

SnapDrive™ 4.1 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 215-01691_A0
April 2006

Copyright and trademark information

Copyright information

Copyright © 1994—2006 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, Data ONTAP, 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. 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, 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.

Table of Contents

Preface	xiii
How to use this Help	xiii
 Chapter 1	
Working with SnapDrive	1
SnapDrive licensable modules	2
Licensing SnapDrive 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
failover	4
filer	4
file system	5
host	5
host bus adapter (HBA)	5
initiator	5
logical unit number (LUN)	5
LUN-type virtual disk	6
Microsoft Cluster Service (MSCS)	6
network interface card (NIC)	6
Snapshot copy	6
storage area network (SAN)	6
target	6
virtual disk	6
VLD-type virtual disk	7
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 storage system interacts with a virtual disk (LUN)	12
How Windows hosts interact with a LUN	12
Virtual disk capabilities and limitations	12
Protocols to access 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 storage system settings	16
What space reservation provides	16
Disk space usage with space reservation	16
What fractional reserve is	19
Icons used in SnapDrive	21

Chapter 2

Preparing to Install SnapDrive	23
What to read	24
Selecting a SnapDrive configuration	25
Recommendations for choosing a configuration	25
Understanding feature availability	26
iSCSI configurations	28
Single host direct-attached to a single storage system	28
Single host attached to a single storage system through a GbE switch	29
Single host attached to a single storage system through a dedicated switch	30
Windows cluster connected to a storage system cluster through a dedicated GbE switch	30
FCP configurations	32
Single host direct-attached to a single storage system	32
Single host attached to a single storage system through a FCP switch	33
Windows cluster attached to a storage system cluster through an FCP switch	33
MPIO configurations	35
Single host direct-attached to single storage system	35
Windows cluster attached to storage system cluster through a switch	36
Preparing hosts	38
Verifying minimum requirements	38
Determining what components are installed	40
Preparing storage systems	42
Verifying minimum storage system requirements	42
Checking storage system licenses	43

Starting FCP and iSCSI services	43
Volume and storage system options set by SnapDrive.	43
SnapDrive-specific limitations	44
Recommendations	45
Preparing a volume for SnapDrive	45
Creating a storage system volume	47
Configuring pass-through authentication for SnapDrive	53
Reasons for configuring pass-through authentication	53
Configuring pass-through authentication	53
Preparing the SnapDrive service account.	57
Types of access to establish	57
SnapDrive user interfaces.	59
SnapDrive user interface capabilities	60

Chapter 3

Installing, Uninstalling, or Upgrading SnapDrive	61
Upgrading to SnapDrive 4.1	62
Upgrading to SnapDrive 4.1 and Windows 2003	63
Upgrade process	63
Upgrading a server cluster to SnapDrive 4.1	65
Upgrade process	65
Preparing for the upgrade	68
Upgrading a single system to SnapDrive 4.1.	70
Upgrade process	70
Installing SnapDrive for the first time	72
Installation process	72
Installing the FCP or iSCSI components	73
Installing the iSCSI Software Initiator.	75
Upgrading the iSCSI Software Initiator	76
Upgrading the storage system	79
Installing the new SnapDrive components	80
Prerequisites	80
Performing unattended SnapDrive installations	85
Unattended install switch descriptions.	85
Examples of unattended install command syntax	87
Setting a preferred IP address for storage system host-name resolution.	88
Stopping and starting the SnapDrive service.	89
Installing SnapDrive on SnapManager verification servers	89
Uninstalling old components	91

	Uninstalling the VLD driver	91
	Uninstalling SnapDrive and MPIO drivers	92
	Uninstalling the FCP driver	92
	Uninstalling the iSCSI Software Initiator	93
Chapter 4	Managing iSCSI Sessions	95
	Tasks for managing iSCSI sessions	96
	Establishing an iSCSI session to a target	97
	iSCSI software initiator node naming standards	97
	Establishing an iSCSI session to a target.	97
	Understanding CHAP authentication	99
	Disconnecting an iSCSI target from a Windows host	100
	Disconnecting a session to an iSCSI target.	101
	Examining details of iSCSI sessions	103
	Examining details of iSCSI sessions.	103
Chapter 5	Creating Virtual Disks	105
	About virtual disk management	106
	Creating a virtual disk	107
	Rules for creating a virtual disk	107
	About volume mount points	107
	Volume mount point limitations	107
	Creating a virtual disk	108
	Creating a shared virtual disk on a Windows cluster.	114
	Creating a virtual disk as a quorum disk on a new Windows cluster.	115
	Creating a virtual disk as a quorum disk on a new Windows 2000 Server cluster.	117
	Creating a virtual disk as a quorum disk on a new Windows Server 2003 cluster.	118
	Creating a shared non-quorum virtual disk on a Windows cluster.	123
Chapter 6	Managing Virtual Disks.	125
	Connecting virtual disks	126
	Connecting a virtual disk.	126
	Making drive letter or path modifications to a virtual disk.	132

Adding or changing a drive letter or path for an existing virtual disk . . .	132
Removing a drive letter or mount point for an existing virtual disk . . .	133
Disconnecting virtual disks	135
Disconnecting a virtual disk	135
Forcing a disconnect	136
Deleting a virtual disk	138
Deleting folders within volume mount points using the Windows Explorer. .	140
Deleting folders within volume mount points	140
Expanding virtual disks.	141
Expanding a virtual disk	142
Expanding a quorum disk	143
Managing LUNs not created in SnapDrive.	146
Prerequisites for SnapDrive to manage LUNs not created in SnapDrive	146
Preparing LUNs not created in SnapDrive in a stand-alone Windows	
configuration	146
Preparing LUNs not created in SnapDrive in a clustered Windows	
configuration	147
Monitoring fractional space reservations.	149
Enabling space reservation monitor e-mail notification	149
Configuring space reservation monitoring.	149
Administering SnapDrive remotely	151
Enabling SnapDrive notification	152

Chapter 7

SnapDrive Snapshot Copies	155
How Snapshot copies work.	156
Creating Snapshot copies.	158
Creating a Snapshot copy	160
Scheduling Snapshot copies	161
Connecting to LUNs in a Snapshot copy.	164
Connecting to a virtual disk (LUN) in a Snapshot copy	165
Restoring virtual disks from Snapshot copies	168
About the Data ONTAP LUN clone feature	168
Benefit of using LUN clones.	169
Restoring a virtual disk from a Snapshot copy.	169
Checking LUN restore status.	170
Deleting Snapshot copies.	172
Deleting a Snapshot copy	172
Problems deleting Snapshot copies due to busy snapshot error	173

	Overview of archiving and restoring Snapshot copies	174
Chapter 8	Overview of the Volume Shadow Copy Service	175
	What Volume Shadow Copy Service is	176
	VSS requirements	176
	Overview of VSS.	176
	Typical VSS backup process.	177
	Troubleshooting the VSS Hardware Provider	179
	NetApp VSS Hardware Provider requirement	179
	Multiple providers installed	179
	Viewing installed VSS providers	179
	Troubleshooting when a Snapshot copy is not made on the storage system. 180	
	Verifying that the VSS Hardware Provider was used successfully	181
	Verifying your VSS configuration	181
Chapter 9	Multipathing	183
	Feature availability	184
	Multipathing overview	185
	SnapDrive MPIO features and requirements.	186
	MPIO setup	188
	Supported MPIO topologies	188
	MPIO path management	193
	Creating an MPIO path.	194
	Understanding MPIO path states.	195
	Changing MPIO path states	196
	Removing MPIO on a Microsoft cluster	197
Chapter 10	SAN Booting with SnapDrive.	199
	What SAN booting is.	199
	How SnapDrive supports SAN booting	199
	Configuring bootable virtual disks	200
Chapter 11	Using SnapMirror with SnapDrive	201
	SnapMirror overview	202
	Understanding replication	202
	Requirements for using SnapMirror with SnapDrive	202

SnapMirror replication	.205
Initiating replication	.207
Connecting to a virtual disk on a destination volume	.209
Reason for connecting to destination volumes.	.209
Requirements for connecting to a virtual disk on a destination volume .209	
Using SnapDrive to meet the requirements for connecting to a destination volume	.209
Connecting to a mirrored destination volume	.209
Recovering a cluster from shared virtual disks on a SnapMirror destination .212	
Connecting to shared virtual disks on a SnapMirror destination. . . .	.213

Appendix A

SnapDrive Command-Line Reference	.219
Using sdcli commands	.220
Executing sdcli commands	.220
Common command switches.	.221
Command-specific switches	.223
SnapDrive configuration commands	.224
SnapDrive license commands	.225
Fractional space reservation monitoring commands	.226
SnapDrive preferred IP address commands	.229
iSCSI connection commands	.230
iSCSI initiator commands	.231
Virtual disk commands	.233
Multipathing commands	.239
Snapshot commands	.243

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™ 4.1 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 ix
- ◆ “[About storage system command execution](#)” on page xi
- ◆ “[Interface conventions](#)” on page xi
- ◆ “[Typographic conventions](#)” on page xii
- ◆ “[Special messages](#)” on page xiii

Audience: This Help is for system administrators who possess a working knowledge of storage systems.

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
- ◆ Storage system management

About storage system command execution: You can manage storage system in the following three ways:

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

Note

The previous three management methods are specific to storage system management only, not to 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 > Microsoft iSCSI Initiator 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, and then double-click Microsoft iSCSI Initiator.

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

Licensing SnapDrive modules

SnapDrive 4.1 enables you to install Data ONTAP 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
- ◆ Both 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 23
- ◆ Chapter 3, “[Installing, Uninstalling, or Upgrading SnapDrive](#),” on page 61
- ◆ Chapter 9, “[Multipathing](#),” on page 183

If you licensed LUN Provisioning and Snapshot Management without MPIO, read everything but Chapter 9.

If you licensed both LUN Provisioning and Snapshot Management and MPIO, read this entire guide.

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 4.1 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 encounter 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
- ◆ “[Microsoft Cluster Service \(MSCS\)](#)” on page 6
- ◆ “[failover](#)” on page 4
- ◆ “[filer](#)” on page 4
- ◆ “[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 copy](#)” 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 7
- ◆ “[volume](#)” on page 7
- ◆ “[Windows Server cluster](#)” on page 7

block pointers

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

failover

Failover refers to situations in which one system component fails, but another component takes over its functions, allowing the system to continue to operate.

filer

A filer is a storage system that supports FCP (Fibre Channel Protocol), iSCSI (Internet SCSI), and GbE (Gigabit Ethernet) protocols.

file system	“File system” refers to NTFS, the native Windows 2000 Server and Windows Server 2003 file system supported by SnapDrive. (NetApp storage systems 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 storage system using Windows procedures only.)
host	A host is a computer system that accesses storage on a storage system. For this document, the host must be running the following software: ◆ One of the following Windows servers: ❖ Windows 2000 Server with Service Pack 4 ❖ Windows 2000 Advanced Server with Service Pack 4 (for Windows-cluster configurations) ❖ Windows Server 2003 with Service Pack 1 (Standard Edition or Enterprise Edition) ❖ Windows Server 2003, x64 versions ◆ SnapDrive 4.1
host bus adapter (HBA)	A host bus adapter (HBA) is the adapter used to connect hosts and storage systems in a NetApp storage area network (SAN) so that hosts can access logical unit numbers (LUNs) on the storage systems using FCP or iSCSI. <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 is a port on an HBA on a host. iSCSI initiator: An iSCSI initiator is a port on an 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.

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.

network interface card (NIC)

A network interface card (NIC) is a Gigabit Ethernet (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 storage systems to a local area network (LAN)
- ◆ Connect hosts and storage systems to data-center switching fabrics: specifically, enable hosts to connect to LUNs on storage systems using iSCSI

Snapshot copy

“Snapshot copy” refers to the Data ONTAP Snapshot technology, which facilitates recovery after accidental deletion or modification of the data stored on a storage system 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 storage systems 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). *See also* target *and* virtual disk.

target

A target is used to receive the SCSI I/O commands that an initiator sends. For SANs, a target is a storage system. *See also* initiator.

virtual disk

A virtual disk is a functional unit of storage system 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) 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 not supported in SnapDrive 4.1 or later versions.

volume

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

Windows Server cluster

A Windows Server cluster is a two-node to 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 two-node cluster)
- ◆ Windows Server 2003 Enterprise Edition (for a two-, three-, or four-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 storage systems 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 storage system, 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 Data ONTAP 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 cannot be configured as an extended partition. SnapDrive supports only a single, primary partition on a virtual disk.

- ◆ Virtual disks created in FilerView or at the storage system 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 146.

SnapDrive virtual boot disk (SAN booting) support

SnapDrive supports both bootable virtual disks (SAN booting) and nonbootable virtual disks. It differentiates between the two in the Microsoft Management Console (MMC) by representing each virtual disk type with a unique icon. For more information, see “[SAN Booting with SnapDrive](#)” on page 199.

SnapDrive cluster support

SnapDrive can be deployed in a nonclustered configuration (a single host connected to a single storage system) 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.
- ◆ fNetApp cluster failover
If a storage system fails, the partner storage system takes over the functions of the failed storage system, 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/>.

Note

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

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

- ◆ SnapDrive “snap-in”
This software module integrates with the Microsoft Management Console (MMC) to provide a graphical interface for managing virtual disks on the storage system. 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 storage system 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 storage system. 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 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 module of the Microsoft VSS framework. The NetApp Hardware Provider enables VSS Snapshot

technology on NetApp storage systems when SnapDrive is installed on Windows 2003 hosts.

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

◆ iSCSI initiator

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

- ❖ It includes an iSCSI driver that supports iSCSI connections between a host and a storage system.
- ❖ 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 storage system. The initiator has the following features:

- ❖ It includes an FCP driver that supports FCP connections between a host and a storage system.
- ❖ 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 section explains how virtual disks work. Go to any of the following topics for more information:

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

How the storage system interacts with a virtual disk (LUN)

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

Note

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

How Windows hosts interact with a LUN

You manage LUNs on the storage system just as you manage other Windows disks that store application data. Similarly, the LUNs on the storage systems 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 storage system; 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 a Snapshot copy 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 unavailable in SnapDrive:

- ◆ Disconnect
- ◆ Delete
- ◆ Expand

Protocols to access LUNs

You can access the SnapDrive-created 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 storage system before you can use these protocols to access virtual disks.

Note

SnapDrive 4.1 supports both FCP and iSCSI on the same Windows host connected to different LUNs. SnapDrive 4.1 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 SAN environment, an initiator (on the Windows host) initiates a SCSI I/O operation to a target (storage system). 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.

Planning disk allocation

This section explains how to plan storage system disk allocation. Go to either 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 storage system volume; in fact, you *should* do so 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 *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 storage system do not belong to any particular volume. In fact, any disk in the storage system that has not yet been assigned to a volume (and has not been marked bad) is treated as a hot spare.

If the storage system 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 storage system as the failed disk.

Always keep at least one hot spare disk in the storage system. This ensures that a spare disk is available at all times. As soon as an active disk fails, the storage system 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 storage system, enable the Data ONTAP AutoSupport feature.

Understanding volume size

This section explains storage system 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 storage system 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, which in turn contain the host data
- ◆ Data that changes between Snapshot copies (Even if all the data on the virtual disks changes following the most recent Snapshot copy, 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 a Snapshot copy 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 Snapshot copies, the entire contents of the disks can be written to the volume. See [“How Snapshot copies work”](#) on page 156 for more information.
- ◆ The volume must also provide enough additional space to hold the number of Snapshot copies you intend to keep online. The amount of space consumed by a Snapshot copy depends on the amount of data that changes after the Snapshot copy is taken. The maximum number of Snapshot copies is 255 per storage system volume.

Requirements for space-related storage system settings

The following space-related settings must be configured on your storage system 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 copy creation. By default, the snap reserve percentage on the storage system 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 51.

What space reservation provides

Space reservation ensures that write operations to a virtual disk always have enough space. Space reservation prevents Snapshot copy creation whenever the storage system 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 in which all writable blocks on the volume are locked by Snapshot copies, and no blocks are available for writing new data.

Disk space usage with space reservation

When you first create a virtual disk 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 storage system volume on which 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 copy of the storage system volume holding the virtual disk, that Snapshot copy locks down all the disk blocks occupied by live data.

By monitoring the remaining available space in the storage system volume, space reservations determine whether Snapshot copy creation is allowed. When the

amount of available space on the storage system 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 storage system 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 copy 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 copy of the virtual disk.	Used: 40 GB Reserved: 40 GB Available: 20 GB Volume Total: 100 GB Snapshot creation succeeds.	The Snapshot copy locks all the data on the virtual disk so that even if that data is later deleted, it remains in the Snapshot copy until the Snapshot copy is deleted. After a Snapshot copy is created, the reserved space must 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 copy 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 make a Snapshot copy now, because no space is available. That is, all space is used by data or held in reserve so that any 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 copy 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 copy, it disappears when the new data replaces it; so the Used total remains unchanged.
Create a Snapshot copy of the virtual disk.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation is allowed.	The Snapshot copy locks all 40 GB of data currently on the virtual disk. A total of 80 GB of data now belongs to the two Snapshot copies of the virtual disk. Reserved space remains equal to the size of the LUN: 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 copy, 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 content of the virtual disk can be written to the volume. Because the available space is now 0, Snapshot copy creation is blocked.
Delete both Snapshot copies.	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 Snapshot copies disappears from the Used total when the Snapshot copies are deleted. Because there are no more Snapshot copies 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 Snapshot copies exist for this volume, deletion of the virtual disk causes the used space to go to 0 GB.

What fractional reserve is

SnapDrive 4.1 enables you to monitor fractional space reservation thresholds when you are using Data ONTAP 7.1 or later. *Fractional reserve* controls the amount of space Data ONTAP reserves in a traditional or flexible volume to enable overwrites to space-reserved LUNs. When you create a space-reserved LUN, fractional reserve is by default set to 100 percent. This means that Data ONTAP automatically reserves 100 percent of the total LUN size for overwrites. For example, if you create a 500-GB space-reserved LUN, Data ONTAP by default ensures that the host-side application storing data in the LUN always has access to 500 GB of space.

You can reduce the amount of space reserved for overwrites to less than 100 percent when you create LUNs in the following types of volumes:

- ◆ Traditional volumes
- ◆ Flexible volumes that have the `guarantee` option set to `volume`.

If the `guarantee` option for a flexible volume is set to `file`, then fractional reserve for that volume is set to 100 percent and is not adjustable.

To set space reservation monitoring in SnapDrive, see “[Monitoring fractional space reservations](#)” on page 149.

For more information about fractional space reservations, see the *Block Access Management Guide*.

Icons used in SnapDrive

The following table displays some of the common icons used by SnapDrive and describes each one.

