

SnapDrive™ 3.0

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 215-00626
October 2003

Copyright and trademark information

Copyright information

Copyright © 1994—2003 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this book 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 and purchase of this product do 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 and the Network Appliance design are registered trademarks of Network Appliance, Inc. in the United States, Canada, and the European Union. Network Appliance is a registered trademark of Network Appliance, Inc. in Monaco and a trademark of Network Appliance, Inc. in the United States and Canada. FAServer is a registered trademark of Network Appliance, Inc. in the United States and the European Union. NetCache is a registered trademark of Network Appliance, Inc. in the United States, Canada, the European Union, and Japan. SnapCopy is a registered trademark of Network Appliance, Inc. in the European Union and a trademark of Network Appliance, Inc. in the United States. WAFL is a registered trademark of Network Appliance, Inc. in the United States, the European Union, and Canada. DataFabric, FilerView, NearStore, SecureShare, SnapManager, SnapMirror, and SnapRestore are registered trademarks of Network Appliance, Inc. in the United States. Data ONTAP is a trademark of Network Appliance, Inc. in the United States and Canada. Snapshot is a trademark of Network Appliance, Inc. in the United States and the European Union. NetApp—the Network Appliance Company is a registered trademark of Network Appliance, Inc. in the United States and other countries. ApplianceWatch, BareMetal, Center-to-Edge, ContentDirector, gFiler, MultiStore, SecureAdmin, Serving Data by Design, Smart SAN, SnapCache, SnapDrive, SnapVault, vFiler, and Web Filer are trademarks of Network Appliance, Inc. in the United States.

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

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

Table of Contents

	Preface	ix
Chapter 1	Overview of SnapDrive	1
	SnapDrive-specific terms and technologies	2
	How SnapDrive works	5
	Configuring pass-through authentication for SnapDrive	8
	How virtual disks work	11
	Understanding filer storage	13
	Planning disk allocation	14
	Understanding volume size	15
Chapter 2	Preparing to Install SnapDrive	21
	What to read	22
	Selecting a SnapDrive configuration	23
	iSCSI configurations	25
	FCP configurations	29
	MPIO configurations	32
	Preparing hosts	34
	Preparing filers	36
	Preparing the SnapDrive service account	48
Chapter 3	Installing or Upgrading SnapDrive	55
	Upgrading to SnapDrive 3.0	56
	Upgrading to SnapDrive 3.0 and Microsoft Windows Server 2003	58
	Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks	60
	Upgrading a single system to SnapDrive 3.0 and converting VLD-type virtual disks	65
	SnapDrive 3.0 upgrade and conversion process	66
	VLD-to-LUN conversion	73
	Upgrading a server cluster to SnapDrive 3.0 if you have no VLD-type virtual disks	

Upgrading a single system to SnapDrive 3.0 if you have no VLD-type virtual disks
99

Installing SnapDrive for the first time	100
Installing the FCP or iSCSI components	101
Installing the new SnapDrive components	104
Upgrading the filer	112
Uninstalling old components	113

Chapter 4

Managing iSCSI connections	119
Tasks for managing iSCSI connections	120
Establishing an iSCSI connection to a target.	121
Disconnecting an iSCSI target from a Windows host	125
Examining details of iSCSI connections	126

Chapter 5

Creating Virtual Disks	129
About virtual disk management	130
Creating a virtual disk	131
Creating a shared virtual disk on a Windows cluster.	141
Creating a virtual disk as a quorum disk on a new Windows cluster.	142
Creating a virtual disk as a quorum disk on a new Windows 2000 Server cluster.	144
Creating a virtual disk as a quorum disk on a new Windows Server 2003 cluster.	146
Creating a shared virtual disk on a Windows cluster.	153

Chapter 6

Managing Virtual Disks.	155
Connecting virtual disks	156
Disconnecting virtual disks	164
Deleting a virtual disk	167
Expanding virtual disks.	168
Examining and modifying virtual disk properties	172

