceed to the next step.</td></tr></table>	If...	Then...	The virtual disk will belong to a single-host system	Select Dedicated, click Next, and then skip to Step 7 .	The virtual disk will be a Windows cluster resource	Select Shared, click Next, and then proceed to the next step.
	If...	Then...					
	The virtual disk will belong to a single-host system	Select Dedicated, click Next, and then skip to Step 7 .					
The virtual disk will be a Windows cluster resource	Select Shared, click Next, and then proceed to the next step.						
6	In the “Information About the Microsoft Cluster Services System” panel, verify that you want the disk to be shared by the nodes listed, and then click Next.						

Step	Action
7	In the Select Virtual Disk Properties panel, perform the following actions: ◆ Select from the list of available drive letters a drive letter for the virtual disk you are creating. ◆ Click Yes or No for the option labeled “Do you want to limit the maximum disk size to accommodate at least one snapshot?” If you select Yes, the disk size limits displayed are accurate only when they first appear on the Select Virtual Disk Properties panel. When this option is selected, the following actions might interfere with the creation of at least one snapshot: ❖ The option is set to No and SnapDrive is used to create an additional virtual disk in the same filer volume. ❖ A virtual disk is created in the same filer volume <i>without</i> using SnapDrive. ❖ Data objects other than virtual disks are stored on this filer volume. ◆ Select a disk size, which must fall within the minimum and maximum values displayed in the panel. ◆ Click Next. Result: If the settings on the filer volume or qtree on which you are creating the virtual disk do not allow SnapDrive to proceed with the create operation, the Important Properties of the Filer Volume panel is displayed, as described in Step 8. Otherwise, Step 8 is skipped.
8	The “Important Properties of the Filer Volume” panel displays the settings that will be used for the volume or qtree you specified in Step 4 of this procedure. SnapDrive requires the filer volume containing virtual disks to have the following properties: ◆ <code>create_ucose = on</code> ◆ <code>convert_ucose = on</code> ◆ <code>snapshot schedule = off</code> Note _____ SnapDrive cannot proceed to create a virtual disk unless these settings are configured as shown. Therefore, you must accept these settings. _____ Click Next.

Step	Action	
9	If...	Then...
	The virtual disk will belong to a single-host system	Go to Step 15 .
	The virtual disk will be a Windows cluster resource	Go to the next step.
10	In the Select Initiators panel, perform the following actions: a. Double-click the cluster group name to display the hosts that belong to the cluster. b. Click the name of a host to select it. Result: The list of Available Initiators for that host is displayed in the bottom-left pane.	
11	In the Select Initiators panel, select the initiator for the virtual disk you are creating and use the arrows to move it back and forth between the two panes. If you select an iSCSI initiator, and an iSCSI connection to the filer on which you are creating the virtual disk does <i>not</i> exist, you are prompted to select a target portal. Also, if your target requires authentication of hosts that connect to it, you can enter that information here. After you click OK, the iSCSI connection from the Windows host to the filer is established, even if you do not complete the Create Disk Wizard.	
12	Repeat Step 10 and Step 11 for all hosts, and then click Next. Result: The Specify Microsoft Cluster Services Group panel is displayed. Note_____ The Next button remains grayed out until initiators for all hosts of a cluster have been selected. _____	

Step	Action
13	In the “Specify Microsoft Cluster Services Group” panel, perform the following actions. ◆ From the Group drop-down list, select a cluster group to which the newly created virtual disk will belong. OR Select Create a New Cluster Group to create a new cluster group and then put the newly created LUN in that group. Note _____ When selecting a cluster group for your virtual disks, choose the cluster group your application will use. ◆ Click Next. Result: The Completing the Create Disk Wizard panel is displayed.
14	Go to Step 16 .
15	In the Select Initiators panel, select the FCP or iSCSI initiator for the virtual disk you are creating, and use the arrows to move it back and forth between the two panes. If you select an iSCSI initiator, and an iSCSI connection to the filer on which you are creating the virtual disk does <i>not</i> exist, you are prompted to select a target portal. Also, if your target requires authentication of hosts that connect to it, you can enter that information here. After you click OK, the iSCSI connection from the Windows host to the filer is established, even if you do not complete the Create Disk Wizard.
16	In the Select Initiators panel, click Next. Result: The Completing the Create Disk Wizard panel is displayed.
17	In the Completing the Create Disk Wizard panel, perform the following actions: ◆ Verify all the settings. ◆ If you need to change any settings, click Back to go back to the previous Wizard panels. ◆ Click Finish. Result: The MMC is displayed, with the new virtual disk now appearing under SnapDrive in the left panel.

Creating a shared virtual disk on a Windows cluster

The process for creating a shared virtual disk depends on how that shared disk is going to be used. In a Windows cluster, shared virtual disks are used as physical disk cluster resources. One of these physical disk cluster resources is used as a quorum disk.

- ◆ For information about how to create a shared virtual disk that will be used as a quorum disk when setting up a new Windows cluster, see “[Creating a virtual disk as a quorum disk on a new Windows cluster](#)” on page 129.
- ◆ For information about how to create a shared virtual disk that will *not* be used as a quorum disk, see “[Creating a shared non-quorum virtual disk on a Windows cluster](#)” on page 139.

Creating a virtual disk as a quorum disk on a new Windows cluster

Prerequisites: When you create a Windows cluster whose quorum disk will be a virtual disk, you must ensure the following:

- ◆ You have one of the following:
 - ❖ Two host machines with Windows 2000 Advanced Server installed
 - ❖ Two to four host machines with Windows Server 2003 Standard Edition or Enterprise Edition installed
- ◆ Your filer is running at least Data ONTAP 6.5.4.
- ◆ Each node of the cluster contains the following:

If...	Then...
You want the quorum disk to be an iSCSI-accessed LUN	Each host node must have the following installed: ◆ If you are using the Microsoft iSCSI Software Initiator: ❖ A GbE NIC (as recommended in the iSCSI Microsoft Initiator Software Support Kit) ❖ The Microsoft iSCSI Software Initiator driver ❖ (Optional) a Fast Ethernet NIC dedicated to internal cluster traffic For information about the Microsoft iSCSI Software Initiator, see the Microsoft site. ◆ If you are using a WHQL signed iSCSI HBA: ❖ The driver and firmware for the iSCSI HBA
You want the quorum disk to be an FCP-accessed LUN	Each host node must have the following installed: ◆ A NetApp qualified FCP HBA ◆ The driver and firmware for the FCP HBA For information about the qualified FCP HBAs, go to http://now.netapp.com/.

Guideline to prevent resource competition in a Windows cluster: To ensure that all nodes of the cluster host never start simultaneously following a power failure, change the file timeout value in the boot.ini file to 10 seconds for one node and 90 seconds for the other nodes. This allows plenty of time for one node to “get ahead” of the other nodes, preventing the computer from competing for the shared disk, which could cause a failure. See Microsoft article 259267 for more information.

Related topics:

- ◆ [“Creating a virtual disk as a quorum disk on a new Windows 2000 Server cluster”](#) on page 131.
- ◆ [“Creating a virtual disk as a quorum disk on a new Windows Server 2003 cluster”](#) on page 133

Creating a virtual disk as a quorum disk on a new Windows 2000 Server cluster

To install and configure a virtual disk as a cluster quorum disk on a new Windows 2000 Server cluster, complete the following steps.

Note

It is important to perform the steps listed in the following procedure in order.

Task	Procedure
1	Make sure that the following are installed on both nodes of the cluster: ◆ Appropriate FCP HBA drivers, WHQL signed iSCSI HBA drivers, or the Microsoft iSCSI Software Initiator drivers For information about the drivers, see “Prerequisites” on page 129. ◆ SnapDrive 3.2 For information about installing SnapDrive, see “Installing or Upgrading SnapDrive” on page 59.
2	Create a shared virtual disk on node 1 and note the drive letter you assign to the virtual disk. For information about how to create a virtual disk, see “Creating a virtual disk” on page 123.
3	Install and configure the Windows cluster on node 1, designating the virtual disk you created in Step 2 as the quorum disk. For detailed information about configuring Windows clusters, see your Microsoft documentation.
4	From node 2, use SnapDrive to connect to the virtual disk you created in Step 2. You are prompted for the name of the cluster you created in Step 3.
5	Install and configure the Windows cluster service on node 2 and join node 2 to the cluster.

Task	Procedure
6	Use the Cluster Administrator to verify that the cluster is functioning correctly by performing a “move group” operation from one node to the other and then back to the original node.

Creating a virtual disk as a quorum disk on a new Windows Server 2003 cluster

The following procedure describes the steps you must perform to set up a new Windows Server 2003 cluster (2-node to 4-node) using a virtual disk (LUN) as a quorum disk.

This procedure does not describe in detail the steps that involve setting up the Windows nodes for a cluster. If you need details about such steps, you must refer to your Microsoft documentation.

Note

It is important to perform the steps listed in the following procedure in order.

To install and configure a virtual disk as a cluster quorum disk on a new Windows Server 2003 cluster, complete the following steps.

Task	Procedure
1	Install Windows Server 2003 on all nodes that will be part of the cluster. For more information about installing the Windows Server 2003 software, see your Microsoft documentation. After the installation is complete, for the purpose of this procedure: ◆ Ignore the “Manage your server” window that is displayed after a new installation of Windows Server 2003. ◆ Do not run the Cluster Administrator utility yet.
2	Make sure that the following are installed on all nodes of the cluster: ◆ Appropriate FCP HBA drivers, WHQL signed iSCSI HBA drivers, or the Microsoft iSCSI Software Initiator drivers For information about the drivers, see “Prerequisites” on page 129. ◆ SnapDrive 3.2 For information about installing SnapDrive, see “Installing or Upgrading SnapDrive” on page 59.

Task	Procedure
3	If you are using the Microsoft iSCSI software, establish iSCSI connections to the filer from all nodes of the cluster using the MMC window of each node. To go to the MMC, select Start > Programs > Administrative Tools > Computer Management. For information about how to establish iSCSI connections, see “Establishing an iSCSI session to a target” on page 113.
4	Create a shared virtual disk on node 1 and note the path and drive letter you assign to the virtual disk. For information about how to create a virtual disk, see “Creating a virtual disk” on page 123. Note _____ Because this virtual disk will be designated as a quorum disk later in this procedure, you must create a disk of adequate size according to Microsoft’s recommendations.
5	On node 1, launch the Windows Server 2003 Cluster Administrator. If the Cluster Administrator is launched for the first time on this node, you are prompted to specify the action to take. Select Create New Cluster from the Action drop-down list. If the Cluster Administrator is launched subsequently, it does not prompt you to specify the action to take. In that case, select File > New > Cluster from the Cluster Administrator. Result: The New Server Cluster Wizard is displayed.

Task	Procedure	
6	In the New Server Cluster Wizard, follow the prompts to enter the following information: ◆ Windows domain name and cluster name ◆ The node that will be the first node in the cluster The node you are working on currently should be the selected node in the wizard. ◆ IP address for the server cluster ◆ User name and password for the cluster service account Note _____ Note the user name and password you enter; you need it in a later step in this procedure. Result: After you have entered the above information in the New Server Cluster Wizard windows, the Proposed Cluster Configuration panel is displayed.	
7	If...	Then...
	The virtual disk you created in Step 4 is automatically selected as the quorum disk	Go to Step 8 .
	The virtual disk you created in Step 4 is not selected as the quorum disk	◆ Click the quorum button. ◆ Change the drive letter to that of the virtual disk and click Next.
8	Step through the remaining panels of the New Server Cluster Wizard. After you finish using the New Server Cluster Wizard, the first node in the cluster is up and functional.	

Task	Procedure
9	Go to the Windows host that will be the next node in the cluster and connect to the virtual disk you created in Step 4 from this node, using the path and drive letter you noted in Step 4. Note _____ The Shared disk option is automatically selected. Result: You are prompted for the cluster name. For information about how to connect a virtual disk, see “Connecting virtual disks” on page 142.
10	Enter the cluster name you created in Step 6 . Click OK.
11	Launch the Windows Server 2003 Cluster Administrator and perform the following actions: ◆ Select File > Open Connection. ◆ Select Add Nodes to Cluster. ◆ Enter the name of the cluster (as in Step 6). ◆ Click Next. Result: The Add Nodes Wizard is displayed with the name of the node on which you are currently working.
12	In the Add Nodes Wizard, follow the prompts to perform the following tasks in the Wizard panels: ◆ If the name of the node on which you are working currently is not displayed, enter the name of the node or click Browse to find the node. Then click Add to add the node to the list. ◆ Select Advanced > Advanced (minimum) Configuration. ◆ Enter the password for the cluster service account. Note _____ This password should be the same as the one you entered in Step 6. Result: After you enter the information, the Proposed Cluster Configuration panel is displayed.

Task	Procedure	
13	If...	Then...
	The proposed cluster configuration is as expected	Follow the Add Nodes Wizard prompts to complete the remaining steps of the Wizard. Result: The node is added to the cluster.
	The proposed cluster configuration is not as expected	Make the appropriate changes, and then follow the Add Nodes Wizard prompts to complete the remaining steps of the Wizard. Result: The node is added to the cluster.
14	Use the Cluster Administrator to verify that the cluster is functioning correctly by performing a “move group” operation from one node to the other and then back to the original node. Note _____ You should perform the “move group” operation for all nodes in the cluster to ensure proper operation. _____	
15	If...	Then...
	The node you added to the cluster was the last node	Go to Step 17 .
	The node you added to the cluster was not the last node	Go to Step 9 .
16	Restart the SnapDrive service. Note _____ NetApp recommends restarting the SnapDrive service after installing MSCS on a Windows 2003 host to ensure the disktimeout value is set to the SnapDrive default of 190 seconds. _____	

Task	Procedure
17	You have added the desired number of nodes to a Windows Server 2003 cluster. The server cluster is up and operational. Now, you can create shared disks for your applications. For information about how to create shared disks, see “Creating a shared non-quorum virtual disk on a Windows cluster” on page 139.

Creating a shared non-quorum virtual disk on a Windows cluster

When to use this this procedure: Follow these instructions if you need to create shared virtual disks on a host that is already running in a Windows 2000 Server or Windows Server 2003 cluster configuration.

About creating a shared virtual disk on a Windows cluster: When creating a shared virtual disk on a Windows cluster, you must connect all the virtual disks that will be shared cluster resources as *shared* disks, rather than as dedicated disks attached to just a single node in the cluster. (The partner node cannot “see” dedicated disks attached to the opposite node.)

Creating a shared virtual disk : To create a shared virtual disk for an existing Windows cluster, complete the following steps.

Step	Action
1	Make sure that the appropriate FCP HBA drivers or the Microsoft iSCSI Software Initiator drivers and SnapDrive are installed on all nodes in a cluster. See “Prerequisites” on page 129 for information about the drivers. See “Installing the new SnapDrive components” on page 101.
2	Create as many shared virtual disks as are necessary to hold your data. See “Creating a virtual disk” on page 123 for detailed information. Note_____ You must perform this operation on the node that owns the cluster group to which the newly created virtual disk will belong. _____
3	Install your host machine application software. Consult your host-side application software documentation for specific instructions.

The topics that follow explain how to use SnapDrive to manage virtual disks.

- ◆ [“Connecting virtual disks”](#) on page 142
- ◆ [“Disconnecting virtual disks”](#) on page 146
- ◆ [“Deleting a virtual disk”](#) on page 149
- ◆ [“Expanding virtual disks”](#) on page 150
- ◆ [“Managing LUNs not created in SnapDrive”](#) on page 155
- ◆ [“Examining and modifying the Monitor Time Interval”](#) on page 158
- ◆ [“Administering SnapDrive remotely”](#) on page 160
- ◆ [“Enabling SnapDrive notification”](#) on page 161

Connecting virtual disks

When connected, a virtual disk enables you to save, delete, modify, and manage the files it contains. You can also take snapshots of the entire disk and restore the disk, along with its contents, to the state captured by a previous snapshot. Additionally, you can disconnect or delete the disk.

Rule for connecting: Unless the virtual disk is shared within a Windows cluster, the virtual disk must not be connected to more than one host.

Caution—
Do not try to connect to a virtual disk if it is already connected to another machine; SnapDrive does not support such simultaneous use.

For instructions for connecting a virtual disk, see “[Connecting a virtual disk](#)” on page 142.

Connecting a virtual disk

To connect your Windows host to a virtual disk, complete the following steps.

Step	Action
1	Close all Explorer windows on your host.
2	Perform the following actions to launch the Connect Disk wizard: a. Expand the Storage option in the left panel of the MMC, if it is not expanded already. b. Double-click SnapDrive in the left panel of the MMC. c. Select Disks. d. Click Action (from the menu choices on top of the MMC). e. Select Connect Disk from the drop-down menu.
3	In the Connect Disk Wizard, click Next.

Step	Action	
4	In the Provide Virtual Disk Location panel, perform the following actions. ◆ Click Browse. ◆ Navigate to the filer volume on which the virtual disk resides. ◆ Select the virtual disk (LUN) with a .lun extension to which you want to connect. ◆ Click Next. Result: The Select a Virtual Disk Type panel is displayed.	
5	If the virtual disk...	Then...
	Will belong to a single system	Select Dedicated, click Next, and then continue to Step 7 .
	Will become a Windows cluster resource	Select Shared, click Next, and then continue to the next step.
6	In the Information about the Microsoft Cluster Services System panel, verify that you want the disk to be shared by the nodes listed, and then click Next.	
7	In the Select Virtual Disk Drive Letter panel, perform the following actions. ◆ Select from the list of available drive letters a drive letter for the virtual disk you are connecting. ◆ Click Next.	
8	If the virtual disk...	Then...
	Will belong to a single-host system	Go to Step 12 .
	Will be a Windows cluster resource	Go to the next step.

Step	Action
9	In the Select Initiators panel, perform the following actions. a. Double-click the cluster group name to display the hosts that belong to the cluster. b. Click the name of a host to select it. The list of available initiators for that host is displayed in the lower-left pane. c. Select the initiator for the virtual disk you are creating, and use the arrows to move it back and forth between the Available Initiators and Selected Initiators list. d. Repeat Step b through Step c for all the hosts. e. Click Next. Note— The Next button is unavailable until initiators for all hosts of a cluster are selected. Result: The Specify Microsoft Cluster Services Group panel is displayed.
10	In the Specify Microsoft Cluster Services Group panel, perform the following actions: ◆ Select a cluster group from the Group drop-down list to which the newly created virtual disk will belong. OR Select Create a New Cluster Group to create a new cluster group and then put the virtual disk you are connecting to in that group. ◆ Click Next. Result: The Completing the Create Disk Wizard panel is displayed.
11	Go to Step 13 .