Icon	Description
	Dedicated LUN
	SAN boot disk
	Clustered LUN
	Mirrored dedicated LUN
	Mirrored clustered LUN
	Read-write LUN in Snapshot copy
	Snapshot copy fail
	iSCSI node

Icon	Description
	MPIO active path
	MPIO passive path.
	MPIO failed path
	MPIO disabled path

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 storage systems
- ◆ 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* storage system 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 24
- ◆ [“Selecting a SnapDrive configuration”](#) on page 25
- ◆ [“iSCSI configurations”](#) on page 28
- ◆ [“FCP configurations”](#) on page 32
- ◆ [“MPIO configurations”](#) on page 35
- ◆ [“Preparing hosts”](#) on page 38
- ◆ [“Preparing storage systems”](#) on page 42
- ◆ [“Configuring pass-through authentication for SnapDrive”](#) on page 53
- ◆ [“Preparing the SnapDrive service account”](#) on page 57

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 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 the iSCSI Host Attach Kit for Windows, the <i>iSCSI Host Attach Kit for Windows Installation and Setup Guide</i>; if you are not, the vendor documentation for your Windows Hardware Quality Lab (WHQL) signed iSCSI HBA ◆ Data ONTAP <i>Block Access Management Guide</i>, which shipped with your storage system
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</i>, which shipped with your storage system

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 32-bit and x64 versions (Standard Edition or Enterprise Edition)
- ◆ Host operating system Service Pack level
 - ❖ For Windows 2000 Server: SP4
 - ❖ For Windows Server 2003, 32-bit: SP1
 - ❖ For Windows Server 2003, x64: no Service Pack at this time
- ◆ 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 26.)
- ◆ Special options (Windows clustering, storage system cluster failover, MPIO)

Go to either of the following topics for more information:

- ◆ [“Recommendations for choosing a configuration”](#) on page 25
- ◆ [“Understanding feature availability”](#) on page 26

Recommendations for choosing a configuration

When deciding which type configuration to use with SnapDrive, keep the following recommendations in mind:

For all configurations, place the host and storage system in the same broadcast domain, so that virtual disk I/O commands do not need to make router hops.

For Windows cluster configurations, segregate internal cluster traffic from both host-storage system traffic and data-center traffic whenever possible.

Do not permit internal cluster traffic on a GbE network used for transferring data from host to storage system. 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, contact technical support.

Related topics:

- ◆ [“Preparing hosts”](#) on page 38
- ◆ [“Preparing storage systems”](#) on page 42

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 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 or Enterprise Edition 32-bit with...		
SP1 with the following hotfixes: ◆ 891957 ◆ 898790 ◆ 902837 ◆ 903081 ◆ 908249 ◆ 911030 ◆ 912848, only if you use an application to extend a partition on Windows Server 2003 and you encounter the problem described in Microsoft Knowledge Base article 912848	Standard features, Windows cluster (two hosts with Standard Edition and up to four hosts with Enterprise Edition), MPIO	Standard features, Windows cluster (up to two hosts with Standard Edition and four hosts with Enterprise Edition), MPIO

Windows Server 2003 R2 Standard or Enterprise Edition 32-bit with...		
The following hotfixes: ◆ 891957 ◆ 898790 ◆ 902837 ◆ 903081 ◆ 908249 ◆ 911030 ◆ 912848, only if you use an application to extend a partition on Windows Server 2003 and you encounter the problem described in Microsoft Knowledge Base article 912848	Standard features, Windows cluster (two hosts with Standard Edition and up to four hosts with Enterprise Edition), MPIO	Standard features, Windows cluster (up to two hosts with Standard Edition and four hosts with Enterprise Edition), MPIO
Windows Server 2003 Standard or Enterprise Edition x64 versions, including R2, with...		
The following hotfixes: ◆ 891957 ◆ 898790 ◆ 902837 ◆ 903081 ◆ 908249 ◆ 911030 ◆ 912848, only if you use an application to extend a partition on Windows Server 2003 and you encounter the problem described in Microsoft Knowledge Base article 912848	Standard features, Windows cluster (two hosts with Standard Edition and up to four hosts with Enterprise Edition), MPIO	Standard features, Windows cluster (up to two hosts with Standard Edition and four hosts with Enterprise Edition), MPIO
Note_____ For a list of the latest service packs and hotfixes required by SnapDrive, see the SnapDrive 4.1 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 storage system”](#) on page 28
- ◆ [“Single host attached to a single storage system through a GbE switch”](#) on page 29
- ◆ [“Single host attached to a single storage system through a dedicated switch”](#) on page 30
- ◆ [“Windows cluster connected to a storage system cluster through a dedicated GbE switch”](#) on page 30

Related topics:

- ◆ [“FCP configurations”](#) on page 32
- ◆ [“MPIO configurations”](#) on page 35
- ◆ [“Understanding feature availability”](#) on page 26

Single host direct-attached to a single storage system

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

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

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

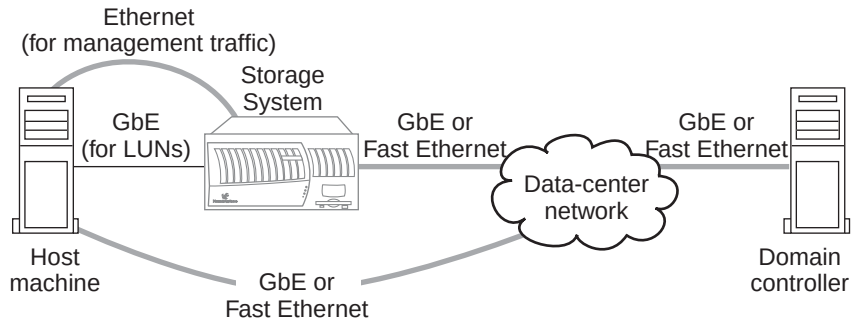
Note

Both the storage system 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, for best results, you should separate the traffic as shown in the following illustration.

Windows requirements: For Windows OS and hotfix requirements for iSCSI, see [“Understanding feature availability”](#) on page 26.



Single host attached to a single storage system through a GbE switch

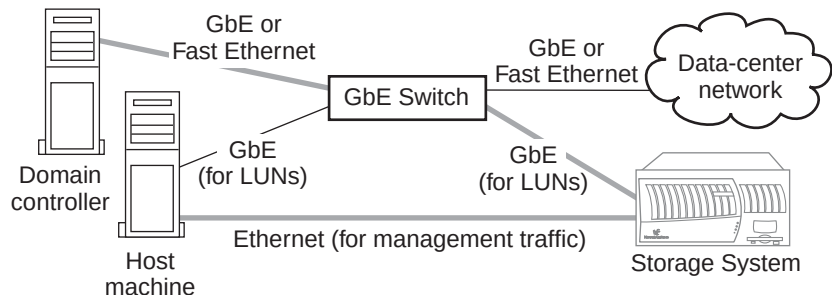
The following illustration depicts a single-homed configuration that places a network switch between the storage system and the host. Such an arrangement provides good performance and also segregates host-storage system traffic by directing it through a single pair of switch ports.

Because the switch connects to the data-center fabric, the host and storage system in this configuration each use a single GbE NIC both for host-storage system 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, for best results, you should separate the traffic as shown in the following illustration.

Windows requirements: For Windows OS and hotfix requirements for iSCSI, see “[Understanding feature availability](#)” on page 26.



Single host attached to a single storage system through a dedicated switch

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

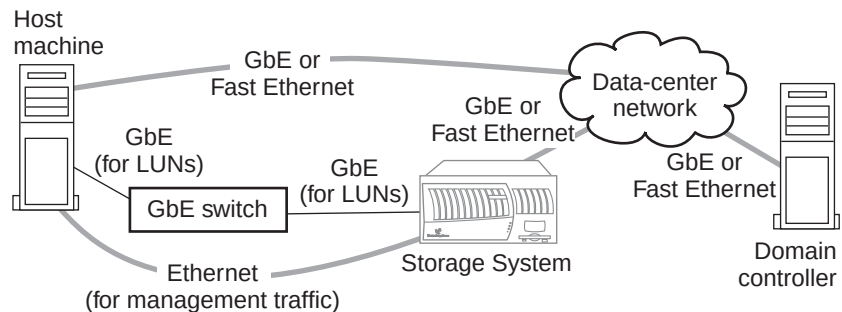
The host and storage system in this configuration each use the following hardware for the connection:

- ◆ 1 GbE NIC dedicated to host-storage system 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, for best results, you should separate the traffic as shown in the following illustration.

Windows requirements: For Windows OS and hotfix requirements for iSCSI, see “[Understanding feature availability](#)” on page 26.



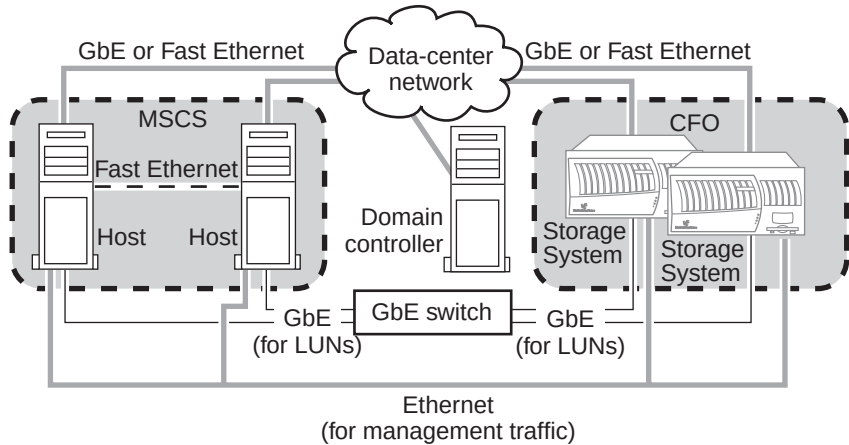
Windows cluster connected to a storage system cluster through a dedicated GbE switch

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

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

Note

LUN traffic and management traffic in an iSCSI configuration can be performed over a single GbE connection; however, for best results, you should separate the traffic as shown in the following illustration.



Windows requirements: For Windows OS and hotfix requirements for iSCSI, see “[Understanding feature availability](#)” on page 26.

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 storage system”](#) on page 32
- ◆ [“Single host attached to a single storage system through a FCP switch”](#) on page 33
- ◆ [“Windows cluster attached to a storage system cluster through an FCP switch”](#) on page 33

Related topics:

- ◆ [“iSCSI configurations”](#) on page 28
- ◆ [“MPIO configurations”](#) on page 35
- ◆ [“Understanding feature availability”](#) on page 26

Single host direct-attached to a single storage system

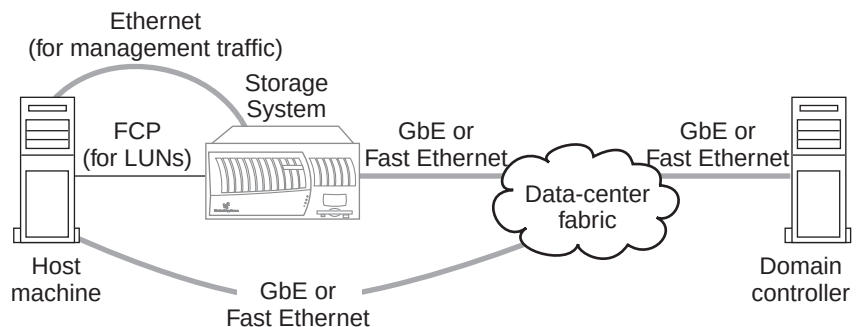
The following illustration shows a configuration that uses a crossover FCP cable to attach the host directly to the storage system.

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

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

Caution

For this configuration, both the storage system 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 26.

Single host attached to a single storage system through a FCP switch

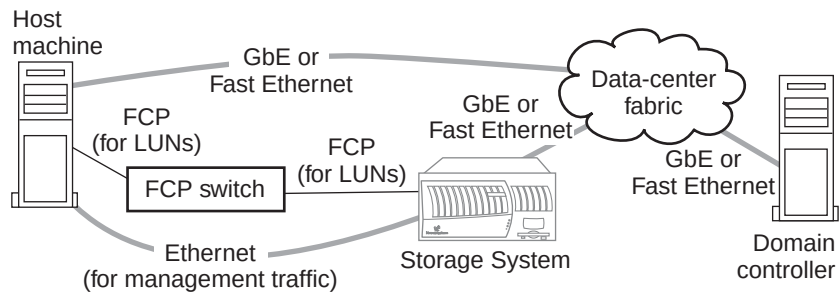
The configuration in the following illustration uses a dedicated FCP switch to handle all host-storage system data traffic for LUNs.

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

- ◆ 1 HBA to transfer LUN data between storage system 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, for best results, you should separate the traffic as shown in the following illustration.

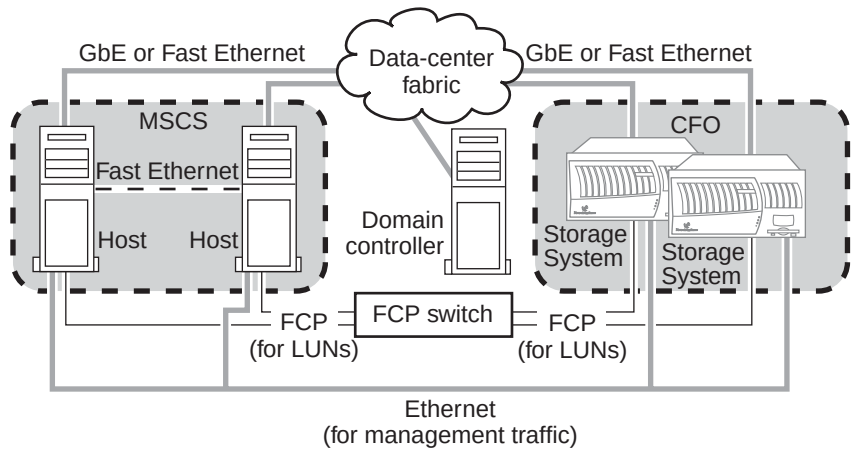


Windows requirements: For Windows OS and hotfix requirements for FCP, see “[Understanding feature availability](#)” on page 26.

Windows cluster attached to a storage system cluster through an FCP switch

The following illustration depicts a configuration that employs both a Windows cluster and a storage system 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 storage systems or storage system clusters.



Windows requirements: For Windows OS and hotfix requirements for FCP, see “[Understanding feature availability](#)” on page 26.

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 storage system”](#) on page 35
- ◆ [“Windows cluster attached to storage system cluster through a switch”](#) on page 36

Related topics:

- ◆ [“iSCSI configurations”](#) on page 28
- ◆ [“FCP configurations”](#) on page 32
- ◆ [“Understanding feature availability”](#) on page 26
- ◆ [“MPIO setup”](#) on page 188

Single host direct-attached to single storage system

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

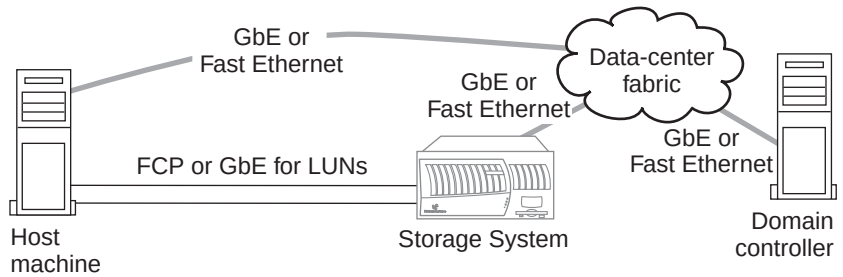
The host and storage system in this configuration each use the following connection hardware:

- ◆ 2 FCP HBAs to transfer multipathed LUN data between storage system 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 storage system. The storage system 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 storage system using either FCP or iSCSI over MPIO.



Windows requirements: For Windows OS and hotfix requirements for MPIO, see “[Understanding feature availability](#)” on page 26.

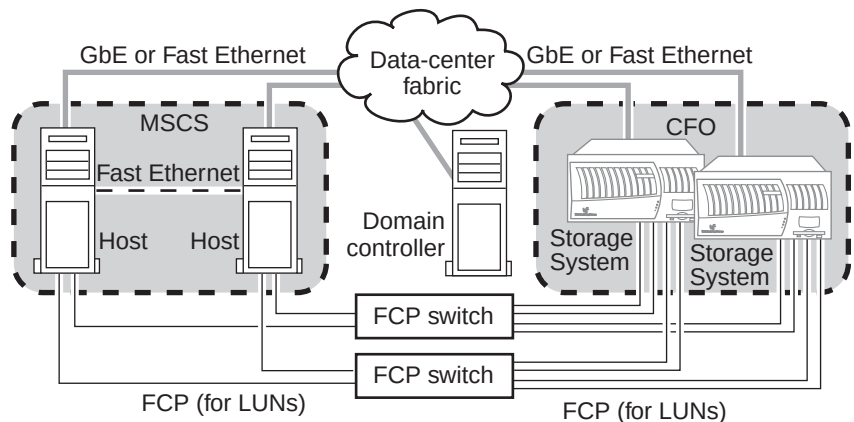
Windows cluster attached to storage system cluster through a switch

FCP configuration: The configuration in the following diagram employs both a Windows cluster and a storage system 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 storage system 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 storage system in this configuration requires two 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 details.)

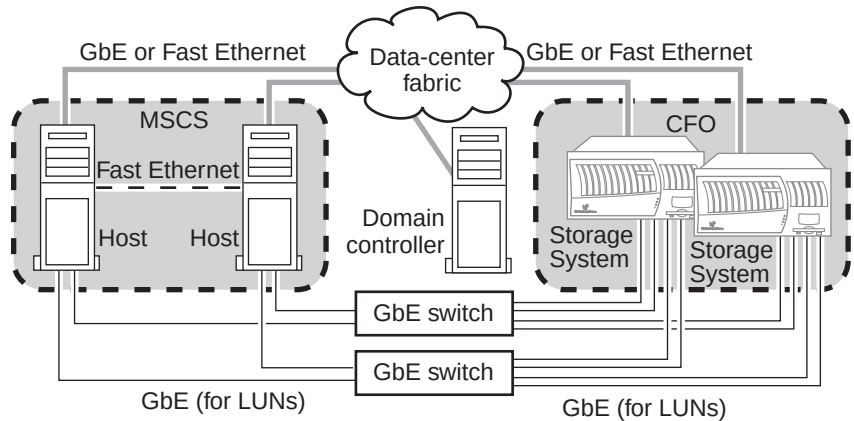


iSCSI configuration: The configuration in the following diagram employs both a Windows cluster and a storage system cluster connected through a GbE switch. The diagram also pictures an optional, but recommended, dedicated network for all internal cluster traffic.