	Administering SnapDrive remotely	174
	Enabling SnapDrive notification	175
Chapter 7	SnapDrive Snapshots	177
	How snapshots work	178
	Creating snapshots	180
	Connecting to LUNs in a snapshot	187
	Restoring virtual disks from snapshots	194
	Deleting snapshots	197
	Overview of archiving and restoring snapshots	199
Chapter 8	Multipathing	201
	Multipathing overview	202
	MPIO setup	204
	MPIO path management	206
Chapter 9	Using SnapMirror with SnapDrive	211
	SnapMirror overview	212
	SnapMirror replication	214
	Initiating replication	216
	Connecting to destination volumes	218
	SnapMirror disaster recovery	221
Appendix A	SnapDrive Command-Line Reference	223
	iSCSI connection commands	227
	Virtual disk commands	229
	Multipathing commands	233
	Snapshot commands	236
Appendix B	SnapDrive Requirements and Recommendations.	241

.....	.249
-------	------

Preface

About this guide

This document describes how to install, configure, and operate SnapDrive™ 3.0 software. It does not cover basic system or network administration topics, such as IP addressing, routing, and network topology.

Audience

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

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

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

About filer command execution

You can manage filers in the following three ways:

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

Note

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

Interface conventions

Throughout this document, all examples involving commands and procedures assume a host running Windows 2000 Server or Windows Server 2003.

For procedures that use the Windows graphical user interface, the term “select” means that you should click, double-click, or right-click the control element, as appropriate. In many instances, you can press a corresponding key to achieve the same result. For example, if that element is a radio button, a dot appears in the

associated circle; if it is a check box, an “x” appears in the box; if it is an item in a drop-down list, that item becomes highlighted; if it is a button control, a command is usually executed, and so on.

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

Keystrokes: When describing key combinations, this guide 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 an 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.
Monospaced font	Command and daemon names. Information displayed on the system console or other computer monitors. The contents of files.

Convention	Type of information
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 guide 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.

About this chapter This chapter explains the SnapDrive technology.

Topics in this chapter This chapter covers the following topics:

- ◆ “[SnapDrive-specific terms and technologies](#)” on page 2
- ◆ “[How SnapDrive works](#)” on page 5
- ◆ “[How virtual disks work](#)” on page 11
- ◆ “[Understanding filer storage](#)” on page 13

SnapDrive-specific terms and technologies

About this section	This section defines the terms and technologies that you come across while reading this document. The section defines the terms in a <i>SnapDrive-specific</i> context.
Block pointers	Block pointers are used by a filer to locate the physical disk block on which data is stored.
Cluster Service—Microsoft Cluster Service (MSCS)	The 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. <i>See also</i> Windows Server cluster.
Failover	Failover refers to situations where a system component fails, and another component takes over its functions while the system continues to operate.
Filer	A filer is a NetApp® storage appliance that supports the FCP (Fibre Channel Protocol), iSCSI, and/or GbE (Gigabit Ethernet) protocols.
File system	A file system refers to NTFS, the native Windows 2000 Server and Windows Server 2003 file system supported by SnapDrive. (NetApp filers use the WAFL® file system internally, but SnapDrive makes WAFL transparent to virtual disk users, who interact with data stored on the filer using Windows procedures only.)
Host	A host is a computer system that accesses storage on a filer. For this document, the host must be running the following software: ◆ One of the following Windows server software: ❖ Windows 2000 Server

- ❖ Windows 2000 Advanced Server (for Windows-cluster configurations)
- ❖ Windows Server 2003 (Standard Edition or Enterprise Edition)
- ◆ SnapDrive 3.0

Host Bus Adapter (HBA)

A Host Bus Adapter (HBA) refers to the adapters used to connect hosts and filers in a NetApp SAN so that hosts can access Logical Unit Numbers (LUNs) on the filers using FCP. *See also* Logical Unit Number (LUN).