Step	Action
12	In the Select Initiators panel, perform the following actions. ◆ Select the FCP or the iSCSI initiator for the virtual disk you are creating from the Available Initiators list on the left side. Note— FCP and iSCSI are supported on the same host, however, FCP and iSCSI are not supported on the same host connecting to the same LUN. SnapDrive will not allow you to select both protocols when connecting a virtual disk. Note— If MPIO is installed on the system, you can select two FCP initiator ports simultaneously or one iSCSI session. ◆ Click the right arrow to move the selected initiator to the Selected Initiators list on the right side. If you change your mind, you can move an initiator from the Selected Initiators list to the Available Initiators list by selecting the initiator and clicking the left arrow. ◆ Click Next. Result: The Completing the Connect Disk Wizard panel is displayed. Note— See the <i>Data ONTAP Block Access Management Guide for FCP</i> or the <i>Data ONTAP Block Access Management Guide for iSCSI</i> for information about how to determine the port for your HBA.
13	In the Completing the Connect Disk Wizard panel, perform the following actions. ◆ Verify all the settings. ◆ If you need to change any settings, click Back to go back to the previous Wizard panels. ◆ Click Finish. Result: The Computer Management window is displayed, with the newly connected virtual disk now appearing under SnapDrive > Disks in the left panel.

Disconnecting virtual disks

When the host is disconnected from a virtual disk, you cannot see or modify the virtual disk’s contents, take snapshots of the virtual disk, or use Snapshot to restore the virtual disk to a previous snapshot. However, the virtual disk still exists on the filer volume.

Guidelines for disconnecting a virtual disk: The following guidelines apply to disconnecting a virtual disk:

- ◆ You must make sure that the virtual disk you are disconnecting is not monitored with the Windows Performance Monitor (perfmon).
- ◆ You can only disconnect a shared virtual disk (that is, a non-quorum disk) after removing the cluster resource dependencies from the virtual disk.
- ◆ You can disconnect a quorum disk only after replacing it with another disk that takes over as a quorum disk for the cluster.
- ◆ You must make sure when disconnecting virtual disks on a Microsoft cluster that all hosts in the cluster are available to SnapDrive in order for disconnect operation to succeed.

Ways to disconnect a virtual disk: You can disconnect a virtual disk in one of the following two ways:

- ◆ By disconnecting in a normal manner, as described in “[Disconnecting a virtual disk](#)” on page 146.
- ◆ By forcing a disconnect, as described in “[Forcing a disconnect](#)” on page 147.

When you force a disk to disconnect, it results in the disk being unexpectedly disconnected from the Windows host.

Under ordinary circumstances, you cannot disconnect a virtual disk that contains a file being used by an application such as Windows Explorer or the Windows operation system. However, you can force a disconnect to override this protection.

Disconnecting a virtual disk

To disconnect a virtual disk from a host, complete the following steps.

Step	Action
1	Make sure that neither Windows Explorer nor any other Windows application is using or displaying any file on the virtual disk you intend to disconnect.

Step	Action
2	Double-click SnapDrive in the left pane of the MMC, and then select Disks. Result: The currently connected disks are displayed in the right panel of the MMC.
3	Select in the right pane the disk that you want to disconnect.
4	Click Action (from the menu choices on top of the MMC), and then select Disconnect Disk.
5	When prompted, click Yes to proceed with the operation. Result: The icons representing the disconnected virtual disk disappear from both the left and right panels of the MMC window.

Related topic:

- ◆ “[Forcing a disconnect](#)” on page 147

Forcing a disconnect

Before you decide to force a disconnect of a SnapDrive virtual disk, be aware of the following consequences:

- ◆ Any cached data intended for the virtual disk at the time of forced disconnection is not committed to disk.
- ◆ A pop-up message announcing that the disk has undergone “surprise removal” appears in the console session.

To force a disconnect from a virtual disk, complete the following steps.

Step	Action
1	Make sure that neither Windows Explorer nor any other Windows application is using or displaying any file on the virtual disk you intend to disconnect.
2	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.

Step	Action
3	Double-click SnapDrive in the left pane of the MMC, and then select Disks. Result: The currently connected disks are displayed in the right panel of the MMC.
4	Select in the right pane the disk that you want to “force disconnect.”
5	Click Action (from the menu choices on top of the MMC), and then select Force Disconnect Disk.
6	When prompted, click Yes to proceed with the operation. Result: The icons representing the disconnected virtual disk disappear from both the left and right panels of the MMC.
7	To reconnect a virtual disk after a forced disconnect, see “ Connecting virtual disks ” on page 142.

Related topic:

- ◆ “[Disconnecting a virtual disk](#)” on page 146

Deleting a virtual disk

Guidelines for deleting a virtual disk: Keep the following guidelines in mind when deleting a virtual disk:

- ◆ Make sure that the virtual disk you are deleting is not being monitored with the Windows Performance Monitor (perfmon).
- ◆ Use the Delete Disk feature cautiously, because after you delete a virtual disk, you can no longer open it, and you cannot use SnapDrive to undelete it.
- ◆ Do not delete a virtual disk being used by a host, because SnapDrive cannot undelete the virtual disk.

Deleting a virtual disk: To delete a virtual disk, complete the following steps.

Step	Action
8	Double-click SnapDrive in the left pane of the MMC, and then select Disks. Result: The currently connected disks are displayed in the right panel of the MMC.
9	In the right pane, select the disk that you want to delete.
10	Click Action (from the menu choices on top of the MMC), and then select Delete Disk.
11	When prompted, click Yes to proceed with the operation. Result: The icons representing the deleted virtual disk disappear from both the left and right panes of the Computer Management window.

Expanding virtual disks

When to expand a virtual disk: As your storage needs increase, you might need to expand a virtual disk to hold more data. A good opportunity for doing this is right after you have expanded your filer volumes.

Note

A virtual disk cannot be expanded more than ten times its original size.

Considerations when expanding a virtual disk: When you expand a virtual disk, keep the following in mind:

- ◆ Understand the storage-management implications of expanding the virtual disk. See “[Understanding volume size](#)” on page 15 for more information.
- ◆ After you increase the size of a virtual disk, you cannot reduce it in size, except by restoring a snapshot taken prior to the expansion of the virtual disk (see the note below). Such a restore causes the loss of any data added to the virtual disk after you expanded the virtual disk. (Conversely, restoring a snapshot of a virtual disk whose size has since been reduced enlarges the virtual disk to its former size.)

Note

If your host is running Windows 2003 and it is necessary to restore a virtual disk from a snapshot taken before the virtual disk was expanded, you must disconnect the disk using SnapDrive, then restore the disk from the filer console. When the virtual disk is restored, reconnect the disk using SnapDrive.

- ◆ When creating a quorum disk, make sure it is the size recommended by Microsoft for your Windows cluster setup. You cannot expand a virtual disk while it is serving as a quorum. If you need to expand your current quorum disk, you must do one of the following:
 - ❖ Create a new virtual disk and designate it as a quorum.
 - ❖ Create a temporary virtual disk to serve as a quorum while you expand the old quorum disk. Once the old quorum disk has been expanded, assign it as the quorum for the cluster and delete the temporary quorum.

For information about how to perform the previous two procedures, see “[Expanding a quorum disk](#)” on page 152.

- ◆ When you expand a virtual disk that serves as a Windows cluster physical disk resource, that physical disk resource is momentarily taken offline and then brought back online to refresh the resource properties. Also taken offline are all the Windows cluster resources having direct or indirect

dependency on the offline physical disk resource. After virtual disk expansion, you must manually bring back online all the cluster resources that were taken offline because of direct or indirect dependencies on the expanded virtual disk.

- ◆ While a virtual disk is being expanded it may not be available for use. Plan your virtual disk expansion at a time when applications are less likely to be accessing the virtual disk.

For instructions for expanding a virtual disk, see the following topics:

- ◆ “[Expanding a virtual disk](#)” on page 151
- ◆ “[Expanding a quorum disk](#)” on page 152

Expanding a virtual disk

To expand a virtual disk, complete the following steps.

Note

If you increase the size of your virtual disk, you might need to close and reopen the MMC window before the increased virtual disk size becomes visible in the Disk Management snap-in.

Step	Action
1	Double-click SnapDrive in the left pane of the MMC, and then select Disks. Result: The currently connected disks are displayed in the right panel of the MMC.
2	Select in the right pane the disk that you want to expand.
3	Click Action (from the menu choices on top of the MMC), and then select Expand Disk. Result: The Expand Disk screen is displayed.

Step	Action
4	In the Expand Disk screen, perform the following steps: ◆ Leave the field labeled “Do you want to limit” set to the default setting of Yes. When you select the option “Do you want to limit the maximum disk size to accommodate at least one snapshot?” the disk size limits displayed are accurate only when they first appear on the Select Virtual Disk Properties panel. When this option is selected, the following actions might interfere with the creation of at least one snapshot: ❖ The option to limit the maximum disk size to accommodate at least one snapshot is <i>not</i> selected when SnapDrive is used to create an additional virtual disk in the same filer volume. ❖ A virtual disk is created in the same filer volume <i>without</i> using SnapDrive. ❖ Data objects other than virtual disks are stored on this filer volume. ◆ Enter the amount by which you want to expand the virtual disk. ❖ Set the units for this value (MB, GB, or TB) in the box to the right of the Expand by Size box. ❖ Pick a value for the Expand by Size box that falls between the maximum and minimum sizes listed on the panel. ◆ Click OK. Result: A message indicating that the expansion operation was completed successfully is displayed.
5	If your host is running Windows 2003, create a new snapshot of the expanded virtual disk. For more information, see “Restoring virtual disks from snapshots” on page 176.

Related topic:

- ◆ [“Expanding a quorum disk”](#) on page 152

Expanding a quorum disk

To expand a virtual disk that is a quorum disk in a Microsoft cluster, complete the following steps.

Step	Action	
1	If...	Then...
	You would like to create a new virtual disk and designate that disk as a quorum	1. Create a new virtual disk as described in “Creating a virtual disk” on page 123. 2. Designate the newly created disk as the quorum using the Cluster Administrator on the owning node of your Windows cluster. For information about how to set a disk as a quorum, see your Windows documentation. 3. Delete the original quorum disk as described in “Deleting a virtual disk” on page 149.
	You would like to keep the original quorum disk and expand it	1. Create a new virtual disk as described in “Creating a virtual disk” on page 123. 2. Designate the newly created disk as the quorum using the Cluster Administrator on the owning node of your Windows cluster. For information about how to set a disk as a quorum, see your Windows documentation. 3. Expand the original quorum disk (which is now a regular virtual disk) as described in “Expanding a virtual disk” on page 151. 4. Designate the expanded disk as the quorum using the Cluster Administrator on the owning node of your Windows cluster. For information about how to set a disk as a quorum, see your Windows documentation. 5. Delete the disk you created in Step 1 as described in “Deleting a virtual disk” on page 149.

Related topic:

- ◆ [“Expanding a virtual disk”](#) on page 151

Managing LUNs not created in SnapDrive

With the addition of iSCSI HBA support, as well as the existing FCP support in SnapDrive 3.2, you can use SnapDrive to manage LUNs on your filer even if SnapDrive was not used to create the LUNs; however, you might need take several steps to prepare the LUNs for SnapDrive.

Prerequisites for SnapDrive to manage LUNs not created in SnapDrive

The following prerequisites must be met in order for SnapDrive to manage LUNs that were not created with SnapDrive.

- ◆ LUN names must be all ASCII characters
- ◆ LUN names must be lowercase
- ◆ Space reservation must be set to On

Preparing LUNs not created in SnapDrive in a stand-alone Windows configuration

To prepare LUNs not created in SnapDrive in a stand-alone Windows configuration to be managed by SnapDrive, complete the following steps.

Step	Action
1	Check that space reservation is on or that there is enough space available for space reservation to be turned on.
2	Shut down the Windows host. Note _____ Shutting down your Windows host ensures that all data has been flushed and that snapshots are consistent. _____
3	Using FilerView or the filer console, complete the following steps. a. Take a snapshot of the volume on which the LUNs reside. b. Unmap the LUN from the initiator group. c. If the LUN name uses uppercase or non-ASCII characters, rename the LUN from the filer console, using the <code>lun move</code> command. d. Turn on space reservation.

Step	Action
4	Restart the Windows host.
5	Using SnapDrive, connect to the renamed LUN, as described in “Connecting virtual disks” on page 142.
6	Using SnapDrive, take a snapshot of the newly connected LUN as described in “Creating snapshots” on page 166.

Preparing LUNs not created in SnapDrive in a clustered Windows configuration

To prepare LUNs not created in SnapDrive in a clustered Windows configuration to be managed by SnapDrive, complete the following steps.

Step	Action
1	In SnapDrive, create a shared disk on the filer to temporarily designate as the quorum disk, as described in “Creating a shared virtual disk on a Windows cluster” on page 128.
2	For each resource in this cluster group, record all dependencies. a. Using Cluster Administrator, right-click the resource and select Properties. b. Select the Dependencies tab. c. Record all dependencies for the resource.
3	Designate the newly created disk as the quorum using the Cluster Administrator on the owning node of your Windows cluster. For information about how to set a disk as a quorum, see your Windows documentation.
4	Check that space reservation is on or that there is enough space available for space reservation to be turned on.
5	Shut down each cluster node. Note _____ Shutting down your Windows hosts ensures that all data has been flushed and that snapshots are consistent. _____

Step	Action
6	Using FilerView or the filer console, complete the following steps. a. Take a snapshot of the volume on which the LUNs reside. b. Unmap the LUN from the initiator group. c. If the LUN name uses uppercase or non-ASCII characters, rename the LUN from the filer console using the <code>lun move</code> command. d. Turn on space reservation.
7	Restart each node in the Windows cluster.
8	Using SnapDrive, connect to the renamed LUN as described in “ Connecting virtual disks ” on page 142.
9	Designate the renamed disk as the quorum using the Cluster Administrator on the owning node of your Windows cluster and recreate any dependencies recorded in Step 2 . For information about how to set a disk as a quorum, see your Windows documentation.
10	Delete the disk you created in Step 1 as described in “ Deleting a virtual disk ” on page 149.
11	Using SnapDrive, take a snapshot of the newly connected LUN as described in “ Creating snapshots ” on page 166.

Examining and modifying the Monitor Time Interval

What the Monitor Time Interval is: The Monitor Time Interval specifies how frequently SnapDrive monitors the snap reserve space on the filer volume for all virtual disks on the system. The default is every 60 minutes.

Guidelines for examining and modifying the Monitor Time Interval:

Keep the following in mind when examining and modifying the Monitor Time Interval:

- ◆ You can examine the Monitor Time Interval by using either the SnapDrive GUI in the Computer Management window or the sdcli.exe command-line interface.
- ◆ The Monitor Time Interval is global—any change you make to this property affects all virtual disks on a Windows host.

Examining and modifying the Monitor Time Interval: To examine or modify the Monitor Time Interval, complete the following steps.

Step	Action
1	Double-click SnapDrive in the left pane of the MMC, then select Disks.
2	Click Action (from the menu choices on top of the MMC), then select Properties. Result: The SnapDrive Properties panel with the Virtual Disk Monitor selected is displayed. Note_____ In earlier SnapDrive releases, the Virtual Disk Monitor tab was labeled Snapshot Monitor.

Step	Action
3	In the Virtual Disk Monitor panel, perform the following actions: ◆ Enter a value in the Monitor Time Interval field, in minutes. ◆ Click OK. The following values are valid: Default—60 minutes Minimum value—30 minutes Maximum value—10,080 minutes (7 days) Note_____ You can also set the Monitor Time Interval value to 0 minutes, which disables periodic snapshot monitoring; however, after configuring the value when you click OK, SnapDrive runs a one-time scan to obtain the current snap reserve space on the filer volume. Additionally, every time you click OK in the Virtual Disk Monitor panel, SnapDrive runs a scan to obtain the current snap reserve space on the filer volume. The scan is also run every time the SnapDrive service starts.

Administering SnapDrive remotely

Remote administration requirements: To run remote administration of SnapDrive, the remote Windows host must meet the following requirements:

The remote administration host machine must meet the same software requirements as the production host machine, except you do not need to install the virtual disk drivers. This entails the following specific requirements:

- ◆ The same version of SnapDrive that is installed on your production machine must be installed on your remote machine.
- ◆ When prompted during installation for the account used to access the filer, you must specify the same account used for access from the production host machine.

Running remote administration: To run remote administration, complete the following steps *from the remote administration machine* (not from the production host machine).

Note _____
Network Appliance recommends that you do not use a Terminal Service session to gain remote access to your virtual disks because you might have trouble viewing your virtual disks and certain types of error messages.

Step	Action
1	Select Computer Management, click Action from the menu choices on top of the MMC, and then select Connect to Another Computer. Result: The Select Computer panel is displayed.
2	In the Select Computer panel, browse to or select the host production machine you want to administer remotely. Result: The MMC window of the host machine appears on your remote machine, enabling you to manage SnapDrive remotely. Note _____ When using a Windows 2000 host to remotely administer SnapDrive on a Windows 2003 host, enter only the name of the host to which you want to connect rather than the fully qualified name. For example, enter lab-win2k1, not lab-win2k1.lab.netapp.com.

Enabling SnapDrive notification

SnapDrive enables you to set up email notification and enable filer AutoSupport in the event of a SnapDrive message or filer error. When you set up notification, you can specify the following information:

- ◆ Whether and where to send email notification
- ◆ What types of messages to report
- ◆ Whether to allow a subset of events to be posted to AutoSupport on the filer.

Note

To use filer AutoSupport with SnapDrive Notification Settings, you must enable AutoSupport on the filer. See your Data ONTAP documentation for information about how to enable AutoSupport.

Enabling SnapDrive notification: To enable email notification for selected SnapDrive events, complete the following steps.