Each host in this configuration uses the following connection hardware:

- ◆ Two GbE (or two iSCSI HBAs) to transfer multipathed LUN data between storage system 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 storage system 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 details.)



Windows requirements: For Windows OS and hotfix requirements for MPIO, see “[Understanding feature availability](#)” on page 26.

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 38 for more information.

Related topics:

- ◆ “[Preparing storage systems](#)” on page 42
- ◆ “[Preparing the SnapDrive service account](#)” on page 57

Verifying minimum requirements

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

Component	Requirement	
CPU	32-bit	64-bit
	2.8 GHz Pentium 4 or compatible	Intel® Xeon® or AMD Opteron™
Memory	1 GB	

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 at: http://now.netapp.com/NOW/cgi-bin/software/ For a list of the latest compatible software for SnapDrive 4.1, 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 26.

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 25.

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, as follows:

- ◆ The NIC you use to facilitate data transfer for the Microsoft iSCSI Software Initiator can come from any vendor, but it 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.

- ◆ The latest iSCSI driver and firmware from NOW at <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 74.

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 72 for more information.
	Multipath support is not listed	See “ Installing the new SnapDrive components ” on page 79 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, Uninstalling, or Upgrading SnapDrive ,” on page 61.

Preparing storage systems

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

- ◆ The storage systems are online.
- ◆ The storage systems are running at least Data ONTAP 7.0.2.
- ◆ The HBAs and NICs in your storage systems meet the requirements for your particular host-target SnapDrive configuration.

Note

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

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

Go to any of the following topics for more information:

- ◆ “[Verifying minimum storage system requirements](#)” on page 42
- ◆ “[Checking storage system licenses](#)” on page 43
- ◆ “[Volume and storage system options set by SnapDrive](#)” on page 43
- ◆ “[SnapDrive-specific limitations](#)” on page 44
- ◆ “[Recommendations](#)” on page 45
- ◆ “[Preparing a volume for SnapDrive](#)” on page 45

Related topics:

- ◆ “[Preparing hosts](#)” on page 38
- ◆ “[Preparing the SnapDrive service account](#)” on page 57

Verifying minimum storage system requirements

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

Component	Minimum requirement
Operating system	Data ONTAP 7.0.2

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 Snapshot copies ◆ 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 storage system, you must install a separate CIFS license on that storage system.

Checking storage system licenses

You can determine which licenses are enabled on your storage system (and enable additional licenses) by opening FilerView in your Web Browser and then navigating to Filer > Manage Licenses. Alternatively, you can connect to the storage system through a Telnet session and issue the license command at the storage system prompt. Use the `license add code` command to enable a license at the storage system 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 storage system, you must start the services by entering the `fcpl start` command or the `iscsi start` command at the storage system command line. See the *Block Access Management Guide* for more information.

Volume and storage system options set by SnapDrive

SnapDrive checks (and resets) various storage system 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; you should *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 copy) ◆ Snapshot copy 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
Storage system	Snapshot copy schedule	Off	◆ Disk creation ◆ Disk connection

Note

SnapDrive checks the space-reservation setting for the target LUN when a Snapshot copy is made. If space reservation is disabled, SnapDrive attempts to enable it; if the attempt fails, no Snapshot copy 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.

Recommendations

Heed the following recommendations whenever you use SnapDrive:

- ◆ Use SnapDrive to create and manage all the virtual disks on your storage system.
- ◆ *Never* disable the space reservation setting for any virtual disk managed by SnapDrive.
- ◆ *Do* set the snap reserve setting on the storage system 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 storage system interface you intend, configure each network interface by *IP address*, rather than by name.
- ◆ If you use Snapshot copies, you cannot use the entire space on a storage system volume to store your virtual disk.

The storage system 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 storage system 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 storage system 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 storage system, you must install a separate CIFS license on that storage system.

- ◆ 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 storage system (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*.

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

- ◆ You can create multiple virtual disks on a storage system volume.
- ◆ A virtual disk must reside at either the root of a volume (traditional or flexible) or the root of a qtree.

Note

Do not create virtual disks on the root volume.

Optimizing your storage system volumes: You can optimize your storage system volumes in the following ways:

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

For more information about this recommendation, see “[Reasons for creating Snapshot copies using SnapDrive](#)” on page 158.

- ◆ When multiple virtual disks exist on a storage system 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 Snapshot copies are consistent and to avoid the possibility of busy Snapshot copies.

Creating a storage system volume

To create a volume on the storage system, complete the following steps.

Step	Action
1	Using your Web Browser, open a FilerView session to the storage system on which you are creating the volume. Example: Enter http://accounting-filer2/na_admin/ 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>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 48.) Reset the snap reserve option for this dedicated virtual disk-storage volume to 0 percent. (See “ Resetting the snap reserve option ” on page 51.)

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

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

Step	Action
1	Using your Web Browser, open a FilerView session to the storage system on which you are creating the volume. Example: Enter http://accting-filer2/na_admin/ in the Address field of your Web browser.
2	From the main FilerView menu, navigate to Volumes > Qtrees > Add.

Step	Action
3	Complete the FilerView transaction to add the qtree. See the FilerView Help and the <i>Storage Management Guide</i> for information about the fields.

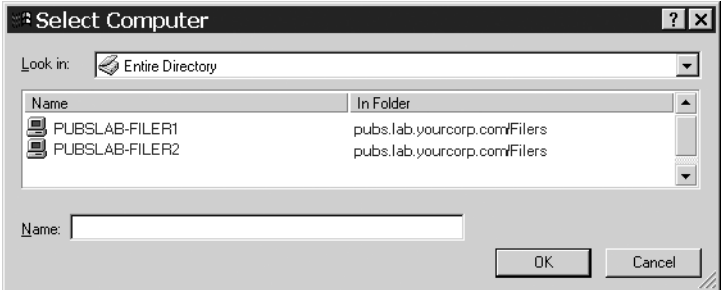
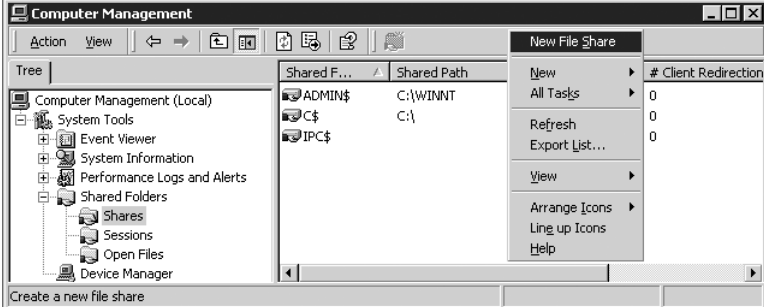
Note

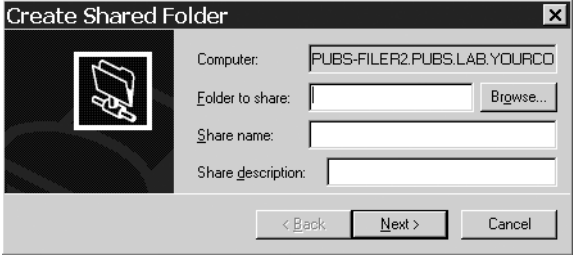
You can create virtual disks at the root of a qtree, but virtual disks do not support the storage system's qtree *quota* capability.

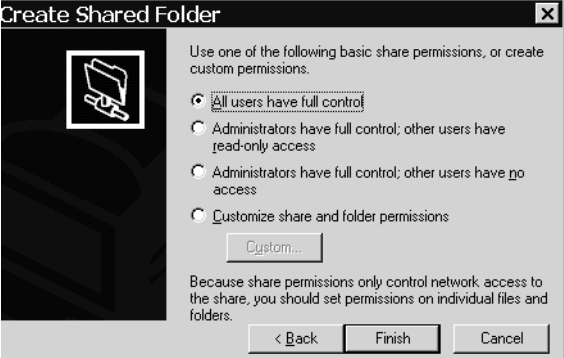
You can also create a qtree by opening a Telnet session and issuing the qtree create *path* command at the storage system prompt. See the *Storage Management Guide* for details.

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 storage system. For SnapDrive to operate properly, the storage system's CIFS (NetBIOS) name must exactly match the storage system listed (UNIX host name). For more information about running CIFS setup, see your Data ONTAP <i>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 storage system 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 and then select “New File Share...” 

Step	Action
9	In the “Folder to share” field of the Create Shared Folder panel, type the following: c:\vol\volname\ <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 and then click Next.

Step	Action
12	Select the appropriate permissions and 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 storage system 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 is 20 percent. You should 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 storage system 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.
4	In the space reservation field, enter 0.

Step	Action
5	Click Apply.

You can also reset the snap reserve option by opening a Telnet session and issuing the `snap reserve vol_name 0` command at the storage system prompt. See the *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 53
- ◆ [“Configuring pass-through authentication”](#) on page 53

Reasons for configuring pass-through authentication

You can use pass-through authentication between a Windows host and a storage system. 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 stand-alone server in a workgroup environment without any dependency on another system for authentication, even if there is a domain controller available.
- ◆ Your Windows host and the storage system are in two different domains.
- ◆ Your Windows host is in a domain and you want to keep the storage system in a workgroup with no direct access by domain users or domain controller.

Related topics:

- ◆ [“Preparing hosts”](#) on page 38
- ◆ [“Preparing storage systems”](#) on page 42

Configuring pass-through authentication

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

Note

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

Step	Action
On the storage system	
1	Enter the following command to create a user account: <pre>useradmin user add <i>user_name</i> -g <i>group</i></pre> <i>user_name</i> is the name of the SnapDrive user. -g is the option you use to specify a user group. <i>group</i> is the name of the group to which you want to add the new user. Example: The following example will add a user called snapdrive to the BUILTIN\Administrators group on the storage system. <pre>useradmin user add snapdrive -g Administrators</pre> 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 letter case—lowercase or uppercase—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 this exact password in a later step in this procedure. Therefore, make a note of the password, including the letter case. _____

Step	Action
3	Check to ensure that the user account you just created belongs to the local administrator's group on the storage system by entering the following command: <pre>useradmin user list</pre> For information about how to assign a user account to a specific storage system group, see “Types of access to establish” on page 57. For additional information, see the section about creating local groups on the storage system in the <i>Data ONTAP File Access Management Guide</i>.
4	Create a CIFS share on the storage system, as described in “Creating a CIFS share” on page 48.
On each Windows host that needs access to the storage system	
5	Create a local user account, using the same user name and password that you specified in Step 1 and Step 2. Tip: Set up the local user account so that the password for the account never expires. For detailed instructions on 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 71. 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 storage system can be in a different domain or workgroup. _____

Step	Action
7	If your Windows host has existing LUNs on a storage system in a domain, disconnect them before setting up your host to work with a storage system in a workgroup; otherwise, the LUNs in the domain will not show up under SnapDrive in the MMC, and SnapDrive might hang. This is because your host can connect only to LUNs on storage systems in a workgroup or to LUNs on storage systems in a domain, but not both.

Preparing the SnapDrive service account

Before installing SnapDrive, you must establish a SnapDrive service account. The service account must be created using ASCII characters only, even when you use non-ASCII operating systems. You must log in to this account whenever you need to perform SnapDrive-related functions on either a host or a storage system. See “[Types of access to establish](#)” on page 57 for more information.

Related topics:

- ◆ “[Preparing hosts](#)” on page 38
- ◆ “[Preparing storage systems](#)” on page 42

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.
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 storage system 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 storage system 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 belong to the BUILTIN\Administrators group on the storage system.

You can accomplish this in several ways, including connecting a Remote Administration session to the storage system 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, and then select the storage system 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 storage system volumes on which virtual disks are stored.

You enable such access by creating a share on the storage system 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 48.

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 storage system management utility.
- ◆ *Storage system console* refers to the command-line prompt of a console attached directly to the storage system.
- ◆ *Telnet session* refers to the command-line prompt of a Telnet session connected to the storage system.
- ◆ *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 SnapDrive user interfaces:

- ❖ The GUI interface of the SnapDrive plug-in
 - ❖ `sdccli.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 out of the Terminal Service session and then log in again.

Note

You must actually log out of the system and log back in; 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 ◆ Storage system console ◆ Telnet session to the storage system ◆ Remote Management session to the storage system
Creating and managing volumes and qtrees	◆ FilerView ◆ Storage system console ◆ Telnet session to the storage system
SnapDrive-related SnapMirror operations	◆ FilerView ◆ Storage system console ◆ Telnet session to the storage system
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 4.1, or to uninstall any version of SnapDrive.

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 4.1](#)” on page 62.
- ◆ If no version of SnapDrive is installed, follow the instructions in the section “[Installing SnapDrive for the first time](#)” on page 71.
- ◆ If you want to uninstall SnapDrive components that you no longer need, follow the instructions in the section “[Uninstalling old components](#)” on page 91.

Upgrading to SnapDrive 4.1

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

If you are not using VLD-type virtual disks: You can upgrade directly to SnapDrive 4.1 from SnapDrive 4.0, 3.2, 3.1, 3.0, 2.1, or 2.0.1, if you have no VLD-type virtual disks.

You can confirm which 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 converted to LUN-type virtual disks using SnapDrive 4.1. If you are using VLDs, upgrade from 2.0.1 or 2.1 to SnapDrive 3.1.1 or 3.2 using the upgrade and conversion process described in the documentation for the release to which you are upgrading; then upgrade to SnapDrive 4.1.

Which procedure to follow: How you upgrade to SnapDrive 4.1 depends on the components of SnapDrive you are currently using and on your Windows configuration.

To upgrade...	Follow procedures under...
A single system with only LUN-type virtual disks connected	“Upgrading a single system to SnapDrive 4.1” on page 69
A Microsoft Windows server cluster with only LUN-type virtual disks connected	“Upgrading a server cluster to SnapDrive 4.1” on page 65
A single system or server cluster to SnapDrive 4.1 and Microsoft Server 2003 Edition	“Upgrading to SnapDrive 4.1 and Windows 2003” on page 63

Upgrading to SnapDrive 4.1 and Windows 2003

Use this section if you intend to upgrade a single Windows system or server cluster to SnapDrive 4.1 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.

Attention

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. 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 4.1 and Windows Server 2003, complete the following stages.

Attention

If you are upgrading to the 64-bit version of SnapDrive, you must first upgrade to Windows Server 2003, x64 Edition. See your Microsoft documentation for more information.

Stage	Process
1	Upgrade to SnapDrive 4.1. Choose one of the following options: ◆ To upgrade a single system that has only LUN-type virtual disks, see “Upgrading a single system to SnapDrive 4.1” on page 69. ◆ To upgrade a server cluster with only LUN-type virtual disks connected, see “Upgrading a server cluster to SnapDrive 4.1” on page 65.

Stage	Process
2	Uninstall the VLD driver. See “ Uninstalling old components ” on page 91.
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 4.1

Use this section only if your Microsoft server cluster is currently running SnapDrive 3.0, 3.1.1, 3.2, or 4.0 and you are not using VLD-type virtual disks.

Note—
You cannot convert VLD-type virtual disks to LUN-type virtual disks using SnapDrive 4.1. If you have VLD-type virtual disks, you must convert them using a version of SnapDrive earlier than 4.x before upgrading to SnapDrive 4.1.

Upgrade process

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

Stage	Process
1	Plan and announce downtime. Pick a time for the upgrade when loss of access will have the least effect on your users. 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 4.1 (see “Selecting a SnapDrive configuration” on page 25).
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. Note— If the cluster service is not running, SnapDrive will be unable to collect data necessary for disk enumeration and will cause warning messages to be logged in the Event Viewer.
4	Prepare your cluster for the upgrade. See “Preparing for the upgrade” on page 67.

Stage	Process
5	If necessary, upgrade Data ONTAP on the storage system. If an upgrade is necessary, you will have to reboot storage system. See “Upgrading the storage system” on page 78.
6	If you are running the DataFabric® Manager Host Agent, stop the DataFabric Manager Host Agent service. Note _____ You may have to upgrade your DataFabric Manager Host Agent depending on the version you are running. See the <i>SnapDrive 4.1 for Windows Release Notes</i> for more information. _____
7	Stop the SnapDrive service and ensure the MMC is closed.

Stage	Process
8	Install the components you need for FCP or iSCSI (see “Selecting a SnapDrive configuration” on page 25 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 74. ◆ 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 4.1, see the SnapDrive Compatibility List at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/.

Stage	Process
9	Install SnapDrive 4.1 on both nodes, starting with the node that does not own the SnapDrive resources. See “Installing the new SnapDrive components” on page 79. The upgrade might 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.
10	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 91.
11	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 38. If you need to apply a new Service Pack or hotfix, you will have to reboot the cluster.
3	Create a full backup, including system state, and create an emergency repair disk for each node before upgrading to SnapDrive 4.1.

Upgrading a single system to SnapDrive 4.1

Use this section only if you are currently running SnapDrive 3.0, 3.1.1, 3.2, or 4.0 and you are not using VLD-type virtual disks.

Note

You cannot convert VLD-type virtual disks to LUN-type virtual disks using SnapDrive 4.1. If you have VLD-type virtual disks, you must convert them using a version of SnapDrive earlier than 4.0 before upgrading to SnapDrive 4.1.

Upgrade process

Follow this process to upgrade a system without VLD-type virtual disks to SnapDrive 4.1.

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 72.
2	Create a full backup, including system state, and create an Emergency Repair Disk.
3	If necessary, upgrade Data ONTAP on the storage system. If an upgrade is necessary, you will have to reboot the storage system and return to Step 6 . See “Upgrading the storage system” on page 78.
4	If you are running the DataFabric® Manager Host Agent, stop the DataFabric Manager Host Agent service. Note — You may have to upgrade your DataFabric Manager Host Agent depending on the version you are running. See the <i>SnapDrive 4.1 for Windows Release Notes</i> for more information.
5	Stop the SnapDrive service and ensure the MMC is closed.
6	Install SnapDrive 4.1. See “Installing the new SnapDrive components” on page 79.

Stage	Process
7	Uninstall the VLD driver if it is still installed. (It might be on your system even if you have not used it recently.) See “ Uninstalling old components ” on page 91.

Installing SnapDrive for the first time

Use this section to install SnapDrive 4.1 if no previous version of SnapDrive or VLD Manager is installed on your system.

Installation process Follow this process to install SnapDrive 4.1 for the first time.

Stage	Process
1	If necessary, upgrade Data ONTAP on your storage system.
2	Install the required version of the iSCSI Software Initiator, iSCSI HBA, or FCP components. See “ Installing the FCP or iSCSI components ” on page 72.
3	Install SnapDrive 4.1. See “ Installing the new SnapDrive components ” on page 79. In a server cluster, install SnapDrive on all nodes.