Initiator

An initiator is used to send SCSI I/O commands to a target.

FCP initiator: An FCP initiator refers to a port on an HBA on a host.

iSCSI initiator: An iSCSI initiator refers to a port on a NIC on a host.

See also 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 Logical Unit Numbers (LUNs) as virtual disks, and vice versa. *See also* 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. SnapDrive 3.0 and later versions support only LUN-type virtual disks.

Network Interface Card (NIC)

A network interface card (NIC) refers to a Gigabit (commonly known as GbE) or a Fast Ethernet card that is compliant with the IEEE 802.3 standards.

These cards can provide the following connectivity functions:

- ◆ Connect hosts and filers to a local area network (LAN)
- ◆ Connect hosts and filers to data-center switching fabrics, specifically, enable hosts to connect to LUNs on filers using iSCSI

Snapshot	A snapshot refers to the NetApp Snapshot™ technology, which facilitates recovery after accidental deletion or modification of the data stored on a filer by referencing a point-in-time image of that data.
Storage Area Network (SAN)	A Storage Area Network (SAN) is a storage setup composed of one or more filers and connected to one or more hosts in an FCP or an iSCSI environment. To a Windows host running SnapDrive, a connected SAN is just another target storage device within which SnapDrive can create and manage virtual disks (LUNs). <i>See also</i> target and virtual disk.
Target	A target is used to receive the SCSI I/O commands that an initiator sends. For NetApp SANs, a target is a NetApp filer. <i>See also</i> initiator.
Virtual disk	A virtual disk is a functional unit of filer storage that, for all practical purposes, behaves like a locally attached disk on a Windows host. This manual often refers to virtual disks as Logical Unit Numbers (LUNs), and vice versa.
VLD-type virtual disk	A VLD-type virtual disk is a type of virtual disk created and supported by SnapDrive 2.1 and earlier versions to store data in GbE environments. VLD-type virtual disks are legacy and are not supported in SnapDrive 3.0 or later versions.
Volume	A volume is a functional unit of filer storage comprising of a collection of physical disks. A volume can be composed of one or more RAID groups to ensure data integrity and availability if multiple disks fail simultaneously within the same volume. For more information about filer volumes, see the <i>Data ONTAP Storage Management Guide</i> .
Windows Server cluster	A Windows Server cluster refers to a two-node to a four-node host cluster. The number of nodes in a cluster depends on the software running on the host nodes. The host nodes in a Server cluster must be running one of the following software packages: ◆ Windows 2000 Advanced Server (for a 2-node cluster) ◆ Windows Server 2003 Enterprise Edition (for up to a 4-node cluster)

How SnapDrive works

What SnapDrive does

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

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

SnapDrive provides the following additional features:

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

What SnapDrive does not do

SnapDrive does not support the following uses:

- ◆ A virtual disk managed by SnapDrive cannot serve as the following:
 - ❖ A boot disk or a system disk
 - ❖ A location for the system paging file or memory dump files
- ◆ A virtual disk managed by SnapDrive cannot be configured as a “dynamic” disk; it can serve only as a “basic” disk (a storage device for host-side application data).
- ◆ In the case of a filer that uses the optional MultiStore™ feature of Data ONTAP™ software to create virtual filers (vFiler™ units), SnapDrive can create, connect to, and manage virtual disks (LUNs) only on the “hosting” filer (the physical filer), not on the vFilers.

For more information, see the *Data ONTAP MultiStore Management Guide*.