Step	Action
1	Select SnapDrive, click Action from the menu choices on top of the MMC, and then select Notification Settings. Result: The Notification Settings panel is displayed.
2	In the Notification Settings panel, perform the following actions. a. Select Send Email Notification. b. Enter the outgoing SMTP server, and the From and the To addresses. c. Select one or more Event Types about which you want to be notified. d. Select the Event Category items about which you want to be notified when the specified event types take place. e. Select Use Filer AutoSupport if you want to enable a subset of the Windows System Events for AutoSupport on the filer. f. Click OK.

Step	Action
3	You can verify the email output of the Event Notification feature by clicking Send a Test Email on the Notification Settings panel.

The topics that follow describe how to use the SnapDrive Snapshot feature to create snapshots for backing up and restoring data, and they also provide an overview of the methods and media you can use to archive your virtual disk snapshots to tape or other offline media. (For detailed instructions, see the documentation for the archiving application you use.)

Go to any of the following topics for more information.

- ◆ [“How snapshots work”](#) on page 164
- ◆ [“Creating snapshots”](#) on page 166
- ◆ [“Connecting to LUNs in a snapshot”](#) on page 172
- ◆ [“Restoring virtual disks from snapshots”](#) on page 176
- ◆ [“Deleting snapshots”](#) on page 178
- ◆ [“Overview of archiving and restoring snapshots”](#) on page 180

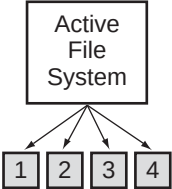
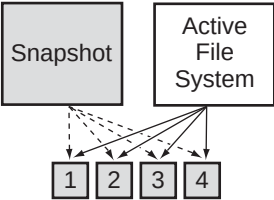
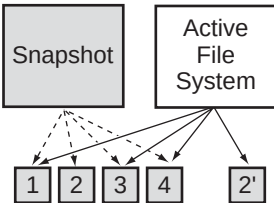
How snapshots work

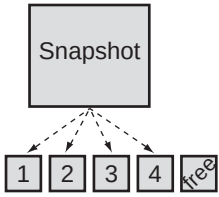
What a snapshot is: A snapshot is a point-in-time, read-only image of the filer volume. Snapshots can restore your databases rapidly if you encounter data corruption or other problems.

Because snapshots reside on disk instead of tape, this technology complements conventional backup processes. Snapshots do not physically replicate the data on your disks, and therefore, they are not intended to replace conventional procedures for archiving to tape or other offline media.

“[Example: How snapshots work](#)” on page 164 provides an illustration.

Example: How snapshots work

Before snapshot 	The file depicted at left spans four disk blocks in the active file system. Block pointers maintained by the active file system point to each of the data blocks.
After snapshot 	When you take a snapshot of the active file, the snapshot and active file system versions match, because their block pointers specify the same four blocks. Except for the relatively insignificant space necessary to store the snapshot block pointers, the snapshot consumes no disk space beyond that already used by the active file system.
After block update 	When you modify one of the four blocks, the new data cannot overwrite the original block, because that block is still needed as part of the snapshot. So the new data is written to a new block, and the active file system block pointers are updated so that they now reference the three original blocks, which have not changed, plus the new block. The snapshot block pointers continue to reference the original four blocks.

After file delete  The diagram shows a gray box labeled "Snapshot" at the top. Below it are five small boxes labeled "1", "2", "3", "4", and "free". Dashed arrows point from the "Snapshot" box to each of the five boxes below it.	When you delete the file, the blocks holding its data are no longer used by the active file system, but the snapshot still needs the blocks to which it points. Any blocks not used by any file or any snapshot are freed for reuse.
After snapshot delete  The diagram shows five small boxes, each labeled "free", arranged in a horizontal row.	The remaining three blocks containing data from the file are freed for reuse only when all snapshots that reference them have been deleted.

Creating snapshots

Reasons for creating snapshots using SnapDrive: Snapshot operations on a single virtual disk actually take a snapshot of all the virtual disks on the volume. Because a filer volume can contain virtual disks from multiple hosts, the only consistent virtual disks are those connected to the host that created the SnapDrive snapshot. In other words, within a snapshot, a virtual disk is not consistent if it is connected to any host other than the one that initiated the snapshot. (This is why Network Appliance recommends that you dedicate your filer volumes to individual hosts.) Therefore, it is important to back up a virtual disk using a SnapDrive snapshot rather than using other means, such as creating snapshots from the filer console.

Note

If you use the SnapManager product to manage your database, you must use SnapManager to create snapshots instead of SnapDrive. For more information about using SnapManager to create snapshots, see the current *SnapManager Installation and Administration Guide* for your product.

Additionally, as part of the SnapDrive snapshot process, the file system (NTFS) is flushed to disk and the disk image in the snapshot is in a consistent state. This consistency cannot be ensured if the snapshot was created outside the control of SnapDrive (that is, at the filer console, or using the FilerView interface or rsh, or by backing up the virtual disk file in the active file system.)

Restrictions on snapshot creation: You need to be aware of the following facts about SnapDrive and snapshots:

- ◆ You can keep a maximum of 255 snapshots with Data ONTAP 6.5.4 and later.
After the number of snapshots has reached the limit, the Snapshot Create operation fails, and you must delete some of the old snapshots before you can create any more.
- ◆ SnapDrive does not support snapshots that are created from the filer console, because such a practice can lead to inconsistencies within the NTFS file system. Therefore, use only SnapDrive to create snapshots of virtual disks.
- ◆ SnapDrive does not support creation of snapshots on bootable virtual disks.
- ◆ You cannot create a snapshot of a LUN connected to a snapshot. For more information, see “[Snapshot cautions](#)” on page 172.

- ◆ SnapDrive automatically turns off the snapshot schedule on a filer volume that stores virtual disks, so that the filer does not create automatic snapshots.

Note

Any snapshots inadvertently taken at the filer console or through FilerView are dimmed (unavailable) in the SnapDrive plug-in and are not usable by SnapDrive.

Snapshot requirements: The following requirements must be met:

- ◆ You must create snapshots through the SnapDrive MMC snap-in or through `sdcli.exe`, rather than the filer console or the volume snapshot schedule on the filer. This is because SnapDrive must first flush NTFS so that the virtual disk is consistent at the moment the snapshot is taken. This ensures the usability of the virtual disk file in the snapshot directory.
- ◆ You must create separate SnapDrive snapshot schedules for each volume that contains virtual disks.
- ◆ Snapshot names must be created using ASCII characters only, even when using non-ASCII operating systems.

SnapDrive limitation: The SnapDrive service can perform only one task at a time. If you schedule multiple tasks to start at exactly the same time, only the first will succeed; the others will fail.

For more information: The following topics provide instructions on using SnapDrive to create a snapshot:

- ◆ [“Creating a snapshot”](#) on page 168
- ◆ [“Scheduling snapshots”](#) on page 169

Creating a snapshot To create a snapshot using SnapDrive, complete the following steps.

Step	Action
1	Perform the following actions to get to the Create Snapshot menu item: a. Expand the Storage option in the left pane of the MMC, if it is not expanded already. b. Double-click SnapDrive. c. Double-click Disks. d. Double-click the disk for which you want to create a snapshot. e. Select Snapshots. f. Click Action (from the menu choices on top of the MMC). g. Select Create Snapshot from the drop-down menu. Result: The Create Snapshot text box is displayed.

Step	Action
2	In the Create Snapshot text box, perform the following actions: a. Enter an easy-to-interpret name for the snapshot. For example, expenses_db_15Jan03_4pm. Note _____ Snapshot names must be created using ASCII characters only, even when using non-ASCII operating systems. b. Click OK. Result: Your snapshot is created under the following directory on the filer: <i>\\Filer Name\Share Name\~snapshot\snapshot name</i> <i>Filer Name</i> is the (NetBIOS) name of the filer on which the virtual disk exists. <i>Share Name</i> is the name of CIFS share on the filer. <i>snapshot name</i> is the name of the snapshot. Information about the snapshot also appears in the right panel of the MMC in a list with all the other previous snapshots for that virtual disk.

Scheduling snapshots

Make sure that you have read the snapshot requirements described in “[Snapshot requirements](#)” on page 167 before you follow this procedure.

To schedule SnapDrive snapshots, complete the following steps.

Note _____
All steps except Step 1 in the following procedure are performed using the Scheduled Task Wizard, a Windows task scheduling tool available on your Windows server.

Step	Action
1	Create a batch file (a file with a .bat extension) containing the following command on the Windows host on which you are scheduling snapshots: <pre>sdcli snap create [-m MachineName] -s SnapshotName -D DriveLetterList [. . .] [-x]</pre> <i>MachineName</i> is the name of the Windows host on which the command will be executed. If no machine name is specified, the command is executed on the local machine. <i>SnapshotName</i> is the name of the snapshot to be created. <i>DriveLetterList</i> is a list of space-separated drive letters. When <i>-x</i> flag is specified, snapshots are created only for the drives specified by the <i>-D</i> flag. Otherwise, snapshots are created for all the disks on the filer volumes used by the listed drives. Example: <code>sdcli snap create -s Jun_13_03 -D j k l</code> The preceding example creates a snapshot named Jun_13_03 for each volume containing one or more of the virtual disks mapped to the specified drives (that is, J:, K:, and L:). The snapshots created are consistent for all virtual disks contained by those volumes.
2	Select Start Menu > Settings > Control Panel > Scheduled Tasks.
3	Double-click Add Scheduled Task. Result: The Scheduled Task Wizard is launched.
4	In the Scheduled Task Wizard appears, click Next.
5	After the next panel appears, click Browse, and navigate to the folder where the batch (.bat) file you created in Step 1 is located.
6	Select the batch file.
7	After the following panel appears, select from the list of frequencies, then click Next.

Step	Action
8	After the following panel appears, enter a start time and complete the detailed frequency parameters. The option details displayed on this panel vary depending on the snapshot frequency you picked in the previous panel.
9	In the following panel, type the user name (the administrator account name and password, repeated for confirmation), then click Next.

Note

Scheduling is not limited to snapshot creation. You can use the Windows task scheduler to execute any of the sdcli.exe options, or even run a batch file containing numerous command operations.

Connecting to LUNs in a snapshot

About read/write connections: You can connect a host to a LUN in a snapshot in read/write mode. (This is useful for conducting tests, for example.)

Such a read/write connection to a virtual disk in a snapshot is actually a connection to a special type of virtual disk with the following properties:

- ◆ It is backed by a virtual disk in a snapshot.
- ◆ It resides in the active file system and always has an .rws extension.
- ◆ When the host reads data from this virtual disk, it receives data that is in the virtual disk that is in the snapshot.
- ◆ When the host writes data to this virtual disk, the data is written to the virtual disk with the .rws extension.
- ◆ When the host reads data that has been written to the LUN with the .rws extension, that data is received from the virtual disk with the .rws extension.

For details, see your Data ONTAP documentation.

Disk space implications: Connecting to a LUN in a snapshot does not in itself consume any additional disk space on the filer volume. You consume additional space only as you write to the .rws file.

Note

Connecting to a LUN in a snapshot works well for temporary needs such as testing. If you want to make the connection permanent, consider making a copy of the original LUN. This new LUN, like any other, will require additional space in the volume as outlined under “[Volume-size rules](#)” on page 15.

Snapshot cautions: Keep the following points in mind when working with snapshots and virtual disks that are backed up by a snapshot:

- ◆ Information written to the .rws file is temporary; SnapDrive deletes the .rws file when you disconnect.
- ◆ You cannot merge the data written to the .rws file with the data in the snapshot referenced by the .rws file.
- ◆ You cannot delete a snapshot that is in use by a virtual disk backed by a snapshot.
- ◆ You can connect to the virtual disk snapshot only by using read/write mode and a virtual disk that is backed by a snapshot.
- ◆ You should avoid creating a snapshot of a virtual disk backed by a snapshot. Doing so will lock the snapshot backing the virtual disk until the newer snapshot—and all snapshots of that virtual disk—are deleted. For more

information about deleting a locked snapshot, see “[Problems deleting snapshots due to busy snapshot error](#)” on page 179.

For instructions on connecting to a LUN in a snapshot, see “[Connecting to a virtual disk \(LUN\) in a snapshot](#)” on page 173.

Connecting to a virtual disk (LUN) in a snapshot

To connect to a virtual disk (LUN) in a snapshot using SnapDrive, complete the following steps.

Caution

This version of SnapDrive is not aware of the Data ONTAP LUN cloning feature. Therefore, do not use the LUN cloning feature to clone a virtual disk backed by a snapshot that is connected using SnapDrive. SnapDrive considers such a disk to be temporary, and it deletes the disk upon disconnect.

Step	Action
1	Perform the following actions to launch the Connect Disk wizard: a. Expand the Storage option in the left pane of the MMC, if it is not expanded already. b. Double-click SnapDrive in the left pane of the MMC. c. Select Disks. d. Click Action (from the menu choices on top of the MMC). e. Select Connect Disk from the drop-down menu.
2	In the Connect Disk Wizard, click Next.

Step	Action
3	In the Provide Virtual Disk Location panel, perform the following actions. a. Click Browse to browse to the \~snapshot directory of the filer volume holding the snapshot of the virtual disk. b. Select a virtual disk file (with a .lun extension). c. Click Next. Result: The Select a Virtual Disk Type panel is displayed. Note _____ If you cannot see the snapshot directory, make sure that <code>cifs.show_snapshot</code> is set to On and <code>vol option nosnapdir</code> is set to No on your filer.
4	In the Select a Virtual Disk Type panel, Dedicated is automatically selected because a snapshot can be connected only as a dedicated virtual disk. Click Next. Result: The Virtual Disk Snapshot Information panel is displayed.
5	In the Virtual Disk Snapshot Information panel, a path is automatically specified where a temporary read-write virtual disk is created when you connect to the disk backed up by the snapshot. Click Next. Result: The Select Virtual Disk Drive Letter panel is displayed.
6	In the Select Virtual Disk Drive Letter panel, perform the following actions. a. Select from the list of available drive letters for the virtual disk you are creating. b. Click Next. Result: The Select Initiators panel is displayed.

Step	Action
7	In the Select Initiators panel, perform the following actions. a. Select the FCP or iSCSI initiator for the virtual disk you are creating and use the arrows to move it back and forth between the Available Initiators and Selected Initiators list. b. Click Next. Result: The Completing the Connect Disk Wizard panel is displayed.
8	In the Completing the Connect Disk Wizard panel, perform the following actions. a. Verify all the settings. b. If you need to change any settings, click Back to go back to the previous Wizard panels. c. Click Finish. Result: The MMC is displayed with the newly connected virtual disk now appearing under SnapDrive > Disks in the left panel.

Restoring virtual disks from snapshots

When you restore a virtual disk from a snapshot, the virtual disk reverts to the state it was in when the snapshot was taken: the restore operation overwrites all data written to the virtual disk since the snapshot was taken.

A virtual disk restore recalls a selected snapshot. During a restore, the entire virtual disk drive is restored from the snapshot. For a restore to succeed, no open connections can exist between the host machine (or any other application) and the files in the virtual disk.

If you expand the virtual disk and then restore it from a snapshot taken prior to that expansion, the restored virtual disk reverts to its size at the moment the snapshot was taken.

Note

If your host is running Windows 2003 and you need to restore an expanded disk from a snapshot, you should use a snapshot that was created after the virtual disk was expanded. SnapDrive does not allow you to restore a virtual disk from a snapshot that was taken before the disk was expanded. If you need to do this, you must disconnect the disk using SnapDrive, then restore the disk from the filer console using the `snap restore` command. For more information, see the *Data Protection Online Backup and Recovery Guide*. When the virtual disk is restored, reconnect the disk using SnapDrive.

For instructions on restoring a virtual disk from a snapshot, go to “[Restoring a virtual disk from a snapshot](#)” on page 176.

Restoring a virtual disk from a snapshot

To restore a virtual disk from a snapshot, complete the following steps.

Step	Action
1	Shut down all resources directly or indirectly dependent on the virtual disk. Make sure that the virtual disk is not being used by the Windows file system or any other process, and that no user has the virtual disk open in Windows Explorer. Shut down any application that is using the virtual disk. Caution_____ Make sure that the Windows Performance Monitor (perfmon) is not monitoring the virtual disk. _____
2	Perform the following actions: a. Expand the Storage option in the left pane of the MMC, if it is not expanded already. b. Double-click SnapDrive in the left pane of the MMC. c. Double-click Disks. d. Select the virtual disk that you want to restore.
3	In the right pane of the MMC, perform the following actions: a. Right-click the specific snapshot you want to restore. b. Select Restore Disk From Snapshot from the drop-down menu. Note_____ You can only restore a snapshot that is consistent with the active file system. Inconsistent snapshots are not available for restoration. _____
4	In the Restore Snapshot panel, click Yes to restore the snapshot you selected. Caution_____ Do not attempt to manage any Windows cluster resources while the restore is in progress. _____

Deleting snapshots

- Reasons to delete snapshots:** Delete older snapshots for the following reasons:
- ◆ To keep the number of stored snapshots less than the hard limit of 255 for Data ONTAP
Be sure to delete old snapshots before the hard limit is reached; otherwise, subsequent snapshots could fail.
 - ◆ To free up space on the filer volume
Even before the snapshot limit is reached, a snapshot fails if insufficient reserved space for it remains on the disk.

For instructions for deleting a snapshot, see “[Deleting a snapshot](#)” on page 178.

Deleting a snapshot To delete a snapshot, complete the following steps.

Note—
You must make sure that the virtual disk whose snapshot you want to delete is not being monitored with the Windows Performance Monitor (perfmon).

Step	Action
1	Perform the following actions: a. Expand the Storage option in the left pane of the MMC, if it is not expanded already. b. Double-click SnapDrive in the left pane of the MMC. c. Double-click Disks. d. Select the virtual disk whose snapshot you want to delete.
2	In the right pane of the MMC, select the snapshot you want to delete. Note — You can only delete a snapshot that is consistent with the active file system. Inconsistent snapshots are not available for deletion.
3	Click Action (from the menu choices on top of the MMC).