Installing the FCP or iSCSI components

Supported protocols: SnapDrive 4.1 supports two protocols for creating and managing virtual disks: 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 4.1, 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 74.
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 74.
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 4.1, 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. Do not install Microsoft MPIO Multipathing Support for iSCSI. SnapDrive 4.1 provides this support when you choose to license and install the SnapDrive MPIO feature. Note The Virtual Port Driver option is grayed out because it is automatically installed during the Microsoft iSCSI Initiator installation and upgrade.
4	Follow the directions in the installer wizard to install the Microsoft iSCSI Initiator. For more information about installing and configuring the Microsoft iSCSI Initiator, see <i>iSCSI Microsoft Windows Initiator Support Kit 2.0 Setup Guide</i>. This document is on the NOW site (http://now.netapp.com/).

Upgrading the iSCSI Software Initiator

Choose one of the following procedures to upgrade your Microsoft iSCSI Software Initiator depending on whether you are using a stand-alone host or a Windows cluster.

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 89.

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 74.
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 74.

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 storage system

Note

If a storage system upgrade is necessary, upgrade the storage system before installing SnapDrive. For more information, see “[Preparing storage systems](#)” on page 42.

SnapDrive 4.1 requires at least Data ONTAP 7.0.2 on the storage system. For a list of the latest compatible software for SnapDrive 4.1, see the SnapDrive Compatibility Matrix at:

http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/

To upgrade the storage system, complete the following steps.

Step	Action
1	Upgrade the storage system to at least Data ONTAP 7.0.2. See the <i>Data ONTAP Upgrade Guide</i> for details.
2	When the storage system 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

Prerequisites

The following prerequisites must be met in order to successfully install the new SnapDrive components:

- ◆ Perform this procedure from the system console, not from a Terminal Service client.
- ◆ Convert VLD-type virtual disks to LUN-type disks before installing SnapDrive 4.1. If you are upgrading from an earlier version of SnapDrive and you have VLD-type virtual disks, you will not be able to proceed with the installation because SnapDrive 4.1 does not support VLD-type virtual disks.
- ◆ In a cluster, install SnapDrive 4.1 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.

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

Note

If you previously installed the IBM version of SnapDrive, the installer will not allow you to upgrade to a NetApp version of the software.

Note

If you are upgrading or installing SnapDrive to support a SnapManager installation, see “[Installing SnapDrive on SnapManager verification servers](#)” on page 89.

Step	Action
1	Make sure that you have installed the required FCP or iSCSI components. See “Installing the FCP or iSCSI components” on page 72. Note _____ If you will be using the iSCSI initiator, you might see a message after the SnapDrive installation has completed stating that SnapDrive will modify the MaxRequestHoldTime parameter. This setting modifies the timeout value to ensure proper cluster failover operation. It is recommended that you reboot your system after installing all your SnapDrive components.
2	If you are running the DataFabric Manager Host Agent, stop the DataFabric Manager Host Agent service.
3	Stop the SnapDrive service, if you have not already done so, and close the Microsoft Management Console (MMC) window. See “Stopping and starting the SnapDrive service” on page 89.
4	Browse to the location of the SnapDrive installation package and double-click SnapDrive4.1.exe.
5	Click Next on the “Welcome to the InstallShield Wizard for SnapDrive” screen.
6	If this is a new SnapDrive installation, accept the license agreement and click Next.
7	If you are upgrading SnapDrive, the Program Maintenance panel appears. Click Modify/Upgrade, and then click Next.
8	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.

Step	Action	
9	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 72), and then restart the SnapDrive InstallShield Wizard.
10	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.
11	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.
12	In the Customer Information panel, type your user name and organization name, and then click Next.	

Step	Action	
13	The Destination Folder panel prompts you for a directory in which to install SnapDrive on the host. By default, this is C:\Program Files\NetApp\SnapDrive\ for new installations. To accept the default, click Next and then proceed to Step 14. 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. Note If you are upgrading SnapDrive from a version earlier than 4.1, the default installation directory is C:\Program Files\SnapDrive\.	
14	On the SnapDrive Service Credentials screen, click Add. Result: The Select User window is displayed.	
15	If you are installing or upgrading SnapDrive for use with a storage system in...	Then in the “From this location” field...
	A domain	Verify that the location is set to the proper domain.
	A workgroup	Click the Locations button and select the local host.
16	In the “Enter the object name to select” text box, type the user name with administrator privileges that you want to use; then click the Check Names button to verify the user you entered. Click OK. Note If you are installing SnapDrive for use with a storage system in a workgroup, enter the name of the user that you configured in “Configuring pass-through authentication” on page 53.	

Step	Action
17	Type the account password in both the Password and Confirm Password text boxes; then click Next.
18	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 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 4.1 installation, an updated NetApp VSS hardware provider will be installed.
19	When the InstallShield Wizard Complete screen appears, click Finish.
20	If you are installing or upgrading the MPIO drivers, the SnapDrive Installer Information pop-up screen appears. Click Yes to reboot the machine.
21	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.
22	If you will be creating and managing LUNs using the iSCSI protocol, establish an iSCSI connection to the storage system. See “Establishing an iSCSI session to a target” on page 97.

Performing unattended SnapDrive installations

To simplify installations when you have multiple systems, you can create batch scripts to perform an unattended install or uninstall of SnapDrive.

To perform an unattended SnapDrive installation, complete the following steps.

Step	Action
1	Copy the SnapDrive executable to your Windows host.
2	Create a batch file (a file with a .bat extension) containing the appropriate switch combinations for your unattended install. See “Examples of unattended install command syntax” on page 87 to view some of the available syntax options.

Unattended install switch descriptions

The following table contains the switches you can use when performing an unattended install and a description of each switch.

Switch	Description
/s /v	Invokes SnapDrive installation in unattended or silent mode.
"/qn"	Enables you to pass arguments and other SnapDrive installation-specific switches and parameters.
SILENT_MODE=1	Enables SnapDrive to properly execute the unattended install feature. This switch is required for first-time installs, upgrades, and complete uninstalls.
LPSM_SERIALNUMBER=	Specifies that a valid LUN Provisioning and Snapshot Management license be entered.
MPIOLICENSECODE=	Specifies that a valid MPIO license be entered.
INSTALLDIR= <i>target installation directory</i>	Specifies the target installation directory to which SnapDrive will be installed. This switch is only required when installing SnapDrive for the first time
SVCUSERNAME= <i>DOMAIN\USERNAME</i>	Specifies the domain and username that SnapDrive will use during the unattended install.
SVCUSERPASSWORD= <i>PASSWORD</i>	Specifies the password that will be used by SnapDrive.

Switch	Description
SVCCONFIRMUSEROPASSWORD= <i>PASSWORD</i>	Specifies the confirmation password for the user being used for the unattended install.
REINSTALLMODE=vomus	Specifies the type of reinstall mode to be used: v indicates that the installation should be run from the source package and to cache the local package. Note Do not use the v option for first time installations of SnapDrive. o reinstalls SnapDrive if an older version is present or if SnapDrive files are missing. m indicates that all SnapDrive required registry entries FROM HKEY_LOCAL_MACHINE and HKEY_CLASSES_ROOT should be rewritten. u indicates that all SnapDrive required registry entries from HKEY_CURRENT_USER and HKEY_USERS should be rewritten. s reinstalls all shortcuts and re-caches all icons, overwriting any existing shortcuts and icons.
REINSTALL=ALL	Reinstalls all SnapDrive features.
/x	Removes SnapDrive from your system.
/Li	Specifies that a SnapDrive installation log should be generated.
IGNORE_COMPMGMT_RUNNING=0	Specifies that the SnapDrive installation will abort if the MMC is open and a message is displayed indicating that the MMC must be closed.
IGNORE_COMPMGMT_RUNNING=1	Specifies that the SnapDrive installation will proceed even if the the MMC is open. If no switch is specified, the SnapDrive installation will abort if the MMC is open and a message is displayed indicating that the MMC must be closed.

Switch	Description
REBOOT=F	Specifies that a reboot should be forced with no user confirmation. Note —— If you do not use REBOOT=F during an unattended install, you will have to reboot your system manually. SnapDrive may not work properly until your system is rebooted.
CUSTOMHELP=1	Displays usage information for all unattended install switches.

Examples of unattended install command syntax

The following are examples of the common syntax variations of the unattended install command.

Command syntax for a complete SnapDrive installation (both LUN Provisioning and Snapshot Management and MPIO):

```
snapdrive4.1.exe /s /v"/qn SILENT_MODE=1 REBOOT=F /Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber MPIO_LICENSECODE=license
INSTALLDIR="C:\Program Files\NetApp\SnapDrive\"
SVCUSERNAME=domain\username SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password"
```

Command syntax for a LUN Provisioning and Snapshot Management-only installation:

```
snapdrive4.1.exe /s /v"/qn SILENT_MODE=1 REBOOT=F /Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber INSTALLDIR="c:\Program Files\
NetApp\SnapDrive\" SVCUSERNAME=domain\username
SVCUSERPASSWORD=password SVCCONFIRMUSERPASSWORD=password"
```

Command syntax for MPIO-only installation:

```
snapdrive4.1.exe /s /v"/qn SILENT_MODE=1 REBOOT=F /Li
SDInstall.log MPIO_LICENSECODE=license INSTALLDIR="c:\Program
Files\NetApp\SnapDrive\" SVCUSERNAME=domain\username
SVCUSERPASSWORD=password SVCCONFIRMUSERPASSWORD=password"
```

Command syntax for a complete upgrade:

```
snapdrive4.1.exe /s /v"/qn REINSTALLMODE=vomus REINSTALL=ALL
SILENT_MODE=1 REBOOT=F /Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber MPIO_LICENSECODE=license"
```

Command syntax for MPIO-only upgrade:

```
snapdrive4.1.exe /s /v"/qn REINSTALLMODE=vomus REINSTALL=ALL  
SILENT_MODE=1 REBOOT=F /Li SDInstall.log MPIO_LICENSECODE=license"
```

Command syntax for LUN Provisioning and Snapshot Management-only upgrade:

```
snapdrive4.1.exe /s /v"/qn REINSTALLMODE=vomus REINSTALL=ALL  
SILENT_MODE=1 REBOOT=F /Li SDInstall.log  
LPSM_SERIALNUMBER=serialnumber"
```

Command syntax for a complete uninstall:

```
snapdrive4.1.exe /s /x /v"/qn SILENT_MODE=1 REBOOT=F /Li  
SDInstall.log"
```

Note

If you have previously installed MPIO with a version of SnapDrive earlier than 4.0, the MPIO components will not be uninstalled using this command.

Command syntax for custom help:

```
snapdrive4.1.exe /s /v"/qn CUSTOMHELP=1"
```

For help when upgrading from versions of SnapDrive earlier than 4.0:

```
/s /v"/qn REINSTALLMODE=v CUSTOMHELP=1"
```

Setting a preferred IP address for storage system host-name resolution

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

To set the preferred IP address for a storage system 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.

Step	Action
2	In the Disks Properties window, select the Preferred Filer IP Addresses tab.
3	Enter the storage system name and preferred IP address for that storage system in the spaces provided.
4	Click Apply.
5	Repeat Step 3 and Step 4 for each storage system 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.
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 4.1 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 74) and establish a session from the verification server to the iSCSI target on the storage system where the database to be verified resides. This connection enables the verification server to connect to the Snapshot copy 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 97.

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 91
- ◆ “[Uninstalling SnapDrive and MPIO drivers](#)” on page 92
- ◆ “[Uninstalling the FCP driver](#)” on page 92
- ◆ “[Uninstalling the iSCSI Software Initiator](#)” on page 93

Uninstalling the VLD driver

After you 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. VLD-type virtual disks must be converted to LUN-type virtual disks before installing SnapDrive 4.1. 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, click Action > Uninstall and then click OK in the dialog box to confirm that you want to uninstall the VLD driver.

Uninstalling SnapDrive and MPIIO drivers

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

- ◆ Uninstall SnapDrive
- ◆ Uninstall the MPIIO drivers

Step	Action
1	Navigate to the folder containing the SnapDrive installation package from which you did the installation (or the CD directory). Note _____ When removing MPIIO, always perform this step on the passive node in the MSCS cluster. For more information see “Removing MPIIO on a Microsoft cluster” on page 197.
2	Launch the SnapDrive executable, which guides you through the uninstall procedure.

Note

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

Caution

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

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 and then choosing Properties > Hardware > Device Manager.
3	Open SCSI and RAID Controllers.

Step	Action
4	Select the entry for the Fibre Channel HBA, click Action > 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. - Create a temporary shared FCP LUN. In Cluster Administrator, right-click the top-level cluster name and select Properties. - In the Properties dialog, select the Quorum tab. - Select the temporary shared LUN from the list of available drives, and then click OK. The temporary LUN is now the quorum disk. - From SnapDrive, disconnect the quorum disk, then reconnect using FCP. - In Cluster Administrator, redirect the cluster back to the original quorum disk. - Delete the temporary shared LUN.
3	Stop the SnapDrive service. See “ Stopping and starting the SnapDrive service ” on page 89.

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 74.
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 (storage systems).

Go to any of the following topics for more information:

- ◆ [“Tasks for managing iSCSI sessions”](#) on page 96
- ◆ [“Establishing an iSCSI session to a target”](#) on page 97
- ◆ [“Disconnecting an iSCSI target from a Windows host”](#) on page 100
- ◆ [“Disconnecting a session to an iSCSI target”](#) on page 101
- ◆ [“Examining details of iSCSI sessions”](#) on page 103

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 97.
- ◆ 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 97.

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 100.
- ◆ Examine details about iSCSI sessions
For detailed information, see “[Examining details of iSCSI sessions](#)” on page 103.

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 107.

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 (storage system) you want to establish the iSCSI session with, and then click Next. Note The IP address you enter is the storage system's management port IP address, <i>not</i> the target portal IP address to which SnapDrive will establish an iSCSI session. You will select the IP address for establishing an iSCSI session in Step 6. 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.

Step	Action
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 99. c. Click Next. Result: The Completing the iSCSI Session Wizard panel is displayed.
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 storage system.

During the initial stage of the iSCSI session, the initiator sends a login request to the storage system to begin the session. The login request includes the initiator’s CHAP user name and algorithm. The storage system responds with a CHAP challenge. The initiator provides a CHAP response. The storage system 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 183.

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 103.

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 106
- ◆ [“Creating a virtual disk”](#) on page 107
- ◆ [“Creating a shared virtual disk on a Windows cluster”](#) on page 114
- ◆ [“Creating a virtual disk as a quorum disk on a new Windows cluster”](#) on page 115
- ◆ [“Creating a shared non-quorum virtual disk on a Windows cluster”](#) on page 123

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 storage system command line.
- ◆ You must perform all virtual disk management functions using SnapDrive from the host machine.

Note

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 107
- ◆ “[About volume mount points](#)” on page 107
- ◆ “[Creating a virtual disk](#)” on page 108

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, “[Creating a virtual disk](#)” on page 108, on whichever node owns that cluster’s physical disk resources.

Note

Shared disks on cluster nodes that do not own the disks often display as unknown and unreadable in the MMC Disk Management utility; however, the disks will continue to function normally on all nodes in the cluster.

- ◆ To ensure that Snapshot copies can be made, do not attempt to create a virtual disk on a storage system volume that holds anything other than virtual disks. Conversely, do not put anything other than virtual disks on a storage system volume that contains virtual disks.
- ◆ Virtual disk names must be created using ASCII characters only, even when using non-ASCII operating systems.

About volume mount points

A *volume mount point* is a drive or volume in Windows that is mounted to a folder that uses NTFS. A mounted drive is assigned a drive path instead of a drive letter. Volume mount points enable you to surpass the 26-drive-letter limitation. By using volume mount points, you can graft, or mount, a target partition into a folder on another physical disk. SnapDrive supports the creation of up to 120 mount points. For more information about volume mount points, see Microsoft article 280297 and 205524.

Volume mount point limitations

When creating mount points on clustered Windows 2003 servers, keep these additional limitations in mind:

- ◆ The mounted volume must be of the same type as its root; that is, if the root volume is a shared cluster resource, the mounted volume must also be

shared, and if the root volume is dedicated, the mounted volume must also be dedicated.

- ◆ You cannot create mount points to the Quorum disk.
- ◆ If you have a mount point from one shared disk to another, SnapDrive will verify that they are in the same group and that the mounted disk resource is dependent on the root disk source.
- ◆ Volume mount points are not supported on clustered Windows 2000 servers.
- ◆ You can use either a drive letter or a mount point for a shared disk, but not both.

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 storage system and create CIFS shares for those volumes. For more information on creating volumes, see “Creating a storage system volume” on page 47. For more information about creating CIFS shares, see “Creating a CIFS share” on page 48, 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 storage system. For more information, see “Starting FCP and iSCSI services” on page 43.
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.

Step	Action						
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 storage system 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: ◆ Either select a drive letter from the list of available drive letters or enter a volume mount point for the virtual disk you are creating. When you create a volume mount point, enter the drive path that the mounted drive will use: for example, G:\mount_drive1\. Note You can create cascading volume mount points (one mount point mounted on another mount point); however, in the case of a cascading mount point created on a MSCS shared disk, you may receive an system event warning indicating that disk dependencies may not be correctly set. This is not the case, however, and the mounted disks will function as expected. ◆ 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 copy: ❖ The option is set to No and SnapDrive is used to create an additional virtual disk in the same storage system volume. ❖ A virtual disk is created in the same storage system volume <i>without</i> using SnapDrive. ❖ Data objects other than virtual disks are stored on this storage system 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 storage system 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.

Step	Action	
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 storage system volume containing virtual disks to have the following properties: ◆ create_unicode = on ◆ convert_unicode = on ◆ snapshot schedule = off Note_____ SnapDrive cannot proceed to create a virtual disk unless these settings are configured as shown. Therefore, you must accept these settings. _____ Click Next.	
9	If...	Then...
	The virtual disk will belong to a single-host system	Go to Step 14 .
	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 storage system 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 storage system is established, even if you do not complete the Create Disk Wizard.	

Step	Action
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.
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	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 storage system 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 storage system is established, even if you do not complete the Create Disk Wizard.
15	In the Select Initiators panel, click Next. Result: The Completing the Create Disk Wizard panel is displayed.

Step	Action
16	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 115.
- ◆ 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 123.

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 storage system is running at least Data ONTAP 7.0.2.
- ◆ Each node of the cluster contains the features in the following table:

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 Data ONTAP 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 117.
- ◆ [“Creating a virtual disk as a quorum disk on a new Windows Server 2003 cluster”](#) on page 118

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.

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 115. ◆ SnapDrive 4.1 For information about installing SnapDrive, see “Installing, Uninstalling, or Upgrading SnapDrive” on page 61.
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 107.
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.
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 to set up the Windows nodes for a cluster. If you need details about such steps, you must refer to your Microsoft documentation.