SnapDrive cluster support

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

About the SnapDrive components

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

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

Caution

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

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

- ◆ SnapDrive “snap-in”
This software module integrates with the Microsoft Management Console (MMC) to provide a graphical interface for managing virtual disks on the filer. The module
 - ❖ Resides in the Windows 2000 Server and Windows Server 2003 computer management storage tree
 - ❖ Provides a native MMC snap-in user interface for configuring and managing virtual disks
 - ❖ Supports Remote Administration so that you can manage SnapDrive on another host
 - ❖ Provides SnapMirror integration
 - ❖ Provides autosupport integration, including event notification
- ◆ SnapDrive command-line interface
The `sdcli.exe` utility enables you to manage virtual disks from the command prompt of the Windows host. You can do the following tasks with the `sdcli.exe` utility:
 - ❖ Enter individual commands
 - ❖ Run management scripts

- ◆ Underlying SnapDrive service

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

- ❖ A host
- ❖ Applications running on a host

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

- ◆ iSCSI initiator

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

- ❖ Includes an iSCSI driver that supports iSCSI connections between a host and a filer
- ❖ Is installed like a SCSI/RAID controller on a host
- ❖ Does not include an HBA hardware component (Instead the iSCSI driver enables host's standard Ethernet NIC [preferably GbE] to be used for the SCSI operations)

The necessary software for the iSCSI driver is in the iSCSI Host Support Kit for Windows at <http://now.netapp.com>.

- ◆ FCP initiator

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

- ❖ Includes an FCP driver that supports FCP connections between a host and a filer
- ❖ Is a SCSI/RAID controller on the host
- ❖ Includes an HBA hardware component

The necessary software and firmware for the FCP driver is in the FCP HBA Attach Kit for Windows at <http://now.netapp.com>.

- ◆ MPIO drivers

This set of drivers protects against path failure by enabling redundant paths from the host (initiator) to a LUN (target storage device) on the filer. These drivers

- ❖ Include one NetApp module and three Microsoft drivers
- ❖ Get installed as an option during SnapDrive installation
- ❖ Support the use of redundant FCP paths to LUNs
- ❖ Require the pair of HBAs supplied in the NetApp Dual HBA FCP Attach Kit for Windows

Configuring pass-through authentication for SnapDrive

Reasons for configuring pass-through authentication

You can use pass-through authentication between a Windows host in workgroup mode and a filer for SnapDrive. You might want to use pass-through authentication for the following reasons:

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

Configuring pass-through authentication

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

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

Step	Action
On the filer	
1	Enter the following command to create a user account: useradmin useradd <i>user_name</i> <i>user_name</i> is the name of the SnapDrive user. Note— You will need to provide the exact user name that you used to create the user account in a later step in this procedure. Therefore, make a note of the user name, including the case—lower or upper—of each character in the user name.

Step	Action
2	Enter a password when prompted to do so for the user account you are creating. You are prompted to enter the password twice. Note_____ You will need to provide the exact user name that you used to create the user account in a later step in this procedure. Therefore, make a note of the user name, including the case—lower or upper—of each character in the user name. _____
3	Check to ensure that the user account you just created belongs to the local administrator's group on the filer. For information about how to assign a user account to a specific filer group, see “Creating local groups on the filer” in the <i>Data ONTAP File Access Management Guide</i>.
4	Create a CIFS share on the filer, as described in “Creating a CIFS share” on page 43.
On each Windows host that needs access to the filer	
5	Create a local user account, making sure that the user name and password for the local user account is the same as the one you specified in Step 1 and Step 2. Tip: You should create the local user account so that the password for the account never expires. For detailed instructions about how to create local user accounts, see your Windows documentation.
6	Configure and confirm rsh access to the filer, as described in “Enabling rsh access” on page 49.

Step	Action
7	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 100. Note_____ If you are configuring pass-through authentication for Windows hosts that are clustered, you must use a domain account to run the cluster service. All nodes of the cluster must be in the same domain; however, the filer can be in a different domain or workgroup. _____

How virtual disks work

How the filer interacts with a virtual disk (LUN)

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

Note

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

How Windows hosts interacts with a virtual disk (LUN)

You manage virtual disks (LUNs) on the filer just as you manage other Windows disks that store application data. Similarly, the virtual disks on the filers are automatically formatted by SnapDrive as 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 don't need to be aware that your data files actually are part of a single virtual disk file that is stored on the filer; the intricacies of WAFL file management remain completely transparent to you as you manage SnapDrive virtual disks from the Windows host.