Step	Action
4	Select Delete from the drop-down menu.
5	In the Delete Snapshot panel, click Yes to delete the snapshot you selected. Note_____ If you get an error message stating that the snapshot is busy or cannot be deleted, it is likely that the snapshot is in use by a virtual disk that is backed by a snapshot. For more information, see “Problems deleting snapshots due to busy snapshot error” on page 179

Problems deleting snapshots due to busy snapshot error

If you attempt to delete a snapshot and you get an error message saying that the snapshot is busy and cannot be deleted, you either have a snapshot that was taken of a LUN backed by another snapshot or the snapshot backed LUN is still connected. In the first instance, you need to delete the newer snapshot before the older snapshot, the snapshot backing the LUN, can be deleted. If the LUN backed by a snapshot is still connected, disconnect it.

To see if you have busy snapshots, you can view your application event log in the Event Viewer to check for messages related to busy snapshots. For more information about deleting busy snapshots, see the *Block Access Management Guide* for your version of Data ONTAP.

Overview of archiving and restoring snapshots

A good way to protect and retain data is to archive the SnapDrive snapshots of the virtual disks (LUNs) to offline, offsite media, such as NetApp NearStore® technology or alternate storage methods. This practice is particularly beneficial for disaster recovery.

What to back up: When archiving backups, it is important that you select the virtual disks that are *not* in the active file system. The disks in the active file system are not consistent and, therefore, will not result in reliable backups. You must also select the *snapshots* of the virtual disks when creating backups.

Ways to archive SnapDrive backups: You can use the Data ONTAP `dump` command or an NDMP-based backup application to archive the snapshots your virtual disks (LUNs).

Note

You cannot use CIFS-based or NFS-based backup products to archive the snapshots of your virtual disks (LUNs).

Process for restoring virtual disks from archival media: First, restore the virtual disk file from your archive media to the active file system. After the file is restored, use the SnapDrive management interface to connect to the virtual disk file using its original drive letter.

For more information about virtual disk (LUN) backups, see the Data ONTAP *Block Access Management Guide*. For more information about how to perform a recovery from an offline archive, see your backup application software documentation.

Note

Further steps might be required to bring online data recovered in virtual disk files. This holds true for all SnapManager products. For more information about recovering virtual disks using SnapManager, see the current *SnapManager System Administrator's Guide* for your product.

What Volume Shadow Copy Service is

Microsoft® Volume Shadow Copy Service (VSS) is a new feature of Microsoft Windows® Server 2003 that coordinates among data servers, backup applications, and storage management software to support the creation and management of consistent backups. These backups are called shadow copies, or snapshots.

VSS requirements

In order to use VSS with SnapDrive 3.2, VSS requires the following:

- ◆ Your filer must be running at least Data ONTAP 6.5.4.
- ◆ The Virtual Disk Service must be running on your Windows 2003 host.

Overview of VSS

VSS coordinates snapshot-based backup and restore. VSS includes these four components:

- ◆ Volume Shadow Copy Service (VSS)
Volume Shadow Copy Service is the Windows Server 2003 service that coordinates among the other components to provide snapshot-based backups and restores.
- ◆ VSS requestor
The VSS requestor is a backup application, such as the SnapManager 3.0 for Microsoft Exchange application or NTBackup. It initiates VSS backup and restore operations. The requestor also specifies snapshot attributes for backups it initiates.
- ◆ VSS writer
The VSS writer owns and manages the data to be captured in the snapshot. Microsoft Exchange 2003 is an example of a VSS writer.
- ◆ VSS provider
The VSS provider is responsible for the creation and management of the snapshot. A provider can be either a hardware provider or a software provider.
 - ❖ A hardware provider integrates storage array-specific snapshot and cloning functionality into the VSS framework. NetApp VSS Hardware Provider is a VSS hardware provider; it integrates the SnapDrive service and NetApp filers into the VSS framework.

Note

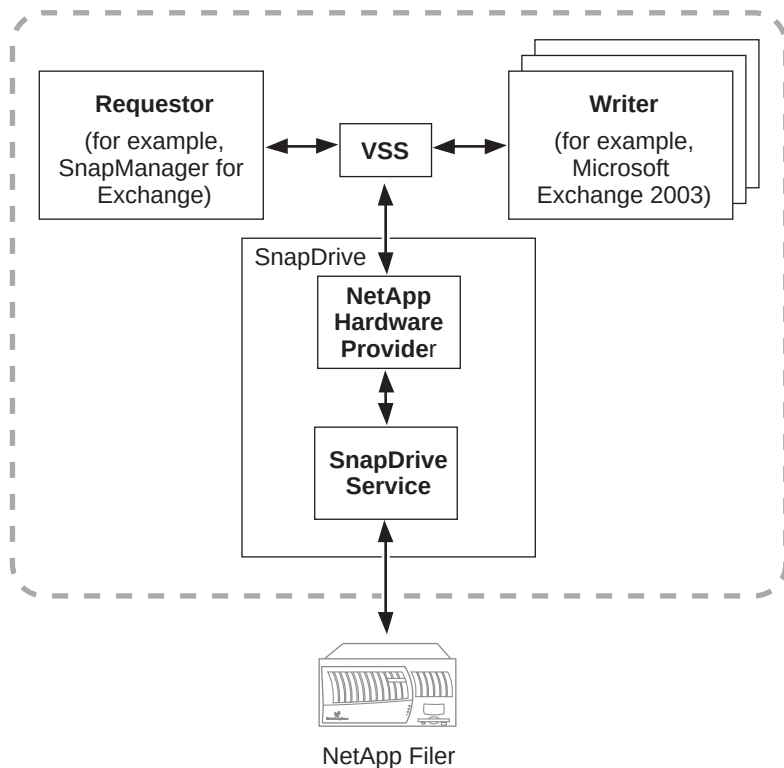
NetApp VSS Hardware Provider is installed automatically as part of the SnapDrive 3.2 software installation.

- ❖ A software provider implements snapshot or cloning functionality in software that is running on the Windows system.

Note

To ensure the NetApp Hardware Provider works properly, do not use the VSS software provider on NetApp LUNs. If you use the VSS software provider to create snapshots on a NetApp LUN, you will be unable to delete that LUN using the VSS hardware provider.

The following figure shows how the modules communicate through VSS.



Typical VSS backup process

A typical backup using SnapManager 3.0 for Exchange, Exchange 2003, and NetApp VSS Hardware Provider is outlined in the following process:

1. SnapManager determines what LUNs it wants to capture and makes sure that Exchange 2003 is present as a valid writer.
2. SnapManager initiates the shadow copy process.
3. VSS informs Exchange 2003 and NetApp VSS Hardware Provider that a shadow copy is starting. Exchange stops writing to disk.
4. VSS ensures that NTFS is in a consistent state.
5. VSS requests NetApp VSS Hardware Provider to create a shadow copy.
6. NetApp VSS Hardware Provider requests SnapDrive to create a snapshot of the filer volume that contains the specified LUN.
7. SnapDrive requests the filer to create a snapshot of the specified volume.
8. When the shadow copy is complete, VSS returns NTFS to a normal state and informs Exchange 2003 that it can resume disk writes.
9. VSS manages the shadow copy of the LUN based on the attributes specified by the requestor. For example, VSS could mount the LUN in snapshot. In the case, however, where SnapManager is the requestor, SnapManager tells VSS to forget about the shadow copy it just created. This enables SnapManager to have complete control of the snapshot.

Troubleshooting the NetApp VSS Hardware Provider

NetApp VSS Hardware Provider requirement

When you use a VSS requestor, such as SnapManager 3.0 for Exchange or NTBackup, to back up a LUN backed by a NetApp storage appliance, NetApp VSS Hardware Provider must be used for the snapshot to succeed.

Multiple providers installed

There can be many providers installed on the same Windows host, including the VSS software provider, which is always installed. The provider used is determined by either the Requestor or VSS, not the provider. If the first choice provider is not available, an alternative can be silently substituted.

To take a snapshot on the filer, NetApp VSS Hardware Provider must be used. If a snapshot on the filer is not created successfully, verify that NetApp VSS Hardware Provider was used to create the snapshot.

Only NetApp VSS Hardware Provider can take a snapshot on a NetApp storage appliance.

Viewing installed VSS providers

To view the VSS providers installed on your host, complete the following steps.

Step	Action
1	Select Start > Run and enter the following command to open a Windows command prompt: <code>cmd</code>
2	At the prompt, enter the following command: <code>vssadmin list providers</code> Result: The output should be similar to this example: Provider name: 'NetApp VSS Hardware Provider' Provider type: Hardware Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102} Version: 1.0.0.0

Troubleshooting when a snapshot is not taken on the filer

If you attempt to create a backup on a NetApp filer and a snapshot is not created on the filer, complete the following steps.

Step	Action
1	Verify that NetApp VSS Hardware Provider was used to create the snapshot and that it was completed successfully. For details, see “Verifying that NetApp VSS Hardware Provider was used successfully” on page 185.
2	If NetApp VSS Hardware Provider was not used or failed to create the snapshot successfully, verify your VSS configuration. For details, see “Verifying your NetApp VSS configuration” on page 186. Note_____ The VSS auto recovery feature is not supported in this release and VSS snapshot requests are rejected if this option is enabled. When the VSS auto recovery feature is enabled or if auto recovery is set on SQL Server 2005 or similar applications, snapshot requests fail and the Application Event Log reports the error “NetApp VSS hardware provider does not support this context. Please check AutoRecovery option, which is currently NOT supported.”

Verifying that NetApp VSS Hardware Provider was used successfully

To verify that NetApp VSS Hardware Provider was used successfully after a snapshot was taken, complete the following step.

Step	Action		
1	Open the Application Event Viewer in the MMC console and look for an event with the following values:		
	Source	Event ID	Description
	Navssprv	4098	Netapp VSS provider has successfully completed CommitSnapshots for SnapshotSetId <id> in <n> milliseconds.

Note

VSS requires that the provider initiate a snapshot within 10 seconds. If this time limit is exceeded, the NetApp VSS Hardware Provider logs Event ID 4364. This limit could be exceeded due to a transient problem. If this event is logged for a failed backup, retry the backup.

**Verifying your
NetApp VSS
configuration**

If NetApp VSS Hardware Provider failed to run, or did not successfully complete a snapshot, complete the following steps.

Step	Action
1	Verify that SnapDrive is installed and running, and can communicate with the filer. To do this, complete the following steps: a. Open the MMC and select the Disks icon under Snapdrive. b. Select Action > Refresh. No error messages should be displayed.
2	Verify that the drives for which NetApp VSS Hardware Provider failed are backed by a LUN on a NetApp storage appliance. To do this, open the MMC and verify that the drives appear under the Disks icon under SnapDrive.

Step	Action
3	Verify that the account used by NetApp VSS Hardware Provider is the same as the account used by SnapDrive. To do this, complete the following steps: a. In the MMC left pane, select Services and Applications > Services. b. Double-click the SnapDrive service in the right pane and select the Log On tab. c. Note the account listed in the This Account field. d. Double-click the NetApp VSS Hardware Provider service in the right pane and select the Log On tab. e. Verify that the This Account field is selected, and that it contains the same account as the SnapDrive service.

Feature availability

If you did not license and install the MPIO module, these features are not available to you in SnapDrive.

If you licensed and installed only the MPIO module and you did not install LUN Provisioning and Snapshot Management, you cannot use SnapDrive to create and manage LUNs. To create and manage LUNs with only the MPIO module installed, use FilerView or the `filer lun` command. For more information, see the *Data ONTAP Block Access Management Guide for FCP* or the *Block Access Management Guide for iSCSI*.

Note

When mapping and unmapping LUNs using FilerView or the `filer lun` command in an MPIO-only installation, SnapDrive does not recognize that the LUNs have been mapped or unmapped. To update drive mappings in SnapDrive, you must use Disk Management to rescan disks on your host then refresh SnapDrive.

The topics that follow explain how SnapDrive implements multipathing to connect hosts to virtual disks (LUNs).

Go to any of the following topics for more information:

- ◆ [“Multipathing overview”](#) on page 190
- ◆ [“MPIO setup”](#) on page 193
- ◆ [“MPIO path management”](#) on page 198

Related topics:

- ◆ [“Multipathing commands”](#) on page 238 lists MPIO-related commands (and associated parameters) that run under `sdcli.exe`, the SnapDrive command-line utility.
- ◆ [“MPIO configurations”](#) on page 33 describes supported MPIO configurations.

Multipathing overview

What multipathing does: Multipathing uses redundant paths between a Windows host and a virtual disk, thus eliminating the “single point of failure” vulnerability that exists when a host connects to a filer across a single, fixed physical path.

SnapDrive multipathing establishes two physical paths between the host and the virtual disk (LUN). One of the paths is designated active and the other one passive (standby). If the active physical path fails, the passive (standby) path takes over and continues to maintain connectivity between the host and the virtual disk.

How SnapDrive implements multipathing: SnapDrive facilitates multipath redundancy by integrating a NetApp device-specific module (ntapdsm.sys) with a trio of Microsoft software drivers (mpio.sys, mpdev.sys, and mspspfltr.sys). This multipathing solution, which this document refers to as “MPIO,” is managed through the SnapDrive plug-in under the MMC or the sdcli.exe command-line utility.

Related topic:

- ◆ [“SnapDrive MPIO features and requirements”](#) on page 191.

SnapDrive MPIO features and requirements

SnapDrive supports MPIO on systems configured according to the conditions set forth in the following table.

Component	Supported configurations
Operating system on host	Windows 2000 Server ◆ Advanced Server is required for Windows cluster configurations. ◆ Both Server and Advanced Server require Service Pack 4. Note _____ For more information, see “Understanding feature availability” on page 24. For a list of the latest service packs and hotfixes required by SnapDrive, see the SnapDrive 3.2 Description Page at http://now.netapp.com/NOW/cgi-bin/software/. OR Windows Server 2003 ◆ Enterprise Edition is required for Windows cluster configuration. Note _____ For more information, see “Understanding feature availability” on page 24. For a list of the latest service packs and hotfixes required by SnapDrive, see the SnapDrive 3.2 Description Page at http://now.netapp.com/NOW/cgi-bin/software/.
Disk-access protocol	FCP or iSCSI

Component	Supported configurations
Host clustering (optional)	Windows cluster. Host clustering using an FCP configuration also requires installation of the NetApp Dual HBA FCP Attach Kit for Windows on each Windows cluster node. Host clustering using an iSCSI configuration requires the installation of at least two GbE NICs and the Microsoft iSCSI Software Initiator or two iSCSI HBAs on each Windows cluster node. For a list of the latest supported iSCSI HBAs, see the SnapDrive Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/. Note——— MPIO with iSCSI is not supported on Windows 2000 clusters.
Operating system on filer	Data ONTAP 6.5.4 (minimum)
Filer clustering (optional)	NetApp filer clusters

Related topic:

- ◆ “[Supported MPIO topologies](#)” on page 193.

MPIO setup

Installation assumptions: This section assumes that you successfully licensed and installed the MPIO module on a supported hardware-and-software configuration. For a complete list of requirements for MPIO, see “[SnapDrive MPIO features and requirements](#)” on page 191.

How MPIO features become available: When you create a virtual disk (LUN) on a Windows host with MPIO installed, you select the initiators that will be part of the MPIO setup on a Windows host just as you select the initiators when creating a virtual disk, as described in “[Creating a virtual disk](#)” on page 123. For Windows clusters, you specify an initiator for each Windows node in the cluster, as described in “[Creating a virtual disk](#)” on page 123.

After you have successfully created the LUN, the multipath management features become available.

Note

When connecting MPIO paths over different networks, whether public or private, NetApp recommends that each network be attached to a domain controller. The domain controller is necessary for user authentication.

Related topics:

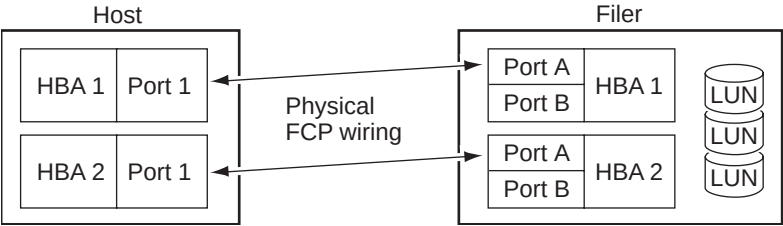
- ◆ “[SnapDrive MPIO features and requirements](#)” on page 191
- ◆ “[Supported MPIO topologies](#)” on page 193

Supported MPIO topologies

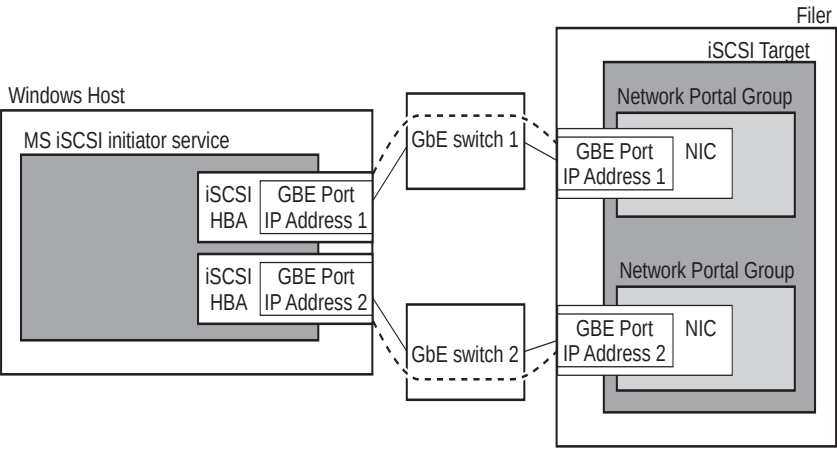
MPIO configurations consist of three basic sets of physical components:

- ◆ Host (a single node or a Windows cluster pair)
- ◆ Switch (two per configuration provides maximum protection for filer clusters. Switches are not used in direct attached configurations.)
- ◆ Filer (a single appliance or a filer cluster pair)

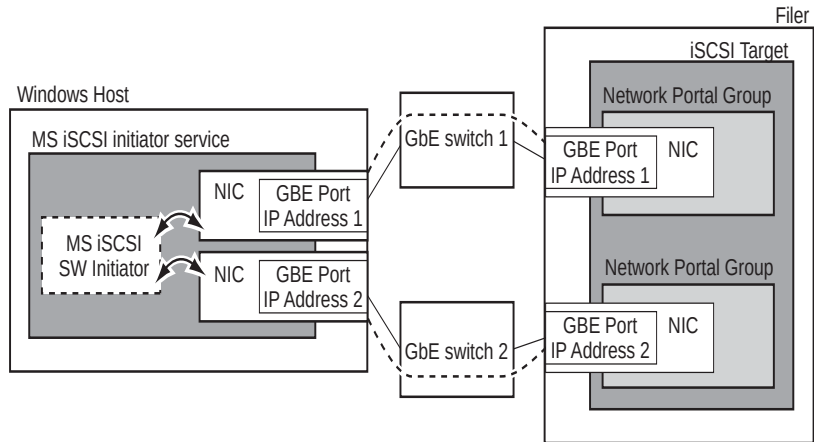
Single host direct-attached to a single filer using FCP: The following diagram shows a pair of FCP crossover cables used to support MPIO between a single host and a single filer. If the active path fails, MPIO routes data across the passive (standby) path. The host has two HBAs and the filer has two HBAs.