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 115. ◆ SnapDrive 4.1 For information about installing SnapDrive, see “Installing, Uninstalling, or Upgrading SnapDrive” on page 61.
3	If you are using the Microsoft iSCSI software, establish iSCSI connections to the storage system 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 97.

Task	Procedure
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 107. 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.
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.

Task	Procedure	
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.	
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 126.	
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.	

Task	Procedure	
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.	
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.	

Task	Procedure	
15	If...	Then...
	The node you added to the cluster was the last node	Go to Step 16 .
	The node you added to the cluster was not the last node	Go to Step 9 .
16	Restart the SnapDrive service. Note _____ Restart 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. _____	

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 123.

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 detect dedicated disks attached to the opposite node.)
- ◆ You must ensure that each node in the cluster is powered on and is functioning properly.

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 115 for information about the drivers. See “Installing the new SnapDrive components” on page 79.
2	Create as many shared virtual disks as are necessary to hold your data. See “Creating a virtual disk” on page 107 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 126
- ◆ [“Disconnecting virtual disks”](#) on page 135
- ◆ [“Deleting a virtual disk”](#) on page 138
- ◆ [“Expanding virtual disks”](#) on page 141
- ◆ [“Managing LUNs not created in SnapDrive”](#) on page 146
- ◆ [“Monitoring fractional space reservations”](#) on page 149
- ◆ [“Administering SnapDrive remotely”](#) on page 151
- ◆ [“Enabling SnapDrive notification”](#) on page 152

Connecting virtual disks

When connected, a virtual disk enables you to save, delete, modify, and manage the files it contains. You can also make Snapshot copies of the entire disk and restore the disk, along with its contents, to the state captured by a previous Snapshot copy. 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 126.

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 a Virtual Disk Location panel, perform the following actions. ◆ Click Browse. ◆ Navigate to the storage system volume on which the virtual disk resides. ◆ Select the virtual disk 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. ◆ Either select a drive from the list of available drive letters or enter a mount point for the virtual disk you are connecting. When you create a volume mount point, enter the drive path that the mounted drive will use: for example, G:\mount_drive1\. Note _____ You can create cascading volume mount points (by mounting one mount point on another mount point); however, in the case of a cascading mount point created on a MSCS shared disk, you may receive an system event warning indicating that disk dependencies may not be correctly set. This is not the case, however, and the mounted disks will function as expected. _____ ◆ Click Next.	

Step	Action	
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.
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.	

Step	Action
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>Block Access Management Guide</i> for information about how to determine the port for your HBA.

Step	Action
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. Note _____ If a virtual disk has volume mount points when you connect it, SnapDrive removes the mount points before completing the connection. Result: The Computer Management window is displayed, with the newly connected virtual disk now appearing under SnapDrive > Disks in the left panel.

Note _____

If a virtual disk displays in the SnapDrive MMC with no drive letter and all operations are grayed out, the disk has no volume. Creating a partition on the virtual disk and formatting it will create a volume.

Making drive letter or path modifications to a virtual disk

There might be instances when you need to change the drive letter or mount point path for a virtual disk. SnapDrive enables you to add, change, or remove a drive letter or path for an existing virtual disk.

Adding or changing a drive letter or path for an existing virtual disk

To add or change a drive letter or mount point path to which a virtual disk has been assigned, complete the following steps.

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	In the right pane, right-click on the disk that you want to modify and choose Change Drive Letter and Paths from the menu. Result: The Change Drive Letter and Paths window is displayed.
3	Click either Add or Change, depending on the action you want to take. Note _____ The Change option is unavailable for mount points.

Step	Action
4	In the Add or Change Drive Letter or Path window, select a drive letter or enter path in the space provided, then click OK. By removing the last volume mount point on a shared disk, SnapDrive removes the resource dependency from the root disk. If you are creating a mount point from one shared disk to another, SnapDrive will verify they are in the same group and SnapDrive will create a dependency to the root disk resource if it is the first volume mount point to that root disk. Note_____ When you create the first volume mount point to a root disk that is shared and is being used by MSCS, SnapDrive takes offline the physical disk resource, presenting the mounting volume, as part of the resource dependency process. As a result, any other cluster resources that depend on the physical disk resource will also be taken off line. An example of this is the Exchange System Attendant cluster resource. SnapDrive automatically brings the physical disk resource back online but will not bring the Exchange resources back online. Exchange resources should be brought back online manually by the administrator using the Cluster Administrator. Note_____ You cannot add a second mount point or a drive letter to a shared LUN that is already using a mount point.

Removing a drive letter or mount point for an existing virtual disk

To remove a drive letter or mount point path to which a virtual disk has been assigned, complete the following steps.

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.

Step	Action
2	In the right pane, right-click on the disk that you want to modify and choose Change Drive Letter and Paths from the menu. Result: The Change Drive Letter and Paths window is displayed.
3	Click Remove, then click OK to proceed with the operation. Note_____ When you remove the last volume mount point to a root disk that is shared and is being used by MSCS, SnapDrive takes offline the physical disk resource, presenting the mounted volume, as part of the resource dependency removal process. As a result, any other cluster resources that depend on the physical disk resource will also be taken offline. An example of this is the Exchange System Attendant cluster resource. SnapDrive automatically brings the physical disk resource back online but will not bring the Exchange resource back online. Exchange resources should be brought back online manually by the administrator using the Cluster Administrator. _____ Note_____ This command will not delete the folder that was created at the time the volume mount point was added. After you remove a mount point, an empty folder will remain with the same name as the mount point you removed. _____

Disconnecting virtual disks

When the host is disconnected from a virtual disk, you cannot see or modify the virtual disk's contents, make Snapshot copies of the virtual disk, or use Snapshot technology to restore the virtual disk to a previous Snapshot copy. However, the virtual disk still exists on the storage system 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.

Note

SnapDrive does not allow you to disconnect disks containing volume mount points. To disconnect a disk with volume mount points, first disconnect the mount point and then disconnect the disk to which it was mounted. For more information, see “[Disconnecting a virtual disk](#)” on page 135

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 135.
- ◆ By forcing a disconnect, as described in “[Forcing a disconnect](#)” on page 136.
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.
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. Note_____ If you are disconnecting a disk that contains volume mount points, disconnect the mounted disk first before disconnecting the disk containing the mount points; otherwise, you will not be able to disconnect the root disk. For example, disconnect G:\mount_disk1\, then disconnect G:\.
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. Note_____ This procedure will not delete the folder that was created at the time the volume mount point was added. After you remove a mount point, an empty folder will remain with the same name as the mount point you removed.

Related topic:

- ◆ [“Forcing a disconnect”](#) on page 136

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.
- ◆ Any mount points associated with the virtual disk will also be unmounted. The directory created for the volume mount point will not be deleted.
- ◆ 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.
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 126.

Related topic:

- ◆ “[Disconnecting a virtual disk](#)” on page 135

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.
 - ◆ You can only delete a shared virtual disk (that is, a non-quorum disk) after removing the cluster resource dependencies from the virtual disk and verifying that all nodes in the cluster are powered on and functioning properly.
 - ◆ When deleting virtual disks on a Microsoft cluster, you must make sure that all hosts in the cluster are available to SnapDrive for the delete operation to succeed.
 - ◆ 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
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	In the right pane, select the disk that you want to delete. Note _____ If you are deleting a disk that contains volume mount points, delete the mounted disk first before deleting the disk containing the mount points: for example, delete G:\mount_disk1\, then delete G:\. If your volume mount point contains data, keep in mind that SnapDrive will not warn you that data is present when you delete the mount point. For more information about deleting a folder within a volume mount point, see “Deleting folders within volume mount points using the Windows Explorer” on page 140. _____

Step	Action
3	Click Action (from the menu choices on top of the MMC), and then select Delete Disk.
4	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. Note _____ This procedure will not delete the folder that was created at the time the volume mount point was added. After you remove a mount point, an empty folder will remain with the same name as the mount point you removed. _____

Deleting folders within volume mount points using the Windows Explorer

When you use the Windows Explorer to delete a folder that you have created under a volume mount point, you may receive an error message similar to the following:

Cannot delete *Foldername*: Access Denied. The source file may be in use.

Foldername is the name of the folder you want to delete.

This happens because the Windows Recycle Bin does not understand volume mount points and tries to delete the drive on which the mount point resides rather than the folder on the mount point.

Deleting folders within volume mount points

To delete a folder within a mount point, complete the following steps.

Step	Action
1	Using Windows Explorer, click on the folder you want to delete.
2	Click Shift and Delete simultaneously to bypass the Recycle Bin.

For more information about deleting folders within volume mount points, see [Microsoft article 243514](#).

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 storage system 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, except by restoring a Snapshot copy made 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 copy of a virtual disk whose size has since been reduced enlarges the virtual disk to its former size.)

Note

If it is necessary to restore a virtual disk from a Snapshot copy made before the virtual disk was expanded, you must disconnect the disk using SnapDrive and then restore the disk from the storage system 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 143.

- ◆ 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 142
- ◆ [“Expanding a quorum disk”](#) on page 143

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 copy: ❖ The option to limit the maximum disk size to accommodate at least one Snapshot copy is <i>not</i> selected when SnapDrive is used to create an additional virtual disk in the same storage system volume. ❖ A virtual disk is created in the same storage system volume <i>without</i> using SnapDrive. ❖ Data objects other than virtual disks are stored on this storage system 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 copy of the expanded virtual disk. For more information, see “Restoring virtual disks from Snapshot copies” on page 168.

Related topic:

- ◆ [“Expanding a quorum disk”](#) on page 143

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 107. 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 138.
	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 107. 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 142. 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 138.

Related topic:

- ◆ [“Expanding a virtual disk”](#) on page 142

Managing LUNs not created in SnapDrive

You can use SnapDrive to manage LUNs on your storage system even if SnapDrive was not used to create the LUNs; however, you might need take several steps to prepare the LUNs for SnapDrive management.

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
- ◆ LUNs must have the .lun extension

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 Snapshot copies are consistent. _____

Step	Action
3	Using FilerView or the storage system console, complete the following steps: - Take a Snapshot copy of the volume on which the LUNs reside. - Unmap the LUN from the initiator group. - If the LUN name uses uppercase or non-ASCII characters, rename the LUN from the storage system console, using the <code>lun move</code> command. - Turn on space reservation.
4	Restart the Windows host.
5	Using SnapDrive, connect to the renamed LUN, as described in “Connecting virtual disks” on page 126.
6	Using SnapDrive, take a Snapshot copy of the newly connected LUN as described in “Creating Snapshot copies” on page 158.

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 storage system to temporarily designate as the quorum disk, as described in “Creating a shared virtual disk on a Windows cluster” on page 114.
2	For each resource in this cluster group, record all dependencies. - Using Cluster Administrator, right-click the resource and select Properties. - Select the Dependencies tab. - Record all dependencies for the resource.

Step	Action
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 Snapshot copies are consistent.
6	Using FilerView or the storage system console, complete the following steps: a. Make a Snapshot copy 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 storage system 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 126.
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 138.
11	Using SnapDrive, make a Snapshot copy of the newly connected LUN as described in “ Creating Snapshot copies ” on page 158.

Monitoring fractional space reservations

SnapDrive 4.1 enables you to monitor fractional space reserved for LUNs on a storage system volume when your storage system is running Data ONTAP 7.1 or later. To monitor the fractional space reserved on your storage system from your Windows host, SnapDrive enables you to perform the following tasks:

- ◆ Set fractional space reservation thresholds for volumes containing LUNs
- ◆ Set rate-of-change percentage between two Snapshot copies or between a Snapshot copy and the active file system of the storage system volume
- ◆ Monitor space that can be reclaimed by deleting a Snapshot copy
- ◆ Set monitor polling interval
- ◆ Enable and disable e-mail notification

For more information about fractional space reservations, see the *Block Access Management Guide*.

Enabling space reservation monitor e-mail notification

To enable the space reservation e-mail notification feature in SnapDrive, see “[Enabling SnapDrive notification](#)” on page 152.

Configuring space reservation monitoring

To configure fractional space reservation monitoring 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. Right-click Disks and select Properties from the menu.
2	In the Disks Properties window, select the Space Reservations Monitor tab.

Step	Action
3	In the Space Reservations Monitor panel, perform the following actions: ◆ Enter a value in the Monitor Time Interval field, in minutes. Values can be between 0 and 10,080 minutes (7 days). ◆ Under the Space Reservations Monitor Settings tree, select the storage system and volume name. Your selections are displayed in the Filer and Volume fields to the right of the tree. ◆ Enter the Reserve Available percentage threshold. ◆ Enter the Rate of Change threshold (in kilobytes, megabytes, gigabytes, or terabytes). ◆ Select “Alert when there is no space left to create snapshot” if you want to be notified if this condition occurs.
4	Click Apply or, if you are making changes to an existing entry, click Add/Update.
5	Click OK.

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 storage system, 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

Avoid using 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 e-mail notification and enable storage system AutoSupport in the event of a SnapDrive message or storage system error. When you set up notification, you can specify the following information:

- ◆ Whether and where to send e-mail notification
- ◆ What types of messages to report
- ◆ Whether to allow a subset of events to be posted to AutoSupport on the storage system

Note

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

Enabling SnapDrive notification: To enable e-mail 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 E-mail 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 storage system. f. Click OK.

Step	Action
3	You can verify the e-mail output of the Event Notification feature by clicking Send a Test E-mail on the Notification Settings panel.

The topics that follow describe how to use the SnapDrive Snapshot copy feature to create Snapshot copies 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 Snapshot copies 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 Snapshot copies work”](#) on page 156
- ◆ [“Creating Snapshot copies”](#) on page 158
- ◆ [“Connecting to LUNs in a Snapshot copy”](#) on page 164
- ◆ [“Restoring virtual disks from Snapshot copies”](#) on page 168
- ◆ [“Deleting Snapshot copies”](#) on page 172
- ◆ [“Overview of archiving and restoring Snapshot copies”](#) on page 174

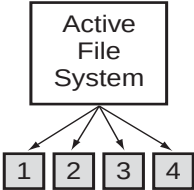
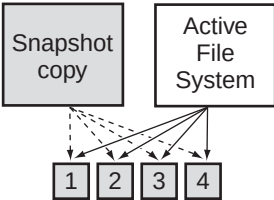
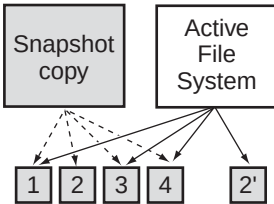
How Snapshot copies work

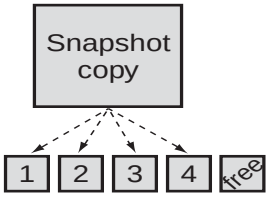
What a Snapshot copy is: A Snapshot copy is a point-in-time, read-only image of the storage system volume. Snapshot copies can restore your databases rapidly if you encounter data corruption or other problems.

Because Snapshot copies reside on disk instead of tape, this technology complements conventional backup processes. Snapshot copies 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 of how Snapshot copies work](#)” on page 156 provides an illustration.

Example of how Snapshot copies work:

Before Snapshot copy  <pre>graph TD AFS[Active File System] --> B1[1] AFS --> B2[2] AFS --> B3[3] AFS --> B4[4]</pre>	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 copy  <pre>graph TD SC[Snapshot copy] -.-> B1[1] SC -.-> B2[2] SC -.-> B3[3] SC -.-> B4[4] AFS[Active File System] --> B1 AFS --> B2 AFS --> B3 AFS --> B4</pre>	When you take a Snapshot copy of the active file, the Snapshot copy 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 copy block pointers, the Snapshot copy consumes no disk space beyond that already used by the active file system.
After block update  <pre>graph TD SC[Snapshot copy] -.-> B1[1] SC -.-> B2[2] SC -.-> B3[3] SC -.-> B4[4] AFS[Active File System] --> B1 AFS --> B2 AFS --> B3 AFS --> B4 AFS --> B2p[2']</pre>	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 copy. 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 copy block pointers continue to reference the original four blocks.

After file delete  The diagram shows a box labeled 'Snapshot copy' at the top. Below it are five boxes labeled 1, 2, 3, 4, and free. Dashed arrows point from the 'Snapshot copy' box to each of the boxes 1, 2, 3, and 4.	When you delete the file, the blocks holding its data are no longer used by the active file system, but the Snapshot copy still needs the blocks to which it points. Any blocks not used by any file or any Snapshot copy are freed for reuse.
After Snapshot copy delete  The diagram shows five 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 Snapshot copies that reference them have been deleted.

Creating Snapshot copies

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

Note

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

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

Restrictions on Snapshot copy creation: Note the following facts about SnapDrive and Snapshot copies:

- ◆ You can keep a maximum of 255 Snapshot copies with Data ONTAP 7.0.2 and later.
After the number of Snapshot copies has reached the limit, the Snapshot Create operation fails, and you must delete some of the old Snapshot copies before you can create any more.
- ◆ SnapDrive does not support Snapshot copies that are created from the storage system console, because such a practice can lead to inconsistencies within the NTFS file system. Therefore, use only SnapDrive to create Snapshot copies of virtual disks.
- ◆ You cannot create a Snapshot copy of a LUN connected to a Snapshot copy. For more information, see “[Snapshot cautions](#)” on page 164.

- ◆ SnapDrive automatically turns off the Snapshot copy schedule on a storage system volume that stores virtual disks, so that the storage system does not create automatic Snapshot copies.

Note

Any Snapshot copies inadvertently made at the storage system console or through FilerView are dimmed (unavailable) in the SnapDrive plug-in and are not usable by SnapDrive.

Snapshot copy requirements: The following requirements must be met:

- ◆ You must create Snapshot copies through the SnapDrive MMC snap-in or through sdcli.exe, rather than the storage system console or the volume Snapshot copy schedule on the storage system. This is because SnapDrive must first flush NTFS so that the virtual disk is consistent at the moment the Snapshot copy is made. This ensures the usability of the virtual disk file in the Snapshot copy directory.
- ◆ You must create separate SnapDrive Snapshot copy 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 copy:

- ◆ [“Creating a Snapshot copy”](#) on page 160
- ◆ [“Scheduling Snapshot copies”](#) on page 161

Creating a Snapshot copy

To create a Snapshot copy 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 copy. 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 copy. For example, expenses_db_15Jan03_4pm. Note _____ Snapshot copy names must be created using ASCII characters only, even when using non-ASCII operating systems. b. Click OK. Result: Your Snapshot copy is created under the following directory on the storage system: <i>\\Storage System Name\Share Name\~snapshot\snapshot name</i> <i>Storage System Name</i> is the (NetBIOS) name of the storage system on which the virtual disk exists. <i>Share Name</i> is the name of CIFS share on the storage system. <i>snapshot name</i> is the name of the Snapshot copy. Information about the Snapshot copy also appears in the right panel of the MMC, in a list with all the other previous Snapshot copies for that virtual disk.