Virtual disk capabilities and limitations

A virtual disk managed by SnapDrive is used for data storage. A virtual disk cannot serve the following roles:

- ◆ Dynamic disk
- ◆ Boot disk
- ◆ System disk
- ◆ Location for the system paging file or memory dump files

SnapDrive can also take snapshots of virtual disks and work with SnapMirror at the volume level for disaster recovery.

Protocols to access virtual disks (LUNs)

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

- ◆ Fibre Channel Protocol (FCP)
- ◆ iSCSI

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

Overview of how data is accessed from virtual disks

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

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

Understanding filer storage

About this section This section explains how virtual disk files are stored on a filer so that you can allocate the proper amount of space as your needs evolve.

Topics covered in this section This section covers the following topics:

- ◆ “[Planning disk allocation](#)” on page 14
- ◆ “[Understanding volume size](#)” on page 15

Planning disk allocation

Configuring RAID groups

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

The number of disks in each RAID group on the filer should be balanced.

Example: Configure a volume of 16 disks as two RAID groups of eight disks each (seven data disks plus one parity disk in each group).

By contrast, if the volume had 13 disks in one RAID group and three disks in another, the three-disk group would be a potential I/O bottleneck liable to slow overall filer performance.

Hot spare disks

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

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

If the filer has multiple volumes, any available spare can replace a failed disk on any volume, as long as

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

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

Note

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

Understanding volume size

What a volume stores

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

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

Volume-size rules

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

- ◆ The volume must be more than twice the combined size of all the virtual disks on the volume if snapshots of the volume will be created. This enables the volume to hold the virtual disks and a special reserved space, so that no matter how much the contents of the virtual disks change between snapshots, the entire contents of the disks can be written to the volume. See “[How snapshots work](#)” on page 178 for more information.
- ◆ The volume must also provide enough additional space to hold the number of snapshots you intend to keep online. The amount of space consumed by a snapshot depends on the amount of data that changes after the snapshot is taken. The maximum number of snapshots is 255 per filer volume.

Requirements for space-related filer settings

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

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

Caution

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

- ◆ The snap reserve option must be reset to 0% for all volumes holding SnapDrive virtual disks.

Data ONTAP can reserve a certain percentage of raw volume capacity exclusively for snapshot creation. By default, the snap reserve percentage on the filer volume is 20%, and SnapDrive does not automatically change this. Therefore, you must manually reset the percentage to 0%. For details, see [“Resetting the snap reserve option”](#) on page 47.

What space reservation provides

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

Disk space usage with space reservation

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

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

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

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

Note

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

Action	Results	Comment
Create a 100-GB volume.	Used: 0 GB Reserved: 0 GB Available: 100 GB Volume Total: 100 GB	
Create a 40-GB virtual disk on that volume.	Used: 0 GB Reserved: 40 GB Available: 60 GB Volume Total: 100 GB Snapshot creation is allowed.	If the virtual disk size was limited to accommodate at least one snapshot when it was created, then it will always be less than one half of the volume size.
Write 40 GB of data to the virtual disk.	Used: 40 GB Reserved: 0 GB Available: 60 GB Volume Total: 100 GB Snapshot creation is allowed.	When you write data to the virtual disk, it counts against the running Used total. The sum of Used, Reserved, and Available always equals Volume Total.
Create a snapshot of the virtual disk.	Used: 40 GB Reserved: 40 GB Available: 20 GB Volume Total: 100 GB Snapshot succeeds.	The snapshot locks all the data on the virtual disk so that even if that data is later deleted, it remains in the snapshot until the snapshot is deleted. After a snapshot is created, the reserved space must now be large enough to ensure that any future writes to the disk succeed.
Overwrite all 40 GB of data on the virtual disk with entirely new data.	Used: 60 GB Reserved: 40 GB Available: 0 GB Volume Total: 100 GB Snapshot creation is blocked.	The amount of space used on the volume increases, because the original 40 GB of data belongs to the snapshot and therefore continues to count against the Used total. Reserved space must be equal to the size of the LUN (40 GB), and reserved and used space together cannot exceed the size of the volume, so used space is displayed as 60 GB rather than the expected 80 GB. However, all data is preserved. You cannot take a snapshot now, because no space is available. That is, all space is used by data or held in reserve so that any and all changes to the content of the virtual disk can be written to the volume.