Single host connected to a single filer through switches using iSCSI: The following diagram shows iSCSI being used to support MPIO between a single host, a single filer, and a pair of GbE switches. The host has two iSCSI HBAs and the filer has two GbE network interfaces.



The following diagram shows iSCSI being used to support MPIO between a single host, a single filer, and a pair of GbE switches. The host has two GbE network interface with a Microsoft iSCSI Software Initiator and the filer has two GbE network interfaces.

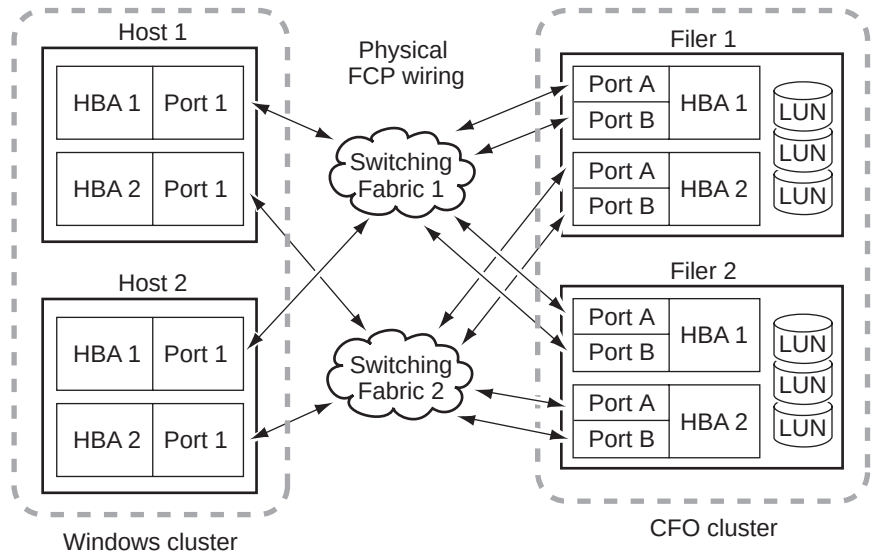


Windows cluster connected to a filer cluster using FCP through switches: One setup offering maximum protection against a single point of failure consists of a Windows cluster, a pair of FCP switches, and a filer cluster.

In the following illustration, the HBAs in the hosts have one port each. The filers are equipped with HBAs that each have a pair of ports.

Note

Ports belonging to the same HBA always connect to the *same* switch. HBAs belonging to the same filer connect to *different* switches.

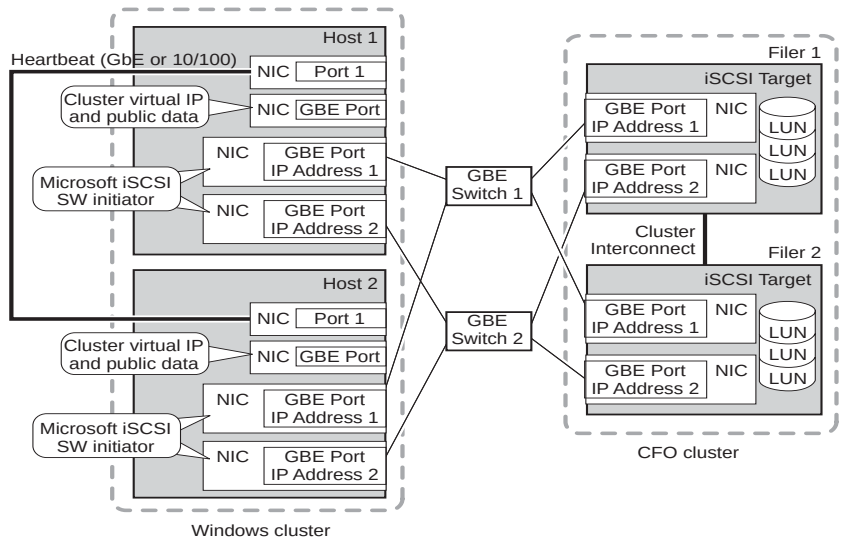


Windows cluster connected to a filer cluster using iSCSI through switches: Another configuration offering maximum protection against a single point of failure consists of a Windows cluster, a pair of GbE switches, and a filer cluster.

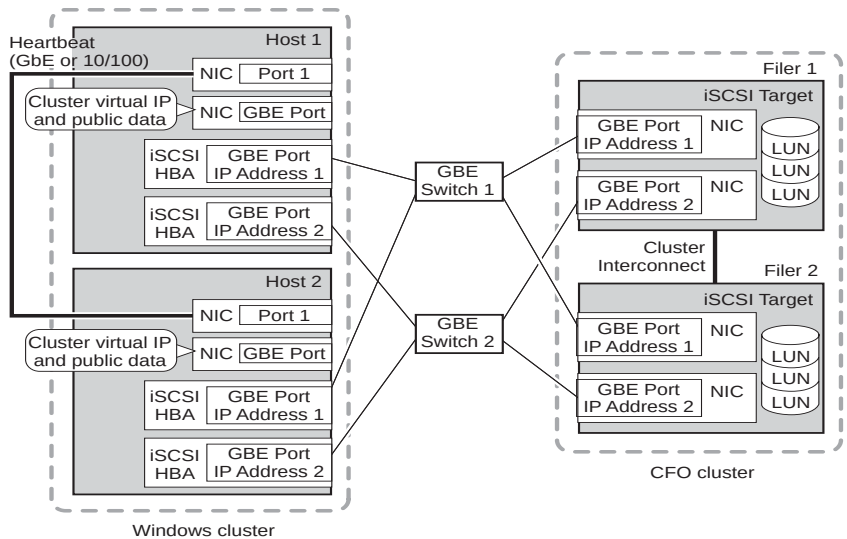
In this type of configuration, NetApp recommends using a total of four NICs, each on different subnets, as follows:

- ◆ One NIC (GbE or 10/100) for private intercluster communication (heartbeat)
- ◆ One NIC (GbE or Fast Ethernet) for the cluster virtual IP and public data
- ◆ Two NICs (GbE or iSCSI HBAs) for iSCSI connections to the target

The following diagram shows the Microsoft iSCSI Initiator being used in an MPIO configuration between a Microsoft cluster, a pair of GbE switches, and a filer cluster.



The following diagram shows iSCSI HBAs being used in an MPIO configuration between a Microsoft cluster, a pair of GbE switches, and a filer cluster.



MPIO path management

Accessing MPIO functionality: As the following table indicates, SnapDrive supports three GUI methods and two command-line methods for manipulating MPIO paths.

Note_____

All GUI details correspond to the Computer Management Console. All command-line details correspond to the “cmd.exe session window.”

Interface	Method	How to access	
GUI	Main menu bar	Select Action > Path Management.	
GUI	Tool bar	Click the Path Management icon, which is pictured at right.	
GUI	Path Management icon in the left pane	Right-click the icon, then select Add/Remove Initiator. If you are using MPIO with iSCSI, you should have created at least two iSCSI sessions before performing this task. For more informantion, see “Establishing an iSCSI session to a target” on page 113 Note_____ The Path Management option is not available if you did not license and install the LUN Provisioning and Snapshot Management module. To add or remove initiators with only the MPIO module installed, use FilerView or the <code>filer igroup add</code> or <code>igroup remove</code> commands. For more information, see the <i>Data ONTAP Block Access Administration Guide for FCP</i> or the <i>Block Access Administration Guide for iSCSI</i>.	

Interface	Method	How to access
Command line	Single command	Launch a cmd.exe window; navigate to the SnapDrive installation directory and enter a <code>sdcli.exe path</code> command at the prompt. Be sure to type input parameters in the correct order and include all necessary switch information. For individual command details, see “Multipathing commands” on page 238.
Command line	Automation script	Launch a cmd.exe window; enter the path and name of the script to be run. Note— When scheduling the batch file through the Windows Task Scheduler, specify a “Log on as” user account that has appropriate host, filer, and domain access permissions. For example, a properly configured SnapDrive service account has all necessary accesses enabled.

Related topic:

- ◆ [“Creating an MPIO path”](#) on page 199

Creating an MPIO path

The following procedure shows how to use one of the GUI methods to create an MPIO path. Specifically, the procedure involves mapping a target (a LUN) on the filer to an initiator (HBA port) on the host.

Note

If you are creating an MPIO path using iSCSI, before performing this procedure you must create a new iSCSI session to which to map the additional path. For more information, see [“Establishing an iSCSI session to a target”](#) on page 113.

Note

You can use this same basic procedure to unmap MPIO paths as well. See also [“Multipathing commands”](#) on page 238 for `sdcli.exe` commands that perform equivalent operations in a nongraphical environment.

Step	Action
1	In the Computer Management window, select Storage > SnapDrive. In the tree in the left pane, click the icon for the virtual disk whose MPIIO paths you want to manage.
2	After the Path Management icon appears on a branch beneath the virtual disk icon, right-click it. On the drop-down menu, select Add/Remove Initiator. Note This option is not available if you did not license and install the LUN Provisioning and Snapshot Management module. To add or remove initiators with only the MPIIO module installed, use FilerView or the <code>filer igroup add</code> or <code>igroup remove</code> commands. For more information, see the <i>Data ONTAP Block Access Administration Guide for FCP</i> or the <i>Block Access Administration Guide for iSCSI</i>.
3	If you are mapping MPIIO paths for a Windows cluster configuration using FCP, skip to Step 4. If you are mapping MPIIO paths for a single-host configuration, select an initiator from the Unused Initiator(s) box in the Initiators Management window, then click the right arrow to move it to the Connected Initiator(s) box. Click OK to complete the procedure.
4	To add MPIIO paths on a Windows cluster, select an initiator for node 1 from the Unused Initiator(s) box in the Initiators Management window, then click the right arrow to move it to the Mapped Initiator(s) box. Repeat this step for the other nodes in the cluster.

Understanding MPIIO path states

You can add, enable, activate, disable, or remove (delete) MPIIO paths. The disable option disables all paths that are mapped to a particular LUN.

When the Path Management icon for a particular virtual disk is selected in the left pane of the Computer Management window, the right pane shows five parameters for each path:

- ◆ State, which can be any one of the following:
 - ❖ Active: I/O traffic currently goes through this path.
 - ❖ Passive: The path is currently on standby.

- ❖ Disabled: No traffic can go through this path (which is useful for maintenance purposes, etc.).
- ❖ Failed: The path failed and has not been recovered.
- ❖ Pending Remove: The path is about to be removed, which is to say, destroyed (although it can be re-created later).
- ❖ Pending Add: The path is in the process of being created. (It changes to passive as soon as the process is complete.)

Note

If you have Data ONTAP proxy paths in partner mode on your filer, NetApp recommends that the proxy path not be made the active path.

- ◆ Initiator HBA Name, which is the name of the initiator installed on your host; for example Microsoft iSCSI Initiator.
- ◆ Initiator HBA Address, which is the network identifier for a port on an HBA in the host; for example, using FCP the address might be “10:00:00:00:cf:2e:4d:fe” or using iSCSI the address might be “10.64.67.99.”
- ◆ Target Adapter/Portal IP, which is the network identifier for an HBA in the filer; for example, using FCP the address might be “50:0a:09:8c:82:de:10:d2 Slot v.5a” or using iSCSI the address might be “10.64.67.100.”
- ◆ Proxy Path, which only applies when using FCP, can be one of the following:
 - ❖ Yes: The path is a proxy path. You will also see Proxy Path Yes if you are using cfmode with dual fabric FAS270C and partner FAS800 or FAS900.
 - ❖ No: The path is not a proxy path.

Related topic: ◆ [“Changing MPIO path states”](#) on page 201.

Changing MPIO path states

Not every multipath state-change command is available for all paths in every state. In the SnapDrive GUI, commands that are not available are dimmed in the drop-down menu that appears when you select a path and try to change its state. The `sdcli.exe` command returns an error if you try to perform a state-change command on a path that is currently in a state that doesn’t support such a change.

The following table shows what happens when you execute a path-change command on a path in a certain state. It also shows the effect of certain outside events on paths in various states.

GUI command, sdcli command, or other event	On	Result
sdcli path add Note _____ This option is not available if you did not license and install the LUN Provisioning and Snapshot Management module.	A LUN	A new path is created.
sdcli path activate	A passive path	The passive path becomes active (and the active path becomes passive).
sdcli path disable	A passive path	The path is disabled.
sdcli path enable	A disabled path	The path becomes passive.
sdcli path remove Note _____ This option is not available if you did not license and install the LUN Provisioning and Snapshot Management module.	Any active, passive, disabled, or failed path	The path is removed (deleted) and the path enters the Pending Remove state.
a cable is disconnected	Any active, passive, disabled, or failed path	The path enters the Pending Remove state.
a virtual disk times out (default = 190 seconds)	A path in the Pending Remove state	The path is deleted.

Removing MPIO on a Microsoft cluster

To remove the MPIO service and related drivers from your Windows MSCS hosts, complete the following steps.

Step	Action
1	Verify that all multipathed LUNs have been changed to single path.
2	On node 2, uninstall SnapDrive and reboot. Result: The cluster resources will move to node 1.
3	From the Cluster Administrator, perform a Move Group to move all resources from node 1 to node 2.
4	Uninstall SnapDrive on node 1 and reboot.

What SAN booting is

The term *SAN booting* means using a SAN-attached disk, such as a filer virtual disk (LUN), as a boot device for a SAN host. It also entails removing internal disks from the host so the host uses the SAN for all its storage needs.

SAN booting does not require support for special SCSI operations. It is not different from any other SCSI disk operations. The HBA has hooks into the BIOS, which enables the host to boot from a virtual disk on the filer.

After the HBA has accessed the BIOS, you use the BIOS boot utility to configure the virtual disk as a boot device. You then configure the PC BIOS to make the LUN the first disk device in the boot order. The following must be installed on the LUN:

- ◆ Windows 2000 or Windows 2003 operating system
- ◆ A driver for the FCP or iSCSI HBA

Note

Following a system failure, the bootable virtual disk may not remain the default boot device. In the event of a system failure, you may need to reconfigure the hard disk sequence in the system BIOS to set the bootable virtual disk as the default boot device.

How SnapDrive supports SAN booting

SnapDrive 3.2 detects both bootable virtual disks (SAN booting) and nonbootable virtual disks and differentiates between the two in the Microsoft Management Console (MMC) by representing each virtual disk type with a unique icon. San bootable virtual disks are represented by an icon containing a disk with a red letter “s” in the upper left corner.

SnapDrive identifies bootable virtual disks and prevents you from performing operations you would normally perform on a nonbootable virtual disk.

When a virtual disk is a boot disk, the following actions are disabled or unavailable in SnapDrive:

- ◆ Disconnect
- ◆ Delete
- ◆ Expand
- ◆ Restore

Note

Restoring snapshots of bootable virtual disks is not allowed by SnapDrive. For important information about snapshots of bootable virtual disks, see the technical white papers on the NOW site (<http://now.netapp.com/>).

**Configuring
bootable virtual
disks**

See your FCP or iSCSI HBA vendor documentation for information on configuring bootable virtual disks. If you are using the SAN Host Attach Kit for Fibre Channel Protocol on Windows, see the *SAN Host Attach Kit for Fibre Channel Protocol on Windows Installation and Setup Guide*. If you are using the QLogic QLA4010/4010C iSCSI HBA, see *Configuring iSCSI SAN Booting with the QLogic QLA 4010/4010C HBA*. These documents are on the NOW site (<http://now.netapp.com/>).

The topics that follow discuss how to use a SnapMirror destination volume, either synchronous or asynchronous, to replicate SnapDrive virtual disks.

These topics do not explain how to set up, configure, or manage SnapMirror on your filer. Instead, they focus on how to use SnapDrive in conjunction with SnapMirror for virtual disk replication. For information about SnapMirror setup and configuration, see your Data ONTAP *Data Protection Online Backup and Recovery Guide*.

Go to any of the following topics for more information.

- ◆ [“SnapMirror overview”](#) on page 208
- ◆ [“SnapMirror replication”](#) on page 211
- ◆ [“Initiating replication”](#) on page 213
- ◆ [“Connecting to a virtual disk on a destination volume”](#) on page 215
- ◆ [“Recovering a cluster from shared virtual disks on a SnapMirror destination”](#) on page 218

SnapMirror overview

SnapMirror creates either asynchronous or synchronous replicas of volumes that host virtual disks.

With synchronous SnapMirror, data on one filer is replicated on another filer at, or near, the same time it is written to the first filer.

When the virtual disk data on your source volume is offline or no longer valid, you can connect to and use the copy of the virtual disk on the SnapMirror destination volume. Unless otherwise indicated, the information discussed in this chapter applies to volumes that host SnapMirror virtual disks, whether they are asynchronous and synchronous.

If a filer volume or filer holding one or more virtual disks suffers a catastrophic failure, you can use a mirrored destination volume to recover the virtual disks.

The following topics provide more information:

- ◆ [“Understanding replication”](#) on page 208
- ◆ [“Requirements for using SnapMirror with SnapDrive”](#) on page 208

Understanding replication

The destination volume stores replicas of the virtual disks. These copies are created each time SnapMirror replication is executed. Therefore, the destination contains data that is valid up to the point when the most recent replication was executed.