Scheduling Snapshot copies

Make sure that you have read the Snapshot copy requirements described in “[Snapshot copy requirements](#)” on page 159 before you follow this procedure.

To schedule SnapDrive Snapshot copies, 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 Snapshot copies: <pre>sdcli snap create [-m <i>MachineName</i>] -s <i>SnapshotName</i> -D <i>DriveLetterList</i> [. . .] [-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 copy to be created. <i>DriveLetterList</i> is a list of space-separated drive letters. When -x flag is specified, Snapshot copies are created only for the drives specified by the -D flag. Otherwise, Snapshot copies are created for all the disks on the storage system 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 copy 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 Snapshot copies 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 copy 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 copy 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 copy

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

Such a read/write connection to a virtual disk in a Snapshot copy 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 copy.
- ◆ 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 copy.
- ◆ 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 copy does not in itself consume any additional disk space on the storage system volume. You consume additional space only as you write to the .rws file.

Note

Connecting to a LUN in a Snapshot copy 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 Snapshot copies and virtual disks that are backed up by a Snapshot copy:

- ◆ 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 copy referenced by the .rws file.
- ◆ You cannot delete a Snapshot copy that is in use by a virtual disk backed by a Snapshot copy.
- ◆ You can connect to the virtual disk Snapshot copy only by using read/write mode and a virtual disk that is backed by a Snapshot copy.
- ◆ You should avoid creating a Snapshot copy of a virtual disk backed by a Snapshot copy. Doing so will lock the Snapshot copy backing the virtual

disk until the newer Snapshot copy—and all Snapshot copies of that virtual disk—are deleted. For more information about deleting a locked Snapshot copy, see “[Problems deleting Snapshot copies due to busy snapshot error](#)” on page 173.

For instructions on connecting to a LUN in a Snapshot copy, see “[Connecting to a virtual disk \(LUN\) in a Snapshot copy](#)” on page 165.

Connecting to a virtual disk (LUN) in a Snapshot copy

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

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: - Click Browse to browse to the \~snapshot directory of the storage system volume holding the Snapshot copy of the virtual disk. - Select a virtual disk file (with a .lun extension). - Click Next. Result: The Select a Virtual Disk Type panel is displayed. Note _____ If you cannot see the Snapshot copy directory, make sure that <code>cifs.show_snapshot</code> is set to On and <code>vol option nosnapdir</code> is set to Off on your storage system.
4	In the Select a Virtual Disk Type panel, Dedicated is automatically selected because a Snapshot copy 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 to a temporary read-write virtual disk created when you connect to the disk backed up by the Snapshot copy is automatically specified. 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. - Either select a drive from the list of available drive letters or enter a mount point for the virtual disk you are connecting. - 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 Snapshot copies

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

A virtual disk restore recalls a selected Snapshot copy. During a restore, the entire virtual disk drive is restored from the Snapshot copy. 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 copy taken prior to that expansion, the restored virtual disk reverts to its size at the moment the Snapshot copy was made.

Note

If you need to restore an expanded disk from a Snapshot copy, you should use a Snapshot copy that was created after the virtual disk was expanded. SnapDrive does not allow you to restore a virtual disk from a Snapshot copy that was made before the disk was expanded. If you need to do this, you must disconnect the disk using SnapDrive, then restore the disk from the storage system 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 copy, go to [“Restoring a virtual disk from a Snapshot copy”](#) on page 169.

About the Data ONTAP LUN clone feature

If you are using Data ONTAP 7.1 or later, SnapDrive uses the LUN clone and split feature of Data ONTAP when restoring a LUN.

A LUN clone is a point-in-time, writable copy of a LUN in a Snapshot copy. Changes made to the parent LUN after the clone is created are not reflected in the clone.

A LUN clone shares space with the LUN in the backing Snapshot copy. The clone does not require additional disk space until changes are made to it. When Data ONTAP splits the clone from the backing Snapshot copy, you copy the data from the Snapshot copy to the clone. After the splitting operation, both the backing Snapshot copy and the clone occupy their own space.

Note

If you do not have enough disk space for both the clone and the backing Snapshot copy when the split is initiated, the split will not occur and the LUN restore will fail.

Benefit of using LUN clones

When LUN cloning is used by SnapDrive, the clone is split from the backing Snapshot copy in the background, and the restored LUN is available to the Windows host for I/O operations within a few seconds.

To take advantage of the LUN clone feature when performing a LUN restore with SnapDrive, the option must be enabled on your storage system. To determine whether this option is enabled, use the options `lun.clone_restore` command at the storage system command line. The option must be set to On. If the option is not set to On, or if you are using a version of Data ONTAP earlier than 7.1, SnapDrive will perform a Single File Snap Restore operation.

For more information about LUN clones, see the *Block Access Management Guide*.

Restoring a virtual disk from a Snapshot copy

To restore a virtual disk from a Snapshot copy, 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.

Step	Action
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 copy you want to restore. b. Select Restore Disk From Snapshot from the drop-down menu. Note _____ You can only restore a Snapshot copy that is consistent with the active file system. Inconsistent Snapshot copies are not available for restoration.
4	In the Restore Snapshot panel, click Yes to restore the Snapshot copy you selected. Caution _____ Do not attempt to manage any Windows cluster resources while the restore is in progress.

Checking LUN restore status

To check the status of a LUN restore, complete the following steps.

Step	Action
1	In the right pane of the MMC, under Storage > SnapDrive, click Disks.

Step	Action
2	In the left pane of the MMC, locate the name of the disk you are restoring. The status is displayed under the column titled Restore Status. If a restore is in progress, SnapDrive will display the percentage completed, otherwise; the status will display Normal. Note————— You can also check the status of a LUN restore using the <code>disk list</code> command of the <code>sdcli.exe</code> utility. For more information see Appendix A, “Virtual disk commands,” on page 233.

Deleting Snapshot copies

Reasons to delete Snapshot copies: Delete older Snapshot copies for the following reasons:

- ◆ To keep the number of stored Snapshot copies less than the hard limit of 255 for Data ONTAP
Be sure to delete old Snapshot copies before the hard limit is reached; otherwise, subsequent Snapshot copies could fail.
- ◆ To free space on the storage system volume
Even before the Snapshot copy limit is reached, a Snapshot copy fails if insufficient reserved space for it remains on the disk.

For instructions for deleting a Snapshot copy, see “[Deleting a Snapshot copy](#)” on page 172.

Deleting a Snapshot copy

To delete a Snapshot copy, complete the following steps.

Note—
You must make sure that the virtual disk whose Snapshot copy 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 copy you want to delete.

Step	Action
2	In the right pane of the MMC, select the Snapshot copy you want to delete. Note— You can only delete a Snapshot copy that is consistent with the active file system. Inconsistent Snapshot copies are not available for deletion.
3	Click Action (from the menu choices on top of the MMC).
4	Select Delete from the drop-down menu.
5	In the Delete Snapshot panel, click Yes to delete the Snapshot copy you selected. Note— If you get an error message stating that the Snapshot copy is busy or cannot be deleted, it is likely that the Snapshot copy is in use by a virtual disk that is backed by a Snapshot copy. For more information, see “Problems deleting Snapshot copies due to busy snapshot error” on page 173

Problems deleting Snapshot copies due to busy snapshot error

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

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

Overview of archiving and restoring Snapshot copies

A good way to protect and retain data is to archive the SnapDrive Snapshot copies of the virtual disks (LUNs) to offline, offsite media, such as Data ONTAP 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 *Snapshot copies* 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 Snapshot copies of your virtual disks (LUNs).

Note

You cannot use CIFS-based or NFS-based backup products to archive the Snapshot copies 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.

The topics that follow describe the Volume Shadow Copy Service:

- ◆ “[What Volume Shadow Copy Service is](#)” on page 176
- ◆ “[Troubleshooting the VSS Hardware Provider](#)” on page 179

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 Snapshot copies.

VSS requirements

In order to use VSS with SnapDrive 4.1, VSS requires the following:

- ◆ Your storage system must be running at least Data ONTAP 7.0.2.
- ◆ The Virtual Disk Service must be running on your Windows 2003 host.

Overview of VSS

VSS coordinates Snapshot copy-based backup and restore and includes these additional components:

- ◆ 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 copy attributes for backups it initiates.

- ◆ VSS writer

The VSS writer owns and manages the data to be captured in the Snapshot copy. 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 copy. A provider can be either a hardware provider or a software provider:

- ❖ A hardware provider integrates storage array-specific Snapshot copy and cloning functionality into the VSS framework. The NetApp VSS Hardware Provider integrates the SnapDrive service and NetApp storage systems running Data ONTAP into the VSS framework.

Note

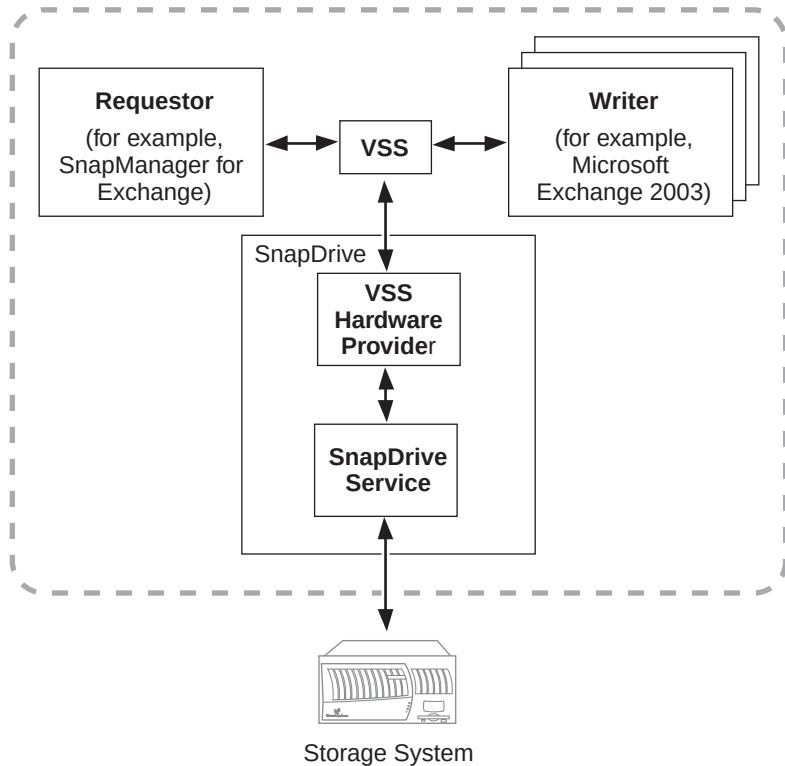
The NetApp VSS Hardware Provider is installed automatically as part of the SnapDrive 4.1 software installation.

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

Note

To ensure the NetApp VSS Hardware Provider works properly, do not use the VSS software provider on Data ONTAP LUNs. If you use the VSS software provider to create Snapshot copies on a Data ONTAP 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 the NetApp VSS Hardware Provider is outlined in the following process:

1. SnapManager determines which 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 the 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 the NetApp VSS Hardware Provider to create a shadow copy.
6. The NetApp VSS Hardware Provider requests SnapDrive to create a Snapshot copy of the storage system volume that contains the specified LUN.
7. SnapDrive requests the storage system to create a Snapshot copy 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 a Snapshot copy. In a case, however, in which 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 copy.

Troubleshooting the 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 storage appliance running Data ONTAP, the NetApp VSS Hardware Provider must be used for the Snapshot copy 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 make a Snapshot copy on the storage system, the NetApp VSS Hardware Provider must be used. If a Snapshot copy on the storage system is not created successfully, verify that the NetApp VSS Hardware Provider was used to create the Snapshot copy.

Only the NetApp VSS Hardware Provider can take a Snapshot copy on a 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>

Step	Action
2	At the prompt, enter the following command: <pre>vssadmin list providers</pre> 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 copy is not made on the storage system

If you attempt to create a backup on a NetApp storage system and a Snapshot copy is not created on the storage system, complete the following steps.

Step	Action
1	Verify that the NetApp VSS Hardware Provider was used to create the Snapshot copy and that it was completed successfully. For details, see “Verifying that the VSS Hardware Provider was used successfully” on page 181.
2	If NetApp VSS Hardware Provider was not used or failed to create the Snapshot copy successfully, verify your VSS configuration. For details, see “Verifying your VSS configuration” on page 181. Note_____ The VSS auto-recovery feature is not supported in this release and VSS Snapshot copy 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 copy 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 the VSS Hardware Provider was used successfully

To verify that the NetApp VSS Hardware Provider was used successfully after a Snapshot copy 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	The VSS provider has successfully completed CommitSnapshots for SnapshotSetId <id> in <n> milliseconds.

Note

VSS requires that the provider initiate a Snapshot copy 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 VSS configuration

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

Step	Action
1	Verify that SnapDrive is installed and running, and can communicate with the storage system. To do this, complete the following steps: - Open the MMC and select the Disks icon under Snapdrive. - Select Action > Refresh. No error messages should be displayed.
2	Verify that the drives for which the 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 the 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 click the Log On tab. e. Verify that the This Account field is selected, and that it contains the same account as the SnapDrive service.

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:

- ◆ [“Feature availability”](#) on page 184
- ◆ [“Multipathing overview”](#) on page 185
- ◆ [“MPIO setup”](#) on page 188
- ◆ [“MPIO path management”](#) on page 193

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 storage system `lun` command. For more information, see the *Block Access Management Guide*.

Note

When mapping and unmapping LUNs using FilerView or the storage system `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.

Related topics:

- ◆ “[Multipathing commands](#)” on page 239 lists MPIO-related commands (and associated parameters) that run under `sdcli.exe`, the SnapDrive command-line utility.
- ◆ “[MPIO configurations](#)” on page 35 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 storage system 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 an MPIO 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 186.

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 26. For a list of the latest service packs and hotfixes required by SnapDrive, see the SnapDrive 4.1 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 26. For a list of the latest service packs and hotfixes required by SnapDrive, see the SnapDrive 4.1 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 Data ONTAP 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 storage system	Data ONTAP 7.0.2 (minimum)
Storage system clustering (optional)	NetApp storage system clusters

Related topic:

- ◆ “[Supported MPIO topologies](#)” on page 188.

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 186.

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 107. For Windows clusters, you specify an initiator for each Windows node in the cluster, as described in “[Creating a virtual disk](#)” on page 107.

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, it is recommended 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 186
- ◆ “[Supported MPIO topologies](#)” on page 188

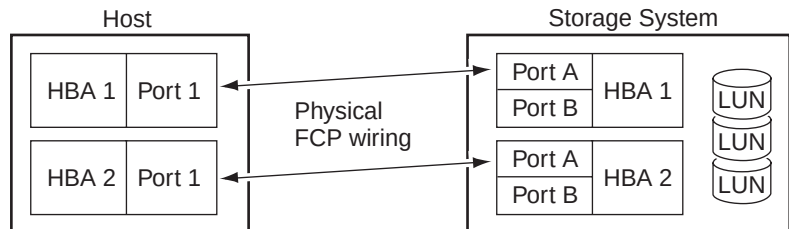
Supported MPIO topologies

MPIO configurations consist of three basic sets of physical components:

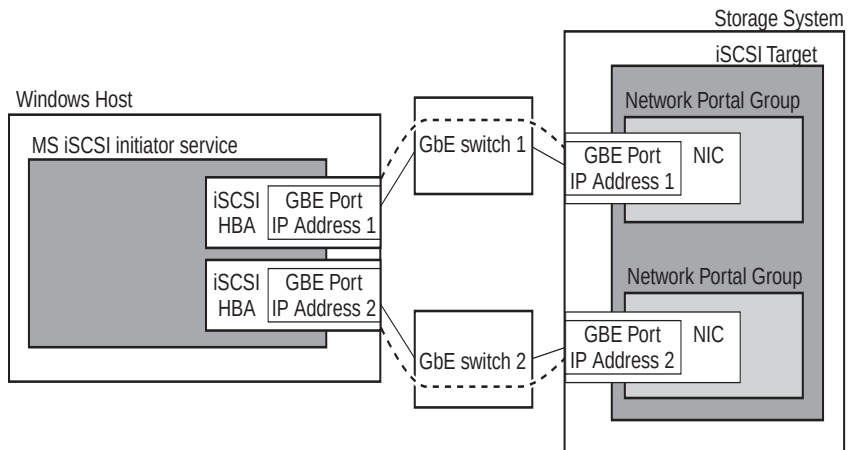
- ◆ Host (a single node or a Windows cluster pair)
- ◆ Switch (two per configuration provides maximum protection for storage system clusters. Switches are not used in direct attached configurations.)
- ◆ Storage system (a single appliance or a storage system cluster pair)

Single host direct-attached to a single storage system using FCP:

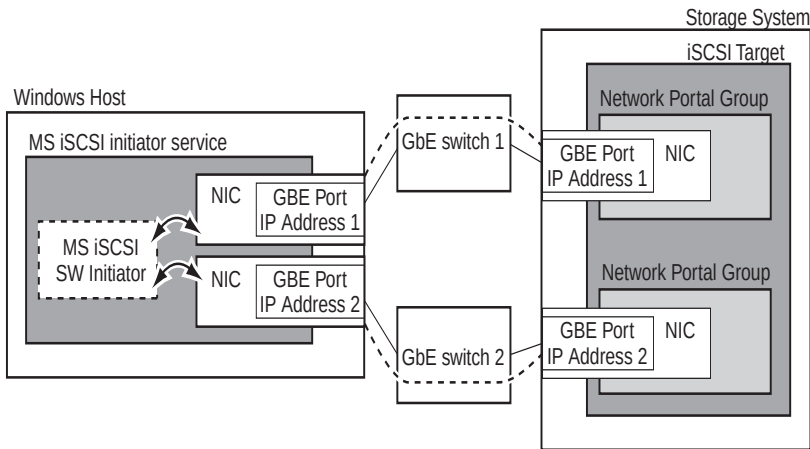
The following diagram shows a pair of FCP crossover cables used to support MPIO between a single host and a single storage system. If the active path fails, MPIO routes data across the passive (standby) path. The host has two HBAs and the storage system has two HBAs.