Because SnapMirror is an asynchronous form of data replication, any disk writes to the source volume that follow the most recent SnapMirror replication do not appear on the destination volume until the next time the destination volume is updated. Therefore, the post-update changes to the source disk are not available in the event of a catastrophic failure.

With synchronous SnapMirror, updates are continuously written to both the source and destination volumes. In the event of a failure, the most recent changes to the source volume are also available on the destination.

Requirements for using SnapMirror with SnapDrive

To use SnapDrive in conjunction with SnapMirror, your system must meet the following requirements:

- ◆ SnapMirror must be licensed on the source and destination filers. For information on how to license and set up SnapMirror, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.
- ◆ Depending on the virtual disk protocols you are using, enable the iSCSI and FCP licenses on both the source and destination filers.
- ◆ You must manually create and initialize a mirror between the source and destination volumes, but you must *not* create a SnapMirror replication schedule.

When setting up SnapMirror on your filer, you can avoid schedule conflicts with SnapDrive by setting the replication schedule on the filer to “- - -”, which disables any scheduled transfers. When you set the replication schedule, make sure that the destination volume is in a restricted state. See the *Data ONTAP Data Protection Online Backup and Recovery Guide* for additional details.

- ◆ You must create your SnapMirror relationship using filer names not IP addresses.
- ◆ The system must contain one or more SnapMirror source volumes hosting virtual disks.
- ◆ The system must contain one or more SnapMirror destination volumes for each source volume.

Note

SnapDrive supports the use of SnapMirror at the volume level only; it does not support qtree-level SnapMirror operations.

- ◆ The destination volume must be at least as large as the source volume.
- ◆ The Windows domain account used by the SnapDrive service must be a member of the local BUILTIN\administrators group on both the source and destination filers.
- ◆ The Windows domain account used to administer SnapDrive must have full access to the Windows domain to which both the source and destination filers belong.
- ◆ If your filers are running Data ONTAP 6.4.4, the source and destination filers must be configured to grant rsh access to the Windows domain account used by the SnapDrive service. For information about configuring your filer to grant rsh access, see “[Preparing the SnapDrive service account](#)” on page 54.
- ◆ The source and destination filers must be configured to grant root access to the Windows domain account used by the SnapDrive service. That is, the `waf1.map_nt_admin_priv_to_root` option must be set to On. For

information about enabling filer options, see your Data ONTAP documentation.

- ◆ If you want to use a Windows host to access the replicated LUNs on the destination volume, the destination filer must have at least one LUN access protocol licensed (iSCSI or FCP).
- ◆ A TCP/IP connection must exist between the source filer and the destination filer.
- ◆ The SnapDrive service can perform one task at a time. Therefore, if you are scheduling multiple tasks on a host, make sure that you do not schedule these tasks to start at exactly the same time. If multiple tasks are scheduled at the same time, only the first one will succeed, while others will fail.

SnapMirror replication

Replication upon snapshot creation: Each time a snapshot of a virtual disk is created—manually or because of a snapshot schedule—SnapDrive determines whether the virtual disk whose snapshot was taken resides on a SnapMirror source volume. If so, then, after the snapshot has been taken, SnapDrive sends a SnapMirror update request to all the destination volumes associated with the source volume for that virtual disk.

When you initiate a snapshot of a LUN on a SnapMirror source through SnapDrive, a window with a checkbox labeled “Initiate SnapMirror Update” is displayed. The checkbox is selected by default.

Replication using rolling snapshots: You can also create a special type of snapshot called “rolling” snapshots, using the SnapMirror GUI in SnapDrive. These snapshots are used exclusively to facilitate frequent SnapMirror volume replication. Like regular snapshots, rolling snapshots are replicated to the SnapMirror destination volume as soon as they are created.

SnapDrive creates a new rolling snapshot every time you initiate a mirror update operation (using the Update Mirror option in the Action menu) for a specific virtual disk drive residing on a SnapMirror source volume.

To guarantee that at least one rolling snapshot for each virtual disk is always available on the destination volume, SnapDrive maintains a maximum of two rolling snapshots on the source volume.

How SnapDrive manages rolling snapshots: When an Update Mirror operation is initiated, SnapDrive checks for any existing rolling snapshots of the virtual disk containing the specified virtual disk drive.

- ◆ If SnapDrive doesn’t find any rolling snapshots containing the virtual disk image, it creates a rolling snapshot on the SnapMirror source volume. SnapDrive then initiates a SnapMirror update operation, which replicates the rolling snapshot on the destination volume.
- ◆ If SnapDrive finds one rolling snapshot, it creates a second rolling snapshot and initiates a SnapMirror update.
- ◆ If SnapDrive detects two rolling snapshots for the virtual disk, it deletes the older rolling snapshot and creates a new one to replace it. Then SnapDrive initiates a SnapMirror update.

How rolling snapshots are named: The following format is used to name the rolling snapshots:

@snapmir@{GUID}

GUID (Globally Unique Identifier) is a unique 128-bit number generated by SnapDrive to uniquely identify each rolling snapshot.

Examples: The following are examples of rolling snapshots:

@snapmir@{58e499a5-d287-4052-8e23-8947e11b520e}

@snapmir@{8434ac53-ecbc-4e9b-b80b-74c5c501a379}

Initiating replication

Requirements: Make sure you have read and satisfied the requirements listed in “[Requirements for using SnapMirror with SnapDrive](#)” on page 208 before you use the procedures in this section.

Initiating replication after snapshot creation: Because SnapDrive automatically initiates SnapMirror replication once a snapshot for a virtual disk on a SnapMirror source volume has been created, to initiate replication after a snapshot has been created, you need either to manually create a snapshot or to set up a schedule for automatic snapshot creation.

If...	Then...
You want to manually create a snapshot	See “ Creating a snapshot ” on page 168.
You want to set up a schedule for snapshot creation	See “ Scheduling snapshots ” on page 169.

Initiating replication using the Update Mirror feature: To initiate replication using the SnapDrive Update Mirror feature, complete the following steps.

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.

Step	Action
2	Perform the following actions to select the virtual disk that you want to replicate and initiate the Update Mirror operation: a. Expand the Storage option in the left pane of the MMC, if it is not expanded already. b. Double-click SnapDrive. c. Double-click Disks. d. Select the virtual disk that you want to replicate in the right panel of the MMC. e. Click Action (from the menu choices at the top of the MMC window). f. Select Update Mirror from the drop-down menu. Note _____ The Update Mirror option is not available if no mirror is configured. Result: The Update Mirror operation is initiated and a rolling snapshot of the virtual disk is created. After the snapshot has been created on the mirrored source volume, SnapDrive automatically updates the mirrored destination volume.

Connecting to a virtual disk on a destination volume

Reason for connecting to destination volumes

When the source virtual disk you want to connect to is offline, you can connect to a mirrored destination volume instead.

Requirements for connecting to a virtual disk on a destination volume

The following requirements must be satisfied before you can connect to a destination volume:

- ◆ The SnapMirror destination volume must be in “broken” state before you can connect to a virtual disk in that volume.
- ◆ The virtual disk on an asynchronous SnapMirror must be restored from the most recent snapshot containing a valid image of that virtual disk.

Using SnapDrive to meet the requirements for connecting to a destination volume

SnapDrive automates the process of meeting the requirements for connecting to a destination volume. SnapDrive checks the SnapMirror state on the destination volume holding the virtual disk. If the destination volume is an unbroken SnapMirror destination, SnapDrive displays the exact actions necessary to complete a connection to the destination volume. If you agree to proceed with the connection, SnapDrive performs the following operations:

- ◆ It breaks the SnapMirror replication for the destination volume.
- ◆ In the case of an asynchronous SnapMirror, it performs a Single File SnapRestore (SFSR) on the most recent snapshot containing a consistent image of the virtual disk.

Connecting to a mirrored destination volume

To connect to a mirrored destination volume, complete the following steps.

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.

Step	Action	
2	If the source volume is not available, you may need to perform the following actions to rescan disks: - Expand the Storage option in the left pane of the MMC, if it is not expanded already. - Double-click Disk Management. - Click Action (from the menu choices at the top of the MMC window). - Select Rescan Disks from the drop-down menu.	
3	Connect to the mirrored virtual disk on the SnapMirror destination filer. See “Connecting virtual disks” on page 142 for more information.	
4	If you want to break the mirror and connect to a SnapMirror destination volume that is online and, in the case of an asynchronous SnapMirror volume, perform a single file SnapRestore operation, click Yes in the Connect Disk dialog box. Note_____ You will need to perform this step only if the destination volume is not in the “broken” state. _____	
5	If the virtual disk...	Then...
	Will belong to a single system	Select Dedicated Drive, click Next, then skip to Step 7 .
	Will be a Windows cluster resource	Select Shared Drive, then click Next.
6	Verify that you want the disk to be shared by the nodes listed, then click Next.	
7	In the Select Virtual Disk Drive Letter window, examine the properties of the virtual disk and assign a drive letter, then click Next.	

Step	Action	
8	In the Select Initiators window, select an initiator for each host in the cluster. See “Connecting virtual disks” on page 142 for more information.	
9	If the virtual disk...	Then...
	Will belong to a single system	Go to Step 10 .
	Will be a Windows cluster resource	Select the cluster group that will own this cluster resource. Alternatively, provide the information for SnapDrive to create a new group, click Next, then go to Step 10 .
10	Click Finish to connect to the virtual disk. Result: The Computer Management window appears, with the virtual disk on the destination volume appearing under SnapDrive in the left (“Tree”) pane. Details appear in the right pane.	

Recovering a cluster from shared virtual disks on a SnapMirror destination

When the volume on which a shared virtual disk (physical disk resource) is located becomes unavailable, the cluster services fail and all MSCS physical disk resources become unavailable.

If the failed volume was configured for SnapMirror, the cluster services can be brought back up by connecting to the virtual disks on the SnapMirror destination volume.

Prerequisites: The following prerequisites must be met before you can successfully use the procedure described in this section to connect to shared virtual disks on a SnapMirror destination and thus recover your MSCS cluster:

- ◆ A SnapMirror replica of the source volume must exist on the destination volume prior to the failure of the physical disk resource.
- ◆ You must know the original drive letters and paths to the shared virtual disks on the SnapMirror source volume.
- ◆ You must know the MSCS cluster name.

For detailed instructions: See “[Connecting to shared virtual disks on a SnapMirror destination](#)” on page 218 for a step-by-step procedure.

Connecting to shared virtual disks on a SnapMirror destination

To connect to shared virtual disks on a SnapMirror destination, complete the following steps.

Step	Action
1	Configure the cluster service to start manually on all nodes of the cluster by performing the following actions on each node of the cluster: a. Select Start > Programs > Administrative Tools > Computer Management. a. Expand the Services and Applications option in the left pane of the MMC, if it is not expanded already. b. Click Services in the left pane of the MMC. c. Double-click Cluster Service. d. Select Manual from the Startup Type list.
2	Reboot all nodes of the cluster. Note_____ The reboot is required so the existing virtual disks fail to mount and, therefore, the drive letters that were in use will be released.
3	On one of the cluster nodes, follow the steps described in “Connecting a virtual disk” on page 142, keeping in mind the following information to connect to a virtual disk: ◆ If the quorum disk is not yet connected, start by connecting to it before you connect to other shared virtual disks. ◆ When prompted for the virtual disk path in the Provide Virtual Disk Location panel, specify or browse to the virtual disk file in the active file system (not the one in the snapshot) on the SnapMirror destination volume. ◆ After you specify the virtual disk path and click Next, you see a message that a single file SnapRestore will be performed. Click Yes to continue. ◆ When prompted for disk type in the Select a Virtual Disk Type panel, select Shared. ◆ When prompted for a drive letter in the Select Virtual Disk Drive Letter panel, select the same drive letter that was being used for the virtual disk on the SnapMirror source volume.

Step	Action
4	After you have successfully completed the Connect Disk wizard, you see one of the following two error messages. These error messages are expected and do not indicate a problem. Error message 1: "Unable to connect disk. Failure in Mounting volume on the disk. Error: Could not find the volume mounted for the virtual disk as there does not seem to be any new volumes mounted by the Mount Manager" This error may appear also in the following form: "Unable to connect disk. Failure in connecting to the virtual disk. Error: Timeout has occurred while waiting for disk arrival notification from the operating system." Error message 2: "Unable to retrieve a list of virtual disk snapshots. Error : The device is not ready." Note_____ Error message 2 is displayed instead of error message 1 when McAfee NetShield is installed on your Windows server. _____
5	Click OK to ignore the error message.
6	Repeat Step 3 through Step 5 for each shared virtual disk on the cluster.
7	Configure the cluster service to start automatically on the system to which you connected shared virtual disks, by performing the actions listed in Step 1 of this procedure; however, this time select Automatic from the Startup Type list.
8	For the remaining nodes of the cluster, repeat Step 3 through Step 7 with the following exceptions: ◆ You are prompted for the MSCS cluster name for the remaining nodes when you use the Connect Disk Wizard. ◆ You do not see the error messages described in Step 4 for the remaining nodes of the cluster.

Step	Action
9	Use the Cluster Administrator to verify that the cluster is functioning correctly as follows: ◆ Ensure that all resources are online. ◆ Perform a “move group” operation from one node to the other and then back to the original node. Result: : You have successfully connected to the shared virtual disks in a SnapMirror destination volume.

This topics that follow detail the SnapDrive operations you can execute through the `sdcli` command-line utility, which enables you to enter SnapDrive commands individually or through automation scripts.

Go to any of the following topics for more information.

- ◆ “[SnapDrive configuration commands](#)” on page 228
- ◆ “[SnapDrive preferred IP address commands](#)” on page 230
- ◆ “[iSCSI connection commands](#)” on page 231
- ◆ “[iSCSI initiator commands](#)” on page 232
- ◆ “[Virtual disk commands](#)” on page 234
- ◆ “[Multipathing commands](#)” on page 238
- ◆ “[Snapshot commands](#)” on page 242

Using sdcli commands

The `sdcli` commands consist of three input parameters (for example, `sdcli snap create`), which must be specified in the correct order, followed by one or more command-line switches. You can specify the command-line switches in any order.

Valid variations:

```
sdcli disk connect -d z -dtype dedicated
-p \\filer2\SD_only\mktng.lun -I host4 10:00:00:00:C9:2B:FD:12

sdcli disk connect -I host4 10:00:00:00:C9:2B:FD:12 -d z
-p \\filer2\SD_only\mktng.lun -dtype dedicated
```

Caution
Failure to specify input parameters in the correct order results in command execution failure.

Caution
Command-line switches are case-sensitive. For instance, the `-d` switch refers to a single drive letter, while the `-D` switch refers to one or more drive letters separated by spaces.

Go to any of the following topics for more information.

- ◆ [“Executing sdcli commands”](#) on page 224
- ◆ [“Common command switches”](#) on page 225
- ◆ [“Command-specific switches”](#) on page 227

Executing sdcli commands

To run `sdcli` commands, complete the following steps.

Step	Action
1	Using a host that has SnapDrive installed, select Start Menu > Run.
2	Type <code>cmd</code> in the dialog box entry field, and then click OK.
3	After the Windows command prompt window opens, navigate to the directory on your host where SnapDrive is installed. Example: C: cd \Program Files\SnapDrive\

Step	Action
4	Enter the individual command you want to run. Make sure to include all input parameters in the proper order and to specify both required and desired command-line switches in any order. Example: <pre>sdcli disk disconnect -d R</pre> Alternatively, enter the name and path of the automation script you want to run. Example: <pre>C:\SnapDrive Scripts\disconnect_R_from_host4.bat</pre>

Common command switches

Some or all of the `sdcli` commands share the command-line switches listed in the following table.

Switch	Comment
-d	The drive letter assigned to the virtual disk. If <code>sdcli</code> can't find the drive letter specified through the <code>-d</code> switch, it displays a list of all virtual disks connected to the host. Example: <code>-d j</code> indicates that the virtual disk is mapped to the J: drive on the host.
-D	A list of drive letters separated by spaces. Example: <code>-D j k l</code> indicates that the command applies to the J:, K:, and L: drives.
-dtype	The drive type (shared or dedicated).
-e	The name of an existing MSCS resource group, which is required only if the virtual disk is shared among MSCS nodes.
-i	The initiator name. ◆ For FCP, the initiator name is the WWPN (World Wide Port Name) for the initiator, which takes the form <i>hh:hh:hh:hh:hh:hh:hh:hh</i>. ◆ For iSCSI, the initiator name takes the form <i>iqn.iSCSI qualified name</i>. For more information on iSCSI node names, see the <i>Block Access Management Guide</i>.

Switch	Comment
-I	The list of hosts and initiators. Separate the character strings that specify hosts and initiators with spaces. To specify the host, you can use either an IP address (<i>nnn.nnn.nnn.nnn</i>) or a machine name recognized by the domain controller. To specify the initiator, type the appropriate WWPn, which you can determine through the <code>lputilnt.exe</code> utility supplied with your NetApp FCP HBA Attach Kit. After you launch <code>lputilnt.exe</code>, navigate to Main Menu > Adapter > Configuration Data and select “16 - World-Wide Name” in the Region field. The available WWPns appear in the list box directly beneath the Region field. When MPIO is running, you can specify up to four node-initiator pairs. The first <code>NodeMachineName</code> in the cluster applies to two of the available initiator WWPns; the other <code>NodeMachineName</code> applies to the remaining pair of initiator WWPns.
-ID	An MPIO path ID. For details, see “ Understanding MPIO path IDs ” on page 238.
-m	The host on which the virtual disk is mounted. You can use an IP address or a machine name to identify the host. Note_____ Do not specify the <code>-m</code> switch when running an <code>sdcli</code> command on the local host. _____
-n	The name and description of an MSCS cluster resource group to be created as part of the associated command. This switch is required only if you need to create an MSCS cluster resource group to facilitate the sharing of a virtual disk among MSCS cluster nodes.
-np	The IP address and port of the network portal on the iSCSI connection target.
-p	The UNC path to the location of the virtual disk on the filer. This string takes the following form: <code>\\filename\sharename\virtualdiskfilename{.lun .vld}</code>
-z	Specifies the size (in megabytes) of a new virtual disk—or the number of megabytes by which an existing virtual disk is to be expanded. The minimum size for virtual disks is 32 MB. The maximum sizes vary according to the remaining available space in your volume. For more information, see “ Understanding volume size ” on page 15.