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



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

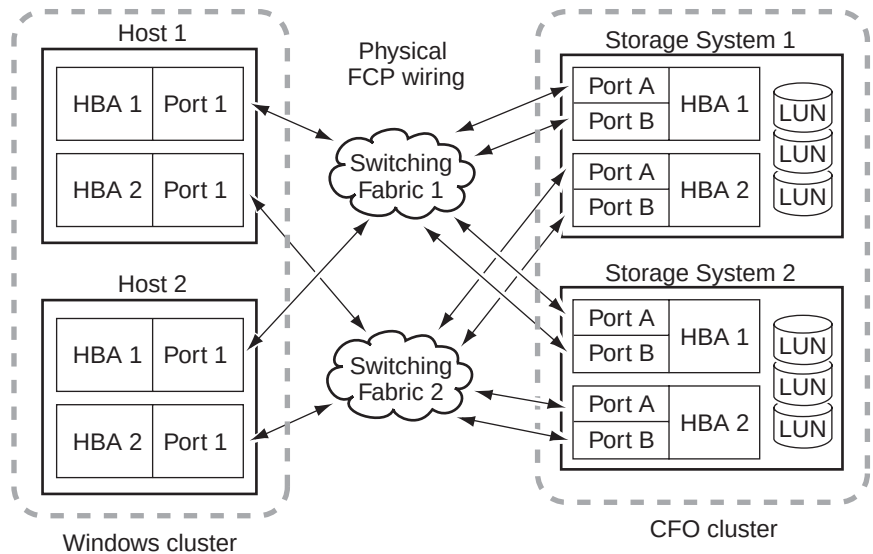


Windows cluster connected to a storage system cluster using FCP through switches: One setup offering maximum protection against a single point of failure consists of a Windows cluster, a pair of FCP switches, and a storage system cluster.

In the following illustration, the HBAs in the hosts have one port each. The storage systems 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 storage system connect to *different* switches.

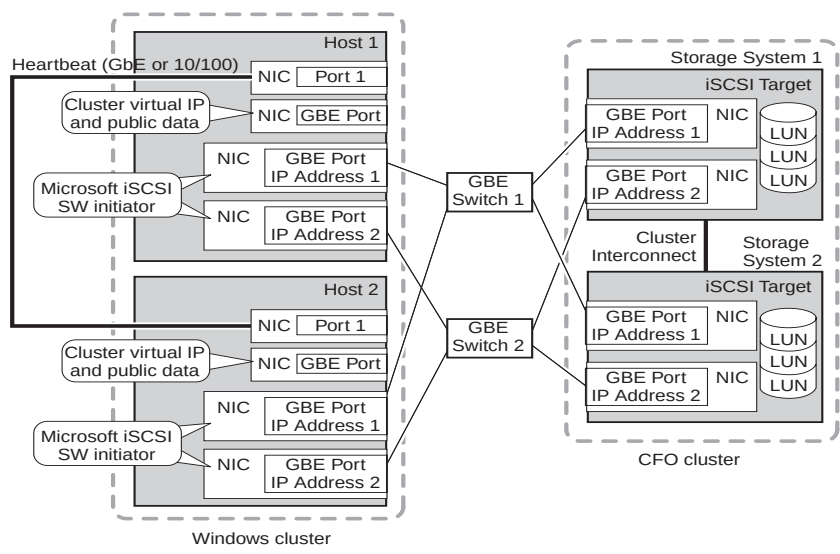


Windows cluster connected to a storage system cluster using iSCSI through switches: Another configuration offering maximum protection against a single point of failure consists of a Windows cluster, a pair of GbE switches, and a storage system cluster.

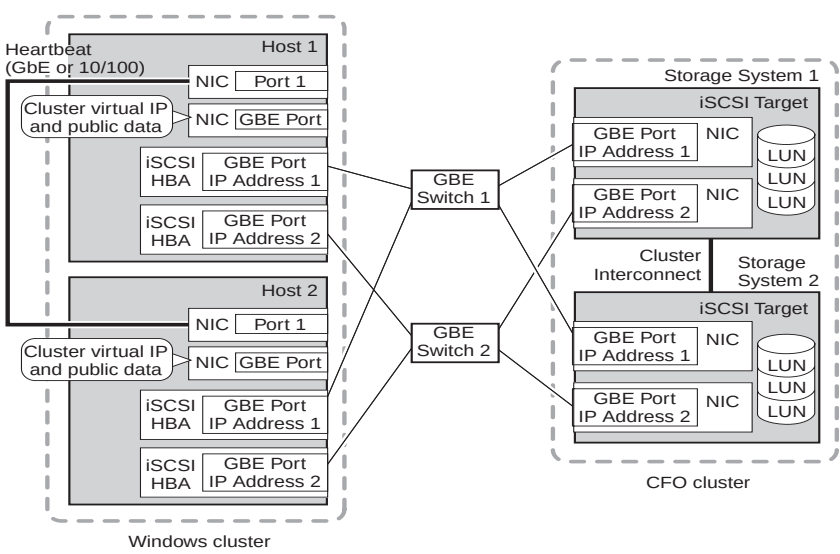
In this type of configuration, it is best to use a total of four NICs, each on different subnets, as follows:

- ◆ 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 storage system cluster.



The following diagram shows iSCSI HBAs being used in an MPIO configuration between a Microsoft cluster, a pair of GbE switches, and a storage system 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 information, see “Establishing an iSCSI session to a target” on page 97 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 storage system <code>igroup add</code> or <code>igroup remove</code> commands. For more information, see the <i>Block Access Administration Guide</i>. _____	
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 239.	

Interface	Method	How to access
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, storage system, and domain access permissions. For example, a properly configured SnapDrive service account has all necessary accesses enabled.

Related topic:

- ◆ [“Creating an MPIIO path”](#) on page 194

Creating an MPIIO path

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

Note

If you are creating an MPIIO 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 97.

Note

You can use this same basic procedure to unmap MPIIO paths as well. See also [“Multipathing commands”](#) on page 239 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.

Step	Action
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 MPIO module installed, use FilerView or the storage system <code>igroup add</code> or <code>igroup remove</code> commands. For more information, see the <i>Block Access Administration Guide</i>.
3	If you are mapping MPIO paths for a Windows cluster configuration using FCP, skip to Step 4. If you are mapping MPIO 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 MPIO 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 MPIO path states

You can add, enable, activate, disable, or remove (delete) MPIO 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 storage system, it is recommended 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 storage system; 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 196.

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 does not 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	Assuming that node 1 is the passive node, uninstall SnapDrive and reboot.
3	From the Cluster Administrator, perform a Move Group to move all resources from node 2 to node 1. Result: Node 1 is now the passive node.
4	Uninstall SnapDrive on node 2 and reboot.

The topics that follow discuss SAN booting and how SAN booting works with SnapDrive:

- ◆ [“What SAN booting is”](#) on page 199
- ◆ [“How SnapDrive supports SAN booting”](#) on page 199
- ◆ [“Configuring bootable virtual disks”](#) on page 200

What SAN booting is

The term *SAN booting* means using a SAN-attached disk, such as a storage system 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 storage system.

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 4.1 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. See [“Icons used in SnapDrive”](#) on page 21.

SnapDrive identifies bootable virtual disks and prevents you from performing some of the 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

SnapDrive supports the following Snapshot copy-related actions on bootable virtual disks:

- ◆ Create
- ◆ Rename
- ◆ Delete

Note

Restoring Snapshot copies of bootable virtual disks is not allowed by SnapDrive. For important information about Snapshot copies 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 storage system. 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 202
- ◆ [“SnapMirror replication”](#) on page 205
- ◆ [“Initiating replication”](#) on page 207
- ◆ [“Connecting to a virtual disk on a destination volume”](#) on page 209
- ◆ [“Recovering a cluster from shared virtual disks on a SnapMirror destination”](#) on page 212

SnapMirror overview

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

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

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 storage system volume or storage system 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 202
- ◆ [“Requirements for using SnapMirror with SnapDrive”](#) on page 202

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 storage systems. 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 storage systems.
- ◆ 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 storage system, you can avoid schedule conflicts with SnapDrive by setting the replication schedule on the storage system 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 storage system 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 storage systems.
- ◆ The Windows domain account used to administer SnapDrive must have full access to the Windows domain to which both the source and destination storage systems belong.
- ◆ The source and destination storage systems must be configured to grant root access to the Windows domain account used by the SnapDrive service. That is, the `waf.l.map_nt_admin_priv_to_root` option must be set to On. For information about enabling storage system 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 storage system must have at least one LUN access protocol licensed (iSCSI or FCP).

- ◆ A TCP/IP connection must exist between the source storage system and the destination storage system.
- ◆ 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 copy creation: Each time a Snapshot copy of a virtual disk is created—manually or because of a Snapshot copy schedule—SnapDrive determines whether the virtual disk whose Snapshot copy was made resides on a SnapMirror source volume. If so, then after the Snapshot copy has been made, 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 copy of a LUN on a SnapMirror source through SnapDrive, a window with a check box labeled “Initiate SnapMirror Update” is displayed. The check box is selected by default.

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

SnapDrive creates a new rolling Snapshot copy 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 copy for each virtual disk is always available on the destination volume, SnapDrive maintains a maximum of two rolling Snapshot copies on the source volume.

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

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

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

@snapmir@{*GUID*}

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

Examples: The following are examples of rolling Snapshot copies:

@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 202 before you use the procedures in this section.

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

If...	Then...
You want to manually create a Snapshot copy	See “ Creating a Snapshot copy ” on page 160.
You want to set up a schedule for Snapshot copy creation	See “ Scheduling Snapshot copies ” on page 161.

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 copy of the virtual disk is created. After the Snapshot copy 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 copy 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 relationship, it performs a Single File SnapRestore (SFSR) on the most recent Snapshot copy containing a consistent image of the virtual disk.

Note

If you are running Data ONTAP 7.1 or later, instead of performing a Single File SnapRestore, SnapDrive will perform a rapid LUN restore (LUN clone and split operation) when restoring a LUN from a Snapshot copy.

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.	
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 storage system. See “Connecting virtual disks” on page 126 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 or rapid LUN restore, 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.	

Step	Action	
7	In the Select Virtual Disk Drive Letter window, examine the properties of the virtual disk and assign a drive letter, then click Next.	
8	In the Select Initiators window, select an initiator for each host in the cluster. See “ Connecting virtual disks ” on page 126 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 213 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. b. Expand the Services and Applications option in the left pane of the MMC, if it is not expanded already. c. Click Services in the left pane of the MMC. d. Double-click Cluster Service. e. 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. _____

Step	Action
3	On one of the nodes in the cluster, complete the following steps. 1. Create a shared disk on the SnapMirror destination storage system to be used as a temporary quorum disk. See “Creating a virtual disk” on page 107. After you have successfully completed the Create Disk wizard, you see the following message. This message is expected and does not indicate a problem. “You have successfully configured a disk on this system with the intention of it being a shared resource in MSCS. As MSCS does not appear to be installed on this system, please install MSCS.” 2. Click OK to ignore the message. 3. Disconnect the shared disk you just created. See “Disconnecting virtual disks” on page 135. 4. Start the cluster service using the -fixquorum option. a. Select Start > Programs > Administrative Tools > Computer Management. b. Expand the Services and Applications option in the left pane of the MMC, if it is not expanded already. c. Click Services in the left pane of the MMC. d. Double-click Cluster Service. e. In the Start Parameters field, enter -fixquorum. f. In the Service Status field, click Start, then click OK. 5. Reconnect the shared disk you created in Step 1. See “Connecting virtual disks” on page 126. 6. Using the Cluster Administrator, make the newly connected shared disk the quorum disk. 7. Stop the cluster service, then restart the cluster service on all nodes in the cluster. 8. Remove dependencies on all failed physical disk resources, then remove the physical disk resources.

Step	Action
4	On the cluster node you used in Step 3, follow the steps described in “Connecting a virtual disk” on page 126, keeping in mind the following information to connect to a virtual disk: ◆ 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 copy) on the SnapMirror destination volume. ◆ After you specify the virtual disk path and click Next, you see a message that a single file SnapRestore or rapid LUN restore 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
5	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 might also appear 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. _____ Click OK to ignore the error message.
6	Repeat Step 4 and 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	Restore any resource dependencies you removed in Step 3 .

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. ◆ Move the quorum disk from the temporary disk you created in Step 3 back to the original disk. ◆ Delete the temporary disk. 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 224
- ◆ “[SnapDrive license commands](#)” on page 225
- ◆ “[Fractional space reservation monitoring commands](#)” on page 226
- ◆ “[SnapDrive preferred IP address commands](#)” on page 229
- ◆ “[iSCSI connection commands](#)” on page 230
- ◆ “[iSCSI initiator commands](#)” on page 231
- ◆ “[Virtual disk commands](#)” on page 233
- ◆ “[Multipathing commands](#)” on page 239
- ◆ “[Snapshot commands](#)” on page 243

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 220
- ◆ [“Common command switches”](#) on page 221
- ◆ [“Command-specific switches”](#) on page 223

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 cmd 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\NetApp\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 or mount point assigned to the virtual disk. If <code>sdcli</code> cannot 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 or mount points 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 239.
-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 storage system. 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> -module either LPSM (LUN Provisioning and Snapshot Management) or NTAPMPIO -key 14 character license key Example: <pre>sdcli license set -module LPSM -key ABCDEFGHIJKLMN</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>

Fractional space reservation monitoring commands

The `sdcli` utility supports the following fractional space reservation monitoring commands: `get`, `set`, `snapdelta`, `snapreclaim`, and `getvolinfo`.

Operation
<code>spacemon get</code> displays the space reservation monitoring settings for the specified host. Syntax: <pre>sdcli spacemon list {-m <i>MachineName</i>}</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.

Operation

spacemon set sets the space reservation monitoring settings for the specified host.

Syntax:

```
sdcli spacemon set -mi Monitoring interval -f filename -vn Volume Name { -m MachineName} -rap Threshold for Reserved Available Percentage -roc Threshold for Rate of Change -ccs true|false
```

Monitoring interval is the frequency, in minutes, at which you want to monitor fractional space available.

filename is the name of the storage system on which the LUNs reside.

Volume Name is the name of the volume you want to monitor.

Threshold for Reserved Available Percentage is the point at which you want to be warned of a low space reservation condition.

Threshold for Rate of Change is the point at which you want to receive a notification. Use kb, mb, gb, or tb to specify the value as kilobytes, megabytes, gigabytes, or terabytes.

-ccs is used to monitor whether a Snapshot copy can be created. True indicates that you want to monitor whether a Snapshot copy can be created. False indicates that you do not want to monitor whether a Snapshot copy can be created.

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.

Example:

```
sdcli spacemon set -mi 30 -f filer1 -vn testvol -rap 90 -roc 500mb -ccs true
```

The preceding example shows that fractional space reservations will be monitored every 30 minutes on the volume named testvol on filer1. The threshold for testvol is 90 percent of the reserved available percentage and the threshold for rate of change is 500 MB. SnapDrive will verify storage system and volume names and that space is available for Snapshot copies to be created.

Operation
<code>spacemon snap_delta</code> displays the rate of change between two Snapshot copies or between a Snapshot copy and the active file system of the storage system volume. Syntax: <pre>sdcli spacemon snap_delta -f <i>filename</i> -vn <i>Volume Name</i> -s1 <i>snapshot1 name</i> -s2 <i>snapshot2 name</i> {-m <i>MachineName</i>}</pre> <i>filename</i> is the name of the storage system on which the volume exists. <i>Volume Name</i> is the name of the volume for which you want to display the snap delta. <i>snapshot1</i> is the name of the Snapshot copy you want to compare with either a second Snapshot copy or with the active file system. <i>snapshot2</i> is name of the second Snapshot copy. <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>spacemon snap_reclaimable</code> displays the space that can be reclaimed by deleting a Snapshot copy. Syntax: <pre>sdcli spacemon snap_reclaimable -f <i>filename</i> -vn <i>Volume Name</i> -s <i>snapshot</i></pre> <i>filename</i> is the name of the storage system on which the volume exists. <i>Volume Name</i> is the name of the volume on which the Snapshot copy resides. <i>snapshot</i> is the name of the Snapshot copy for which you want to view reclaimable space.
<code>spacemon vol_info</code> displays information about fractional space reserved volumes.
<code>spacemon delete</code> enables you to delete the fractional space reservation monitor settings for the specified storage system volume. Syntax: <pre>sdcli spacemon delete -f <i>filename</i> -vn <i>Volume Name</i> {-m <i>MachineName</i>}</pre> <i>filename</i> is the name of the storage system on which the volume exists. <i>Volume Name</i> is the name of the volume from which you want to delete fractional space reservation settings.

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 storage system. Syntax: <pre>sdcli preferredIP set -f <i>FilerName</i> -IP <i>PreferredIPAddress</i></pre> Example: <pre>sdcli preferredIP set -f filer1 -IP 172.18.53.94</pre> The preceding example sets the SnapDrive preferred IP address for the storage system 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 storage system. Syntax: <pre>sdcli preferredIP delete -f <i>FilerName</i></pre> Example: <pre>sdcli preferredIP delete -f 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 <i>TargetName</i></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 <i>FilerName</i> -i <i>InitiatorPortName</i>}</pre> <code>-f</code> displays all targets on the specified storage system. Example: <pre>sdcli iscsi_target list -f filer2</pre> The preceding example lists all the iSCSI targets on the <code>filer2</code> storage system, 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. -s 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> -h <i>HBA_ID</i> is used to establish the iSCSI session. The HBA ID can be obtained by using the <code>sdcli sysconfig list</code> command. -hp <i>HBA Portal ID</i> 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. -t <i>TargetName</i> is the name of the iSCSI target. -np <i>IP Address IPPort</i> specify the IP address and IP port of the network portal on the target. The IP Port can be obtained by using 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
disk create creates a new virtual disk. Syntax: <pre>sdcli disk create [-m MachineName] -p UNC path -d MountPoint -z DriveSize -I [[NodeMachineName InitiatorName] ...] -dtype {shared dedicated} {[-e "ResourceGroupName"] [-n "ResourceGroupName" "ResourceGroupDesc"]}</pre> For an explanation of the switches listed in the <code>disk create</code> syntax, see “Common command switches” on page 221. 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.

Operation

`disk connect` connects a virtual disk (LUN) to a host by mapping the virtual disk to a Windows drive letter.

Syntax:

```
sdcli disk connect [-m MachineName] -p UNCpath -d MountPoint [-I [NodeMachineName  
InitiatorName] ...] -dtype {shared | dedicated} {[-e "ResourceGroupName"] | [-n  
"ResourceGroupName" "ResourceGroupDesc"]} [-c "ClusterName"]
```

Example:

```
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"
```

The preceding example connects a virtual disk (LUN) in the filer2 volume `sd_vds_only` and named `mktng.lun`, which belongs to the MSCS cluster resource group `tech_mktng` on the `mktng` cluster. MPIO paths are connected for both nodes on the cluster.

`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`.