Command-specific switches

Switches that apply to just one command appear with those commands in the sections that follow.

SnapDrive configuration commands

The `sdcli` utility supports the following iSCSI configuration operation: list

Operation
<code>sysconfig list</code> displays the SnapDrive configuration information for your host.
Syntax:
<code>sdcli sysconfig list</code>

SnapDrive license commands

The `sdcli` utility supports the following SnapDrive license operations: set and list.

Operation
<code>license set</code> sets the license key for the specified module. Syntax: <pre>sdcli license set -module <i>ModuleName</i> -key <i>LicenseKey</i></pre> <code>-module</code> either LPSM (LUN Provisioning and Snapshot Management) or NTAPMPIO <code>-key</code> 14 character license key Example: <pre>sdcli license set -module LPSM -key ABCDEFGHIJKLMNOP</pre> The preceding example sets the license key for the LPSM module.
<code>license list</code> displays all SnapDrive licenses installed. Syntax: <pre>sdcli license list</pre>

SnapDrive preferred IP address commands

The `sdcli` utility supports the following SnapDrive preferred IP operations: set, list, and delete.

Operation
<code>preferredIP set</code> sets the SnapDrive preferred IP address for the specified filer. Syntax: <pre>sdcli preferredIP set -filer <i>FilerName</i> -IP <i>PreferredIPAddress</i></pre> Example: <pre>sdcli preferredIP set -filer filer1 -IP 172.18.53.94</pre> The preceding example sets the SnapDrive preferred IP address for the filer named <code>filer1</code> to <code>172.28.53.94</code>.
<code>preferredIP list</code> displays all SnapDrive preferred IP addresses. Syntax: <pre>sdcli preferredIP list</pre>
<code>preferredIP delete</code> deletes the preferred IP address for the specified filer. Syntax: <pre>sdcli preferredIP delete -filer <i>FilerName</i></pre> Example: <pre>sdcli preferredIP delete -filer filer1</pre>

iSCSI connection commands

The `sdcli` utility supports the following iSCSI connection operations: disconnect and list.

Operation
<code>iscsi_target disconnect</code> disconnects the specified iSCSI initiator from the specified iSCSI target on all portals. Syntax: <pre>sdcli iscsi_target disconnect -t TargetName</pre> Example: <pre>sdcli iscsi_target disconnect -t iqn.1992.08.com.netapp:sn.33604307</pre> The preceding example disconnects the specified iSCSI target.
<code>iscsi_target list</code> displays a list of all iSCSI targets. For each target, the command displays all portals through which the target is available or to which the target is connected. Syntax: <pre>sdcli iscsi_target list {-f FilerName -i InitiatorPortName}</pre> <code>-f</code> displays all targets on the specified filer. Example: <pre>sdcli iscsi_target list -f filer2</pre> The preceding example lists all the iSCSI targets on the <code>filer2</code> filer, as well as all portals those targets are available through or connected to.

iSCSI initiator commands

The `sdcli` utility supports the following iSCSI initiator-related operations: list, establish session, and terminate session.

Operation
<code>iscsi_initiator list</code> displays a list of all iSCSI sessions on the specified machine. Syntax: <pre>sdcli iscsi_initiator list {-m MachineName} -s</pre> <i>MachineName</i> is the machine name on which you want to execute the command. If no machine name is specified, the command is executed on the local machine. <code>-s</code> enumerates the iSCSI sessions. Example: <pre>sdcli iscsi_initiator list -s</pre> The preceding example displays all iSCSI sessions on the local host.
<code>iscsi_initiator establish_session</code> establishes a session with a target using the specified HBA. Syntax: <pre>sdcli iscsi_initiator establish_session {-m MachineName} {-h HBA_ID} {-hp HBA Portal ID} -t TargetName -np IPAddress IPPort {-c CHAPName CHAPPassword}</pre> <code>-h HBA_ID</code> is used to establish the iSCSI session. The HBA ID can be obtained by using the the <code>sdcli sysconfig list</code> command. <code>-hp HBA Portal ID</code> is used to specify the portal on the iSCSI HBA to be used to establish the iSCSI session. The HBA Portal ID can be obtained by using the <code>sdcli sysconfig list</code> command. <code>-t TargetName</code> is the name of the iSCSI target. <code>-np IP Address IPPort</code> specify the IP address and IP port of the network portal on the target. The IP Port can be obtained by using the the <code>sdcli iscsi_initiator list</code> command. Example: <pre>sdcli iscsi_initiator establish_session -h 0 -t iqn.1992-8.com.netapp:maya -np 172.18.53.94 3260</pre> The preceding example establishes an iSCSI session with the specified target using the specified HBA ID.

Operation

`iscsi_initiator terminate_session` terminates the session.

Syntax:

```
sdcli iscsi_initiator terminate_session {-m MachineName} -s Session_ID
```

MachineName is the machine name on which you want to execute the command. If no machine name is specified, the command is executed on the local machine.

`-s` is the session ID of the session you want to terminate.

Example:

```
sdcli iscsi_initiator terminate_session -s 0xffffffff868589cc-0x4000013700000006
```

The preceding example terminates the specified iSCSI session on the local machine.

Virtual disk commands

The `sdcli` utility supports the following virtual disk-related operations: create, connect, convert, delete, disconnect, expand, and list.

Operation
<code>disk create</code> creates a new virtual disk. Syntax: <pre>sdcli disk create [-m MachineName] -p UNC path -d DriveLetter -z DriveSize -I [[NodeMachineName InitiatorName] ...] -dtype {shared dedicated} {[-e "ResourceGroupName"] [-n "ResourceGroupName" "ResourceGroupDesc"]}</pre> Examples: <pre>sdcli disk create -dtype dedicated -z 1024 -p \\filer2\sd_vds_only\mktng.lun -d R -I host3 10:00:00:00:C9:2B:FD:12</pre> The preceding example creates a dedicated, 1-GB virtual disk named <code>mktng.lun</code> in the <code>filer2</code> volume named <code>sd_vds_only</code>. Next, it connects this virtual disk to the host as drive <code>R</code>: <pre>sdcli disk create -p \\133.25.61.62\sd_vds_only\mktng.lun -d r -z 4096 -dtype shared -e "mktng" -I host4 10:00:00:00:C9:2B:FD:12 host4 10:00:00:00:C9:2B:FD:11 host5 10:00:00:00:C9:2B:FC:12 host5 10:00:00:00:C9:2B:FC:11</pre> The preceding example creates a shared, 4-GB virtual disk on <code>host4</code> (the local machine running the <code>sdcli</code> command) and maps it to drive <code>R</code>, using a pair of initiators. This command also creates MPIO paths through <code>host5</code>, which is partnered with <code>host4</code> in an MSCS cluster.
<code>disk connect</code> connects a virtual disk (LUN) to a host by mapping the virtual disk to a Windows drive letter. Syntax: <pre>sdcli disk connect [-m MachineName] -p UNCpath -d DriveLetter [-I [NodeMachineName InitiatorName] ...] -dtype {shared dedicated} {[-e "ResourceGroupName"] [-n "ResourceGroupName" "ResourceGroupDesc"]} [-c "ClusterName"]</pre> Example: <pre>sdcli disk connect -d s -dtype shared -p \\filer2\sd_vds_only\mktng.lun -I host3 10:00:00:00:C9:2B:FD:1B host3 10:00:00:00:C9:2B:FD:1C host4 10:00:00:00:C9:2B:FD:12 host4 10:00:00:00:C9:2B:FD:11 -e "tech_mktng" -c "mktng"</pre> The preceding example connects a virtual disk (LUN) in the <code>filer2</code> volume <code>sd_vds_only</code> and named <code>mktng.lun</code>, which belongs to the MSCS cluster resource group <code>tech_mktng</code> on the <code>mktng</code> cluster. MPIO paths are connected for both nodes on the cluster.

Operation

`disk convert` converts a VLD-type virtual disk into a LUN-type virtual disk. The conversion process is irreversible, because you cannot convert a LUN-type virtual disk into a VLD-type virtual disk.

Note

You must disconnect the disk before converting it.

Syntax:

```
sdcli disk convert [-m MachineName] -p UNCpath [-l LUNName]
```

LUN Name is the name of the new virtual disk, including the .lun extension.

Example:

```
sdcli disk convert -p \\filer2\sd_vds_only\mktng.vld -l recycledvld.lun
```

The preceding example converts the VLD-type virtual disk `mktng.vld`, which is in the `sd_vds_only` volume on `filer2`, into a LUN-type virtual disk named `recycledvld.lun`.

`disk delete` deletes a virtual disk. The virtual disk must be connected (mapped to a Windows drive letter) for the command to succeed.

Note

You must make sure that the virtual disk you are deleting is not being monitored with the Windows Performance Monitor (`perfmon`).

Syntax:

```
sdcli disk delete [-m MachineName] {-p UNCpath | -d DriveLetter}
```

Example:

```
sdcli disk delete -p \\133.25.61.62\sd_vds_only\mktng.lun
```

The preceding example deletes the virtual disk `mktng.lun` from the `sd_vds_only` volume on the filer identified by the IP address `133.25.61.62`.

Operation

`disk disconnect` disconnects a virtual disk from the host. The virtual disk must be connected (mapped to a Windows drive letter) for the command to succeed.

Note

You must make sure that the virtual disk you are disconnecting is not monitored with the Windows Performance Monitor (perfmon).

Syntax:

```
sdcli disk disconnect [-m MachineName] {-p UNCpath | -d DriveLetter} [-f]
```

Caution

The `-f` switch causes the virtual disk to be forcibly unmounted, even if an application or the Windows operating system is using it. Therefore, use this feature with extreme care.

Examples:

```
sdcli disk disconnect -d z
```

The preceding example disconnects the virtual disk mapped to the drive letter “Z:” on the SnapDrive host running the `sdcli` command.

```
sdcli disk disconnect -p \\filer2\sd_vds_only\mktng.lun -f
```

The preceding example forces disconnection of the virtual disk `mktng.lun`, which is in the `sd_vds_only` volume on `filer2`. Because the `-f` switch is being used, all open files in the virtual disk might be lost or corrupted.

`disk expand` expands the disk by a user-specified size, as long as that figure falls within the SnapDrive-specified minimum and maximum values.

Syntax:

```
sdcli disk expand [-m MachineName>] {-p UNCpath | -d DriveLetter} -z DriveSizeIncrement
```

DriveSizeIncrement is measured in megabytes.

Example:

```
sdcli disk expand -z 1024 -d p
```

The preceding example increases the virtual disk mapped to “P:” by 1 GB. (In practice, SnapDrive expands the disk by the amount specified by `-z`, plus a certain increment required for system overhead.)

Operation

`disk list` displays a list of all the virtual disks connected to the host.

Syntax:

```
sdcli disk list [-m MachineName]
```

Example:

```
sdcli disk list
```

The preceding example lists all the SnapDrive virtual disks mapped to drive letters on the local host. Among the items listed are the following values:

- ◆ UNC path (filename, sharename, virtualdiskfilename, and may also include qtreename)
- ◆ Filer Name
- ◆ Filer Path (filer-side path, which includes volume name and LUN name)
- ◆ Type
- ◆ Disk serial number
- ◆ Back by Snapshot (if this is a LUN in a snapshot, this displays the filer-side path to the snapshot)
- ◆ Shared (whether the disk is dedicated or shared)
- ◆ BootOrSystem Disk
- ◆ SCSI port
- ◆ Bus
- ◆ Target
- ◆ LUN
- ◆ Readonly
- ◆ Disk size (in megabytes)
- ◆ Mount point (the drive letter to which the virtual disk is mapped on the host)
- ◆ IP Addresses (IP addresses on the target filer)

Multipathing commands

The `sdcli` utility supports the following MPIO-related operations: create, delete, connect, disconnect, expand, list, and convert.

Understanding MPIO path IDs: For all multipathing-related operations executed through `sdcli`, *pathID* specifies the virtual path created by mapping a virtual disk on the filer to an initiator port on the host. This number, which is generated by the Windows enumerator and also known as a DSM Path, is created from four consecutive hex numbers.

Example: 0x4000d07

- ◆ The SCSI port number representing the initiator on the host is 04, but because it begins the string, and because it is between 01 and 09, inclusive, the leading 0 is omitted, and the value is simply represented as 4. (When the value is between 0xA and 0xF, inclusive, the leading 0 is not omitted.)
- ◆ The host bus number is 00.
- ◆ The “target” address ID for the target port is 0d.
- ◆ The LUN number, 07, is generated by the Windows enumerator.

Note

pathID is not relevant for SnapDrive GUI users. Instead of displaying *pathIDs* for each virtual disk, the right pane of the Computer Management window displays the following information about the paths associated with each virtual disk:

- ◆ State
 - ◆ Initiator HBA Name
 - ◆ Initiator HBA Address
 - ◆ Target Adapter/Portal IP
 - ◆ Proxy Path
-

Supported MPIO commands: The table that follows lists the MPIO-related operations supported by sdcli: activate, add, disable, enable, list, remove, and version.

Operation
<code>path activate</code> directs I/O through the specified path and causes the currently active path to become passive. (This command can only be performed on a passive path.) Syntax: <pre>sdcli path activate [-m MachineName] -ID PathID</pre> Example: <pre>sdcli path activate -ID 0x4000d07</pre> The preceding example activates path 0x4000d07 and makes passive whatever path was active when the command was run.
<code>path add</code> creates a new virtual path from the initiator on the host to the virtual disk on the filer. Note This option is not available if you licensed and installed only the MPIO module and you did not license and install the LUN Provisioning and Snapshot Management module. Syntax: <pre>sdcli path add [-m MachineName] {-p UNCpath -d DriveLetter} -i InitiatorPortName</pre> Example: <pre>sdcli path add -p \\filer2\sd_vds_only\mktng.lun -i 10:00:00:00:c9:2b:fd:13</pre> The preceding example creates a new path from the local host to the virtual disk mktng.lun on the sd_vds_only volume on filer2, assigning the new path to the initiator port associated with WWPN 10:00:00:00:c9:2b:fd:13.
<code>path disable</code> puts the specified path on standby. (This operation can only be performed on a passive path.) Syntax: <pre>sdcli path disable [-m MachineName] -ID PathID</pre> Example: <pre>sdcli path disable -ID 0x4000d07</pre> The preceding example places the currently passive path 0x4000d07 on standby.

Operation

`path enable` causes a disabled path to become passive. (This operation can only be performed on a disabled path.)

Syntax:

```
sdcli path enable [-m MachineName] -ID PathID
```

Example:

```
sdcli path enable -ID 0x4000d07
```

The preceding example changes the status of path 0x4000d07 from disabled to enabled (passive).

`path list` enumerates all virtual paths and their status for the specified virtual disk. This command also displays the path ID for the specified LUN.

Note

If you only licensed and installed the MPIO module and did not license and install the LUN Provisioning and Snapshot Management module, SnapDrive will not accept a UNC path when using the `path list` command.

Syntax:

```
sdcli path list [-m MachineName] {-p UNCpath | -d DriveLetter}
```

Example:

```
sdcli path list -d z
```

The preceding example lists all the MPIO paths specified for the virtual disk mapped to Z: on the local host.

`path remove` deletes the specified mapping (virtual path) between the LUN on the filer and the initiator on the host.

Note

This option is not available if you licensed and installed only the MPIO module and you did not license and install the LUN Provisioning and Snapshot Management module.

Syntax:

```
sdcli path remove [-m MachineName] {-p UNCpath | -d DriveLetter} -i InitiatorPortName
```

Example:

```
sdcli path remove -p \\filer2\sd_vds_only\mktng.lun -i 10:00:00:00:c9:2b:fd:13
```

The preceding example deletes the virtual path associated with WWPN 10:00:00:00:c9:2b:fd:13 and the mktng.lun virtual disk on the filer2 volume sd_vds_only.

Operation

`path version` indicates whether NTAPDSM is installed on the specified system.

Syntax:

```
sdcli path version [-m MachineName]
```

Example:

```
sdcli path version
```

The preceding example returns information about whether NTAPDSM is installed on the local host.

Snapshot commands

The table that follows lists the snapshot-related operations supported by `sdcli`:
create, delete, list, mount, rename, restore, unmount, and update mirror.

Operation
<code>snap create</code> creates a new snapshot of the specified virtual disks on the SnapDrive system. Syntax: <pre>sdcli snap create [-m MachineName] -s SnapshotName -D DriveLetterList [. . .] [-x]</pre> <code>-x</code> causes data to be flushed and consistent snapshots to be created only for the drives specified by the <code>-D</code> switch. Otherwise, SnapDrive flushes data and creates consistent snapshots for all virtual disks connected to the host and residing on filer volumes. Note Snapshots are created at the volume level. When a snapshot is created using <code>-x</code> with the <code>-D</code> switch, snapshots are also created for any additional disks mapped to the host that reside on the same volumes as the disks specified. Snapshots for the unspecified disks are grayed out in the SnapDrive MMC because they are inconsistent. Example: <pre>sdcli snap create -s Jun_13_03 -D j k l</pre> The preceding example creates a snapshot named <code>Jun_13_03</code> for each volume containing one or more of the virtual disks mapped to the specified drives (that is, J:, K:, and L:). The snapshots created are consistent for all virtual disks contained by those volumes.
<code>snap delete</code> deletes an existing snapshot. Note You must make sure that the virtual disk whose snapshot you are deleting is not being monitored with the Windows Performance Monitor (perfmon). Syntax: <pre>sdcli snap delete [-m MachineName] -s SnapshotName -D DriveLetterList [. . .]</pre> Example: <pre>sdcli snap delete -s Jun_13_03 -D k</pre> The preceding example deletes the snapshot named <code>Jun_13_03</code> that is associated with the virtual disk mapped to K: on the local host.