Operation

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 MountPoint}
```

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 storage system identified by the IP address 133.25.61.62.

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 MountPoint} [-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.

Operation

`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 MountPoint} -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 copy, this displays the storage system-side path to the Snapshot copy)
- ◆ Shared (whether the disk is dedicated or shared)
- ◆ BootOrSystem Disk
- ◆ SCSI port
- ◆ Bus
- ◆ Target
- ◆ LUN
- ◆ Readonly
- ◆ Disk size (in megabytes)
- ◆ Clone Split Restore status
- ◆ Disk ID
- ◆ Volume name
- ◆ Mount points (the drive letter and path to which the virtual disk is mapped on the host)
- ◆ IP Addresses (IP addresses on the target storage system)

Operation

`disk add_mount` adds a volume mount point.

Syntax:

```
sdcli disk add_mount {-m MachineName} -vn Volume Name -mp Volume Mount Point {-create_folder}
```

Volume Name is the name of the volume where you are creating the mount point. The volume name can be located in the output from the `disk list` command.

Volume Mount Point is the location you want to mount the LUN. This can also be a drive letter.

Example:

```
sdcli disk add_mount -vn \\?\Volume{db6160d8-1f14-11da-8ef3-000d5671229b} -mp  
G:\mount_vol1 -create_folder
```

`disk remove_mount` removes a volume mount point or drive letter.

Note

This command will not delete the folder that was created at the time the volume mount point was added. After you remove a mount point, an empty folder will remain with the same name as the mount point you removed.

Syntax:

```
sdcli disk remove_mount {-m MachineName} -vn Volume Name -mp Volume Mount Point
```

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 storage system 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
path activate 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 <i>MachineName</i>] -ID <i>PathID</i></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.
path add creates a new virtual path from the initiator on the host to the virtual disk on the storage system. 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 <i>MachineName</i>] {-p <i>UNCpath</i> -d <i>MountPoint</i>} -i <i>InitiatorPortName</i></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.
path disable puts the specified path on standby. (This operation can only be performed on a passive path.) Syntax: <pre>sdcli path disable [-m <i>MachineName</i>] -ID <i>PathID</i></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 MountPoint}
```

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 storage system 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 MountPoint} -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 copy-related operations supported by sdcli: create, delete, list, mount, rename, restore, unmount, and update mirror.

Operation
sdcli snap create creates a new Snapshot copy of the specified virtual disks on the SnapDrive system. Syntax: <pre>sdcli snap create [-m MachineName] -s SnapshotName -D MountPointList [. . .] [-x]</pre> -x causes data to be flushed and consistent Snapshot copies to be created only for the drives and mount points specified by the -D switch. Otherwise, SnapDrive flushes data and creates consistent Snapshot copies for all virtual disks connected to the host and residing on storage system volumes. Note Snapshot copies are created at the volume level. When a Snapshot copy is created using -x with the -D switch, Snapshot copies are also created for any additional disks mapped to the host that reside on the same volumes as the disks specified. Snapshot copies for the unspecified disks are dimmed 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 copy 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 Snapshot copies created are consistent for all virtual disks contained by those volumes.
sdcli snap delete deletes an existing Snapshot copy. Note You must make sure that the virtual disk whose Snapshot copy you are deleting is not being monitored with the Windows Performance Monitor (perfmon). Syntax: <pre>sdcli snap delete [-m MachineName] -s SnapshotName -D MountPointList [. . .]</pre> Example: <pre>sdcli snap delete -s Jun_13_03 -D k</pre> The preceding example deletes the Snapshot copy named Jun_13_03 that is associated with the virtual disk mapped to K: on the local host.

Operation
sdcli snap list lists all the Snapshot copies that exist for the specified virtual disk. <pre>sdcli snap list [-m <i>MachineName</i>] -d <i>MountPoint</i></pre> Example: <pre>sdcli snap list -d j</pre> The preceding example displays all the Snapshot copies that exist for the volume containing the virtual disk mapped to “J:” on the local host.
sdcli snap mount mounts a Snapshot copy 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>LiveMountPoint</i> -s <i>SnapshotName</i> -d <i>MountPoint</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, -r defaults to the local host. <i>LiveMountPoint</i> refers to the drive letter or mount point 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 copy named Jun_13_03 to drive T: on the local host. This Snapshot copy represents a point-in-time image of the virtual disk mapped to J: on host3.
sdcli snap rename enables you to change the name of an existing Snapshot copy. Syntax: <pre>sdcli snap rename [-m <i>MachineName</i>] -d <i>MountPoint</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 June_13_03 Snapshot copy associated with the J: drive to last_known_good.

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 copy.

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 MountPoint -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 copy named Jun_13_03 was taken.

`snap unmount` disconnects a Snapshot copy of a virtual disk that is mounted as a virtual disk.

Note

You must make sure that the virtual disk whose Snapshot copy you are disconnecting is not being monitored with the Windows Performance Monitor (perfmon).

Syntax:

```
sdcli snap unmount [-m MachineName] -d MountPoint [-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 copy mapped to K: on the local host.

```
sdcli snap unmount -d k -f
```

The preceding example forces disconnection of the Snapshot copy 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 storage system.

Syntax:

```
sdcli snap update_mirror [-m MachineName] -d MountPoint
```

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 ix.

Host requirements: See the following sections:

- ◆ “[Preparing hosts](#)” on page 38
- ◆ “[Recommendations for choosing a configuration](#)” on page 25

Storage system requirements: See “[Preparing storage systems](#)” on page 42.

SnapDrive service account requirements: See “[Preparing the SnapDrive service account](#)” on page 57.

Volume and storage system options: See “[Volume and storage system options set by SnapDrive](#)” on page 43.

Cluster recommendations: See “[Recommendations for choosing a configuration](#)” on page 25.

SnapDrive-specific limitations: See “[SnapDrive-specific limitations](#)” on page 44.

SnapDrive-specific cautions and recommendations: See “[Recommendations](#)” on page 45.

SnapDrive user interfaces: See “[SnapDrive user interfaces](#)” on page 59.

Index

A

- abnormal disconnect (of virtual disk) 136
- access protocols 13
- accessing virtual disks 13
- administration, remote 151
- archives, restoring from 174
- archiving, Snapshot copies 174
- asynchronous replication 202
- authentication, pass-through 53
- AutoSupport (storage system), enabling 152

B

- BUILTIN/administrators group 57
- busy snapshot error 173

C

- Challenge Handshake Authentication Protocol (CHAP), understanding 99
- changing path states, MPIO 196
- changing SnapDrive service account password 57
- CIFS
 - limited functionality supplied with FCP and iSCSI license 43, 45
 - setup 48
- CIFS shares 48
- cluster
 - See also* Windows cluster
 - "private" network 30
 - Cluster Service (MSCS), definition of 6
 - FCP configurations 33
 - iSCSI configurations 30
 - MPIO configurations 36, 37
 - support in SnapDrive 9
- configurations
 - choosing 25
 - FCP 32
 - guidelines 25
 - iSCSI 28
 - multipathing (MPIO) 35, 188
- connecting

- to (mirrored) destination volumes 209
- to a virtual disk 126
- to virtual disks (LUNs) in a Snapshot copy 164
- create
 - shared virtual disks (on a Windows cluster) 114
 - Snapshot copies using SnapDrive 158
 - Snapshot copy using SnapDrive 160
 - virtual disks 108
- creating
 - CIFS share 48
 - iSCSI session 97
 - qtree 47
 - storage system volume 47
- crossover FCP cable 32

D

- Data ONTAP, required version 42
- data restore from Snapshot copies 168
- dedicated storage system volume required for virtual disks (LUNs) 46
- deleting
 - a virtual disk 138
 - a volume mount point 138
 - a volume mount point folder 140
 - Snapshot copy 172
 - Snapshot copy, problems with 173
- details of iSCSI sessions 103
- df -r (storage system command) 17
- disconnecting
 - a virtual disk 135
 - forced (of virtual disk) 136
 - from an iSCSI target 100
- disks
 - hot spare 14
 - virtual 106
- documentation
 - Data ONTAP 48
 - filer 42
 - obtaining 24
- drive letters, list incorrect when viewed via

Terminal Service 60
drivers, obtaining 39
dump command 174

E

e-mail notification, setting up 152
expand
 virtual disks 141
expanding
 a quorum disk 143
 virtual disks 142

F

failover
 definition 4
 NetApp cluster 9
FCP
 adapters 36
 configurations 32
 crossover cable 32
 documentation 24
 Host Bus Adapter (HBA) 24
 initiator 11
 installing 73
 license required on filer 43
 MPIO configurations 35, 36
 obtaining firmware and driver 39
 single-host, single-filer configurations 32
 switch 33, 36
 switched configuration 33
 uninstalling driver 92
 windows cluster configurations 33
features, updating mirrors 207
Fibre Channel Protocol. *See* FCP
fields in an iSCSI session 103
file system 5
filer, definition of 4
FilerView
 checking filer licenses 43
 creating a volume 47
 definition 59
 opening a session 47
 setting snap reserve 51
firmware, obtaining 39

forcing disconnect (of a virtual disk) 136

G

GbE (Gigabit Ethernet)
 iSCSI configurations 28
 switch 37
 switched configuration 29
guidelines
 for choosing SnapDrive configuration 25
 for creating storage system volumes 46

H

host 5
Host Bus Adapter (HBA)
 definition of 5
 documentation, for FCP 24
host console
 definition 59
hot spare disks 14

I

initiator
 definition of 5
 obtaining iSCSI 39
Initiator HBA field 103
Initiator IP address field 103
installing
 FCP 73
 first time 72
 iSCSI 73
 SnapDrive components 80
IP address, setting preferred 88
iSCSI
 cluster configurations 30
 configurations 28
 initiator 11
 installing 73
 license required on filer 43
 MPIO configurations 35, 37
 obtaining software 39
 single-host, single-filer configurations 28
 software initiator node name standards 97
 upgrading 76

- upgrading a non-clustered host 76
- upgrading a Windows cluster 77
- uninstalling 93
- iSCSI connections
 - creating 97
- iSCSI sessions
 - details 103
 - disconnecting from a target 100
 - establishing 97
 - ways to establish 96
- iSCSI Target Name field 103

L

- latency, minimizing with GbE crossover cable 28
- licensable modules
 - about 2
 - feature availability 2
 - managing 2, 3
- licenses 43
- limitations
 - LUN cloning 45
 - qtree quotas. 44
 - SnapDrive 44
- Logical Unit Numbers. *See* LUNs
- LUN clones
 - about 168
 - how SnapDrive uses 169
- LUNs
 - See also* virtual disks
 - cloning not supported 45
 - dedicated storage system volume required 46
 - definition of 5
 - not visible when created via Terminal Service 59
 - snap reserve setting on filer 51
- LUN-type virtual disks, definition 6

M

- mpdev.sys file 185
- MPIO
 - accessing using MMC 193
 - active path 185
 - changing path states 196
 - configurations 35

- drivers 10
- enabling 188
- overview 185
- passive path 185
- path IDs 239
- path states 195
- requirements, hardware and software 186
- supported topologies 188
- uninstalling 92
- mpio.sys file 185
- MSCS
 - See also* Windows cluster
 - definition 6
 - FCP configurations 33
 - iSCSI configurations 30
 - MPIO configurations 36, 37
- msspsfltr.sys 185
- multipathing. *See* MPIO

N

- NDMP-based backup application 174
- NetApp Windows Attach Kit for FCP
 - documentation 24
- Network Interface Card (NIC), definition of 6
- network, "private" for internal cluster traffic 30
- non-SnapDrive LUNs
 - managing 146
 - preparing for SnapDrive 146
 - prerequisites for SnapDrive 146
- notification settings for SnapDrive 152
- ntapdsm.sys file 185
- NTFS 5
- Number of LUNs field 103

O

- obtaining firmware and drivers 39
- operating system
 - required on Windows host 39
 - storage system requirement 42
- options, snap reserve 51

P

- pass-through authentication 53

- password, changing for SnapDrive service account 57
- path states, MPIO 195
- preferred IP address, setting 88
- protocols, connection 13

Q

- qtrees
 - creating 47
 - SnapDrive limitation 44
- quorum
 - creating a virtual disk as a 115
 - expanding 143

R

- read/write mode, connecting to Snapshot copies in 164
- remote administration
 - definition of 59
 - of SnapDrive 151
- replication
 - asynchronous 202
 - initiating 207
 - SnapMirror 205
 - synchronous 202
 - upon Snapshot copy creation 205
 - using rolling Snapshot copies 205
- requirements
 - administrator access to filer 57
 - Data ONTAP 42
 - filer licenses 43
 - for SnapMirror 202
 - for Snapshot copy 159
 - operating system 39
 - SnapDrive service access to Windows 57
 - SnapDrive service account 57
 - storage system 42
 - Windows domain 57
 - Windows host 38
- restoring
 - from Snapshot copy 168
 - virtual disks from archives 174
- rolling Snapshot copies
 - described 205

- rules
 - for connecting to virtual disks 126
 - for creating virtual disks 107
 - for managing virtual disks 106
 - for Snapshot copies 164

S

- SAN (Storage Area Network), definition of 6
- SAN booting
 - about 199
 - support in SnapDrive 9
- scheduling Snapshot copies 161
- sdcli commands
 - about 220
 - executing 220
 - for iSCSI connection 230
 - for Snapshot copy 243
 - multipathing commands 239
 - switches (options) available for 221
 - disk connect 234
 - disk convert 234
 - disk create 233
 - disk delete 235
 - disk disconnect 235
 - disk expand 236
 - disk list 237
 - iscsi_initiator establish_session 231
 - iscsi_initiator list 231
 - iscsi_initiator terminate_session 232
 - iscsi_target disconnect 230
 - iscsi_target list 225, 230
 - license set 225
 - path activate 197, 240
 - path add 197, 240
 - path disable 197, 240
 - path enable 197, 241
 - path list 241
 - path remove 197, 241
 - path version 242
 - preferredIP list 229
 - preferredIP set 229
 - snap create 243
 - snap delete 243
 - snap list 244

- snap mount 244
 - snap rename 244
 - snap restore 245
 - snap unmount 245
 - snap update_mirror 246
- service account
 - requirements 57
- service packs
 - SP1 26
- session, iSCSI
 - details 103
 - disconnecting 100
 - ways to establish 96
- sessions, iSCSI
 - establishing 97
- setting a preferred IP address 88
- single-homed configuration, using GbE switch 29
- single-host, single-filer configurations
 - FCP 32
 - iSCSI 28
- snap reserve, recommended setting 16, 51
- SnapDrive
 - capabilities 8
 - command-line interface 10
 - command-line interface reference 219
 - components 9
 - determining what components are installed 40
 - filer options set automatically 43
 - installing components 80
 - limitations 44
 - preparing to install 23
 - selecting configurations 25
 - service account 57
 - snap reserve on filer 51
 - uninstalling 91, 92
 - user interfaces 59
- SnapDrive service, stopping and starting
 - stopping and starting the SnapDrive service 89
- SnapMirror
 - asynchronous replication 202
 - connecting to (mirrored) destination volumes 209
 - described 202
 - initiating replication 207
 - license required on filer 43
 - overview 202
 - replication 205
 - requirements for using with SnapDrive 202
 - rolling Snapshot copies 205
 - synchronous replication 202
 - Update Mirror feature 207
 - using with SnapDrive 201
- SnapRestore, licence required on filer 43
- Snapshot copy
 - archival 174
 - connecting to virtual disks (LUNs) 165
 - definition 6
 - deleting 172
 - described 156
 - effect on disk space 17
 - errors when deleting 173
 - how to create 160
 - reason for creating 158
 - replication upon creation of 205
 - requisites for 159
 - restoring from 168
 - restrictions on creating 158
 - rolling 205, 206
 - scheduling 161
 - space required 15
- SP1, feature support 26
- space reservation
 - example 17
 - overview 16
 - storage system setting 16
- states, path (MPIO) 195
- storage system
 - BUILTIN/administrators group 57
 - creating a volume 47
 - dedicated volume required for LUNs 46
 - df -r command 17
 - documentation 42
 - guidelines for creating volumes 46
 - interaction with virtual disks 12
 - licenses required 43
 - options set by SnapDrive 43
 - preparing 42
 - requirements 42
 - resetting the snap reserve 51
 - settings for SnapDrive 16

- upgrading 79
- user interfaces 59
- volume preparation 45
- Windows domain account 57
- storage system cluster
 - FCP configurations 33
 - iSCSI configurations 30
 - MPIO configurations 36, 37
- storage system console, definition 59
- synchronous replication 202

T

- target 6
- Target Portal IP Address field 103
- Target Portal Port field 103
- Telnet, description of 59
- Terminal Service
 - definition 59
 - drawbacks 59
 - workaround for problems 60

U

- unattended installations
 - examples of command syntax 87
 - performing 85
 - switch descriptions 85
- uninstalling
 - FCP driver 92
 - iSCSI initiator 93
 - SnapDrive and MPIO 92
 - SnapDrive components 91
 - VLD driver 91
- Update Mirror feature 207
- upgrading
 - cluster without VLDs 65
 - filer 79
 - iSCSI initiator 76
 - procedures 62
 - single system without VLDs 70
 - to Windows 2003 63
- user interfaces
 - for SnapDrive and the filer 59
 - recommended for various operations 60

V

- viewing
 - details of an iSCSI session 103
- Virtual Disk Service
 - dependency on 8
- virtual disks
 - capabilities 12
 - connecting to 126
 - creating as a quorum 115
 - creating shared 114, 123
 - data access overview 13
 - dedicated storage system volume required 46
 - deleting 138
 - disconnecting 135
 - documentation about protocols 24
 - expanding 142
 - expanding quorum disks 143
 - how to create 108
 - limitations 12
 - LUN-type, definition 6
 - managing, rules about 106
 - not visible when created via Terminal Service 59
 - rules for creating 107
 - snap reserve setting on filer 51
 - storage system interaction 12
 - storage system options set on creation and connection 43
 - VLD-type, definition 7
 - Windows interaction 12
- VLD driver, uninstalling 91
- volume
 - connecting to (mirrored) destination 209
 - contents 15
 - creating 47
 - definition 7
 - guidelines for creating 46
 - options set by SnapDrive 43
 - preparation 45
 - recommendations for configuring 46
 - resetting snap reserve 51
 - restricted to single host 46
 - sizing 15
- volume mount point
 - about 107

- deleting 138
- deleting folder within 140
- limitations 107
- VSS, requirements 176

W

- WAFL 5
- Windows 2000 Server cluster. *See* Windows cluster
- Windows cluster
 - creating a shared virtual disk 114

- creating a virtual disk as a quorum 115
- definition of 7
- FCP configurations 33
- iSCSI configurations 30
- Windows domain, requirements 57
- Windows host
 - administrator access required 57
 - preparing 38
 - requirements 38
- Windows Server 2003 cluster. *See* Windows cluster