Operation
<code>snap list</code> lists all the snapshots that exist for the specified virtual disk. <pre>sdcli snap list [-m <i>MachineName</i>] -d <i>DriveLetter</i></pre> Example: <pre>sdcli snap list -d j</pre> The preceding example displays all the snapshots that exist for the volume containing the virtual disk mapped to “J:” on the local host.
<code>snap mount</code> mounts a snapshot of a virtual disk. Snapshots are always mounted in read/write mode. Syntax: <pre>sdcli snap mount [-m <i>MachineName</i>] [-r <i>LiveMachineName</i>] -k <i>LiveDriveLetter</i> -s <i>SnapshotName</i> -d <i>DriveLetter</i></pre> <i>LiveMachineName</i> refers to the name of the host connected to the virtual disk in the active file system. When left unspecified, <code>-r</code> defaults to the local host. <i>LiveDriveLetter</i> refers to the drive letter assigned to the virtual disk in the active file system. Example: <pre>sdcli snap mount -r host3 -k j -s Jun_13_03 -d t</pre> The preceding example maps the snapshot named <code>Jun_13_03</code> to drive T: on the local host. This snapshot represents a point-in-time image of the virtual disk mapped to J: on host3.
<code>snap rename</code> enables you to change the name of an existing snapshot. Syntax: <pre>sdcli snap rename [-m <i>MachineName</i>] -d <i>DriveLetter</i> -o <i>OldSnapshotName</i> -n <i>NewSnapshotName</i></pre> Example: <pre>sdcli snap rename -d j -o Jun_13_03 -n last_known_good</pre> The preceding example changes the name of the <code>Jun_13_03</code> snapshot associated with the J: drive to <code>last_known_good</code>.

Operation

`snap restore` replaces the current virtual disk image in the active file system with the point-in-time image captured by the specified snapshot.

Note

You must make sure that the virtual disk you are disconnecting is not being monitored with the Windows Performance Monitor (perfmon).

Syntax:

```
sdcli snap restore [-m MachineName] -d DriveLetter -s SnapshotName
```

Example:

```
sdcli snap restore -d l -s Jun_13_03
```

The preceding example restores the virtual disk mapped to L: on the local host to its state when the snapshot named Jun_13_03 was taken.

`snap unmount` disconnects a snapshot of a virtual disk that is mounted as a virtual disk.

Note

You must make sure that the virtual disk whose snapshot you are disconnecting is not being monitored with the Windows Performance Monitor (perfmon).

Syntax:

```
sdcli snap unmount [-m MachineName] -d DriveLetter [-f]
```

Caution

The `-f` argument forcibly unmounts the virtual disk, even if it is in use by an application or Windows. Such a forced operation could cause data loss, so use it with extreme caution.

Examples:

```
sdcli snap unmount -d k
```

The preceding example disconnects the snapshot mapped to K: on the local host.

```
sdcli snap unmount -d k -f
```

The preceding example forces disconnection of the snapshot mapped to the K: drive on the local host.

Operation

`snap update_mirror` updates the virtual disk to a SnapMirror destination volume residing on the same or a different filer.

Syntax:

```
sdcli snap update_mirror [-m MachineName] -d DriveLetter
```

Example:

```
sdcli snap update_mirror -d l
```

The preceding example updates the SnapMirror destination for the virtual disk mapped to the L: drive on the local host. You don't need to specify the location of the SnapMirror destination because that information was entered when mirroring was set up for the virtual disk.

The following list directs you to the various SnapDrive requirements and recommendations set out in this document.

Assumed competence: See “[Audience](#)” on page xiii.

Host requirements: See the following sections:

- ◆ “[Preparing hosts](#)” on page 36
- ◆ “[Recommendations for choosing a configuration](#)” on page 23

Filer requirements: See “[Preparing filers](#)” on page 40.

SnapDrive service account requirements: See “[Preparing the SnapDrive service account](#)” on page 54.

Volume and filer options: See “[Volume and filer options set by SnapDrive](#)” on page 41.

Cluster recommendations: See “[Recommendations for choosing a configuration](#)” on page 23.

SnapDrive-specific limitations: See “[SnapDrive-specific limitations](#)” on page 42.

SnapDrive-specific cautions and recommendations: See “[Cautions and recommendations](#)” on page 43.

SnapDrive user interfaces: See “[SnapDrive user interfaces](#)” on page 56

Index

A

- abnormal disconnect (of virtual disk) 147
- access protocols 13
- accessing virtual disks 13
- administration, remote 160
- applications, stopping for VLD conversion 76
- archives, restoring from 180
- archiving, snapshots 180
- asynchronous replication 208
- authentication, pass-through 51
- Autosupport (filer), enabling 161

B

- BUILTIN/administrators group 54
- busy snapshot error 179

C

- cautions and recommendations for SnapDrive 43
- Challenge Handshake Authentication Protocol (CHAP)
 - understanding 115
- changing path states, MPIO 201
- changing SnapDrive service account password 54
- CIFS
 - limited functionality supplied with FCP and iSCSI license 41, 44
 - setup 46
- cifs setup command 46
- CIFS shares
 - cifs setup command 46
 - creating 46
- cluster
 - See also* Windows cluster
 - "private" network 28
 - Cluster Service (MSCS), definition of 4
 - converting VLDs in cluster groups 85
 - FCP configurations 31
 - iSCSI configurations 28
 - MPIO configurations 34, 35
 - support in SnapDrive 9

- configurations
 - choosing 23
 - FCP 30
 - guidelines 23
 - iSCSI 26
 - multipathing (MPIO) 33, 193
- configuring, filer volumes 44
- connect
 - to (mirrored) destination volumes 215
 - to a virtual disk 142
 - to virtual disks (LUNs) in a snapshot 172
- converting
 - VLD quorum disk 86
 - VLDs for MSCS 82
 - VLDs in a cluster group 85
 - VLDs to LUNs 77
- create
 - iSCSI session 113
 - shared virtual disks (on a Windows cluster) 128
 - snapshots using SnapDrive 166, 168
 - virtual disks 123
- creating a CIFS share 46
- creating a filer volume 45
- creating a qtree 45
- crossover FCP cable 30

D

- Data ONTAP, required version 40
- data restore from snapshots 176
- dedicated filer volume required for virtual disks (LUNs) 44
- delete
 - a virtual disk 149
 - snapshots 178
- deleting
 - snapshots, problems with 179
- details of iSCSI sessions 119
- df -r (filer command) 17
- disconnect
 - a virtual disk 146

- forced (of virtual disk) 147
- from an iSCSI target 116
- disks
 - hot spare 14
 - virtual 122
- documentation
 - Data ONTAP 46
 - filer 40
 - obtaining 22
- drive letters, list incorrect when viewed via Terminal Service 56
- drivers, obtaining 37
- dump command 180

E

- email notification, setting up 161
- expand
 - a quorum disk 152
 - virtual disks 150, 151

F

- failover
 - definition 4
 - NetApp cluster 9
- FCP
 - adapters 34
 - configurations 30
 - crossover cable 30
 - documentation 22
 - Host Bus Adapter (HBA) 22
 - initiator 11
 - installing 94
 - license required on filer 41
 - MPIO configurations 33, 34
 - obtaining firmware and driver 37
 - single-host, single-filer configurations 30
 - switch 31, 34
 - switched configuration 31
 - uninstalling driver 108
 - windows cluster configurations 31
- features, updating mirrors 213
- Fibre Channel Protocol *See* FCP
- fields
 - iSCSI Initiator Name 119

- iSCSI Target Name 119
- Number of LUNs 119
- Target Portal IP Address 119
- Target Portal Port 119
- file system 5
- filer
 - administrator access required for SnapDrive 54
 - BUILTIN/administrators group 54
 - checking licenses 41
 - creating a volume 45
 - dedicated volume required for LUNs 44
 - definition 5
 - df -r command 17
 - documentation 40
 - guidelines for creating volumes 44
 - interaction with virtual disks 12
 - licenses required 41
 - options set by SnapDrive 41
 - preparing 40
 - requirements 40
 - resetting the snap reserve 49
 - settings for SnapDrive 16
 - upgrading 100
 - user interfaces 56
 - volume preparation 43
 - Windows domain account 54
- filer cluster
 - FCP configurations 31
 - iSCSI configurations 28
 - MPIO configurations 34, 35
- filer console, definition 56
- FilerView
 - checking filer licenses 41
 - creating a volume 45
 - definition 56
 - opening a session 45, 46
 - setting snap reserve 49
- firmware, obtaining 37
- forcing disconnect (of a virtual disk) 147

G

- GbE
 - switch 35
- GbE (Gigabit Ethernet)

- iSCSI configurations 26
 - switched configuration 27
- guidelines
 - for choosing SnapDrive configuration 23
 - for creating filer volumes 44

H

- host 5
- Host Bus Adapter (HBA)
 - definition of 5
 - documentation, for FCP 22
- host console
 - definition 56
 - error messages not seen in Terminal Service session 56
- hot spare disks 14

I

- initiator
 - definition of 5
 - obtaining iSCSI 37
- Initiator HBA field 119
- Initiator IP address field 119
- installing
 - FCP 94
 - first time 93
 - iSCSI 94
 - SnapDrive components 101
- IP address, setting preferred 105
- iSCSI
 - cluster configurations 28
 - configurations 26
 - initiator 11
 - installing 94
 - license required on filer 41
 - MPIO configurations 33, 35
 - obtaining software 37
 - single-host, single-filer configurations 26
 - software initiator node name standards 113
 - upgrading 97
 - upgrading a non-clustered host 97
 - upgrading a Windows cluster 98
 - uninstalling 109
- iSCSI connections

- creating 113
- iSCSI sessions
 - details 119
 - disconnecting from a target 116
 - establishing 113
 - ways to establish 112
- iSCSI Target Name field 119

L

- latency, minimizing with GbE crossover cable 26
- licensable modules
 - about 2
 - feature availability 2
 - managing 2, 3
- licenses
 - checking with FilerView 41
 - required on filer 41
- limitations
 - LUN cloning 43
 - MultiStore 43
 - qtree quotas. 42
 - SnapDrive 42
- Logical Unit Numbers. *See* LUNs
- LUNs
 - See also* virtual disks
 - cloning not supported 43
 - conversion to 77
 - dedicated filer volume required 44
 - definition of
 - not visible when created via Terminal Service 56
 - snap reserve setting on filer 49
 - with MultiStore, limited to vfiler0 43
- LUN-type virtual disks, definition 6

M

- modify, virtual disk properties 158
- Monitor Time Interval property 158
- mpdev.sys 190
- MPIO
 - accessing using MMC 198
 - active path 190
 - changing path states 201
 - configurations 33

- drivers 10
- enabling 193
- overview 190
- passive path 190
- path IDs 238
- path states 200
- requirements, hardware and software 191
- supported topologies 193
- uninstalling 108

mpio.sys 190

MS Exchange, stopping for VLD conversion 74

MS SQL Server, stopping for VLD conversion 75

MSCS

- See also* Windows cluster

- converting VLDs 82

- definition 4

- FCP configurations 31

- iSCSI configurations 28

- MPIO configurations 34, 35

mspsfltr.sys 190

multipathing. *See* MPIO

MultiStore, SnapDrive limitation 43

N

NDMP-based backup application 180

NetApp Windows Attach Kit for FCP

- documentation 22

Network Interface Card (NIC), definition of 6

network, "private" for internal cluster traffic 28

non-SnapDrive LUNs

- managing 155

- preparing for SnapDrive 155

- prerequisites for SnapDrive 155

notification settings, for SnapDrive 161

ntapdsm.sys 190

NTFS 5

Number of LUNs field 119

O

obtaining firmware and drivers 37

operating system

- filer requirement 40

- required on Windows host 37

options, snap reserve 49

P

pass-through authentication 51

password, changing for SnapDrive service account 54

path states, MPIO 200

preferred IP address, setting 105

properties, modifying virtual disk 158

protocols, connection 13

Q

qtrees

- creating 45

- SnapDrive limitation 42

quorum

- converting to LUN 86

- creating a virtual disk as a 129

- expanding 152

R

read/write mode, connecting to snapshots in 172

recommendations

- and cautions for using SnapDrive 43

- for configuring filer volumes 44

- snap reserve 49

remote administration

- definition of 56

- of SnapDrive 160

replication

- asynchronous 208

- initiating 213

- SnapMirror 211

- synchronous 208

- upon snapshot creation 211

- using rolling snapshots 211

requirements

- administrator access to filer 54

- Data ONTAP 40

- filer 40

- filer licenses 41

- for SnapMirror 208

- for snapshots 167

- operating system 37

- SnapDrive service access to Windows 54

- SnapDrive service account 54
- Windows domain 54
- Windows host 36
- restore
 - from snapshots 176
 - virtual disks from archives 180
- rolling snapshots
 - and replication 211
 - described 211
 - management of 211
 - naming 211
- rules
 - for connecting to virtual disks 142
 - for creating virtual disks 123
 - for managing virtual disks 122
 - for snapshots 172

S

- SAN (Storage Area Network), definition of 6
- SAN booting
 - about 205
 - how SnapDrive supports 205
- scheduling snapshots 169
- sdcli commands
 - about understanding 224
 - executing 224
 - for iSCSI connection 231
 - for snapshots 242
 - multipathing commands 238
 - switches (options) available for 225
 - disk connect 234
 - disk convert 235
 - disk create 234
 - disk delete 235
 - disk disconnect 236
 - disk expand 236
 - disk list 237
 - iscsi_initiator establish_session 232
 - iscsi_initiator list 232
 - iscsi_initiator terminate_session 233
 - iscsi_target disconnect 231
 - iscsi_target list 229, 231
 - license set 229
 - path activate 202, 239

- path add 202, 239
- path disable 202, 239
- path enable 202, 240
- path list 240
- path remove 202, 240
- path version 241
- preferredIP list 230
- preferredIP set 230
- snap create 242
- snap delete 242
- snap list 243
- snap mount 243
- snap rename 243
- snap restore 244
- snap unmount 244
- snap update_mirror 245
- service account
 - for SnapDrive 54
 - requirements 54
 - Windows domain 54
- service packs
 - SP1 25
- session, iSCSI
 - details 119
 - disconnecting 116
 - ways to establish 112
- sessions, iSCSI
 - establishing 113
- setting a preferred IP address 105
- single-homed configuration, using GbE switch 27
- single-host, single-filer configurations
 - FCP 30
 - iSCSI 26
- snap reserve, recommended setting 16, 49
- SnapDrive
 - administrator access to filer required 54
 - capabilities 8
 - cautions and recommendations 43
 - command-line interface 10
 - command-line interface reference 223
 - components 9
 - configuring filer volumes 44
 - determining what components are installed 38
 - filer options set automatically 41
 - installing components 101

- limitations 42
- preparing to install 21
- selecting configurations 23
- service account 54
- snap reserve on filer 49
- uninstalling 107, 108
- user interfaces 56
- SnapDrive service, stopping and starting
 - stopping and starting the SnapDrive service 105
- SnapMirror
 - asynchronous replication 208
 - connecting to (mirrored) destination volumes 215
 - described 208
 - initiating replication 213
 - license required on filer 41
 - overview 208
 - replication 211
 - requirements for using with SnapDrive 208
 - rolling snapshots 211
 - synchronous replication 208
 - Update Mirror feature 213
 - using with SnapDrive 207
- SnapRestore, licence required on filer 41
- snapshots
 - archival 180
 - connecting to virtual disks (LUNs) 173
 - definition 6
 - deleting 178
 - described 164
 - effect on disk space 17
 - errors when deleting 179
 - how to create 168
 - reason for creating 166
 - replication upon creation of 211
 - requisites for 167
 - restoring from 176
 - restrictions on creating 166
 - rolling 211
 - scheduling 169
 - space required 15
- SP1, feature support 25
- space reservation
 - example 17

- filer setting 16
- overview 16
- states, path (MPIO) 200
- synchronous replication 208

T

- target 6
- Target Portal IP Address field 119
- Target Portal Port field 119
- Telnet
 - description of 56
- Terminal Service 56
 - definition 56
 - drawbacks 56
 - workaround for problems 57

U

- uninstalling
 - FCP driver 108
 - iSCSI initiator 109
 - SnapDrive and MPIO 108
 - SnapDrive components 107
 - VLD driver 107
- Update Mirror feature 213
- upgrading
 - cluster with VLDs 64
 - cluster without VLDs 88
 - filer 100
 - iSCSI initiator 97
 - procedures 60
 - single system with VLDs 69
 - single system without VLDs 92
 - to Windows 2003 62, 63
- user interfaces
 - for SnapDrive and the filer 56
 - recommended for various operations 57

V

- vFilers (virtual filers)
 - SnapDrive limitations 43
 - using with SnapDrive 9
- view
 - details of an iSCSI session 119

- Virtual Disk Service
 - dependency on 8
 - virtual disks
 - capabilities 12
 - connecting to 142
 - converting connected 77
 - converting for MSCS 82
 - converting unconnected 80
 - creating as a quorum 129
 - creating shared 128, 139
 - data access overview 13
 - dedicated filer volume required 44
 - deleting 149
 - disconnecting 146
 - documentation about protocols 22
 - expanding 151
 - expanding quorum disks 152
 - filer interaction 12
 - filer options set on creation and connection 41
 - how to create 123
 - limitations 12
 - LUN-type, definition 6
 - managing, rules about 122
 - not visible when created via Terminal Service 56
 - rules for creating 123
 - snap reserve setting on filer 49
 - VLD-type, definition 6
 - Windows interaction 12
 - virtual filers (vFilers), using with SnapDrive 9
 - VLD driver, uninstalling 107
 - VLDs
 - converting connected 77
 - converting for MSCS 82
 - converting in cluster group 85
 - converting quorum disk 86
 - converting to LUNs 77
 - converting unconnected 80
 - volume
 - connecting to (mirrored) destination 215
 - contents 15
 - creating 45
 - definition 7
 - guidelines for creating 44
 - options set by SnapDrive 41
 - preparation 43
 - recommendations for configuring 44
 - resetting snap reserve 49
 - restricted to single host 44
 - sizing 15
 - VSS
 - requirements 181
- ## W
- WAFL 5
 - Windows 2000 Server cluster. *See* Windows cluster
 - Windows cluster
 - creating a shared virtual disk 128
 - creating a virtual disk as a quorum 129
 - definition of 7
 - FCP configurations 31
 - iSCSI configurations 28
 - Windows domain, requirements 54
 - Windows host
 - administrator access required 54
 - preparing 36
 - requirements 36
 - Windows Server 2003 cluster. *See* Windows cluster
 - Windows Server 2003, supported versions and feature support 25