Action	Results	Comment
Expand the volume by 100 GB.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation is allowed.	After you expand the volume, free space becomes available again. Therefore, snapshot creation is no longer blocked. In addition, the Used and Available totals are adjusted to reflect the fact that reserved space is no longer being used to hold disk data.
Overwrite all 40 GB of data on the virtual disk with entirely new data.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation is allowed.	Because none of the overwritten data belongs to a snapshot, it disappears when the new data replaces it, so the Used total remains unchanged.
Create a snapshot of the virtual disk.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation is allowed.	The snapshot locks all 40 GB of data currently on the virtual disk. A total of 80 GB of data now belongs to the two snapshots of the virtual disk. Reserved space remains the size of the LUN, or 40 GB.
Overwrite all 40 GB of data on the virtual disk with entirely new data.	Used: 120 GB Reserved: 40 GB Available: 40 GB Volume Total: 200 GB Snapshot creation is allowed.	Because the data being replaced belongs to a snapshot, it remains on the volume.
Expand the virtual disk by 40 GB.	Used: 120 GB Reserved: 80 GB Available: 0 GB Volume Total: 200 GB Snapshot creation is blocked.	The amount of reserved space increases to match the expanded size of the virtual disk. This guarantees that the entire contents of the virtual disk can be written to the volume. Because the available space has gone to 0, snapshot creation is blocked.
Delete both snapshots.	Used: 40 GB Reserved: 40 GB Available: 120 GB Volume Total: 200 GB Snapshot creation is allowed.	The 80 GB of data locked by the two snapshots disappears from the Used total when the snapshots are deleted. Because there are no more snapshots of this virtual disk, the reserved space goes to 40 GB, enough to guarantee any future write operations. Snapshot creation is once again allowed.

Action	Results	Comment
Delete the virtual disk.	Used: 0 GB Reserved: 0 GB Available: 200 GB Volume Total: 200 GB	Because no snapshots exist for this volume, deletion of the virtual disk causes the used space to go to 0 MB.

About this chapter

This chapter explains the tasks you must complete before installing the SnapDrive application software.

- ◆ Determine your SnapDrive configuration and what it requires in terms of hardware, software, settings, and background reading
- ◆ Configure your hosts
- ◆ Configure your filers
- ◆ Cable your SnapDrive configuration
- ◆ Set up your SnapDrive service account
- ◆ Verify your configuration and domain settings

Note

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

Topics in this chapter

This chapter contains the following sections:

- ◆ [“What to read”](#) on page 22
- ◆ [“Selecting a SnapDrive configuration”](#) on page 23
- ◆ [“Preparing hosts”](#) on page 34
- ◆ [“Preparing filers”](#) on page 36
- ◆ [“Preparing the SnapDrive service account”](#) on page 48

What to read

Protocol-specific reading

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

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

To create...	Read...
iSCSI-accessed virtual disks	◆ This document ◆ <i>Setup Guide for iSCSI Microsoft Windows Initiator Support Kit 1.0</i> ◆ <i>Data ONTAP Block Access Management Guide for iSCSI</i>, which shipped with your filer
FCP-accessed virtual disks	◆ This document ◆ <i>Host Bus Adapter Installation and Setup Guide 1.1 for Fibre Channel Protocol on Windows</i>, which shipped with your NetApp Windows Attach Kit ◆ <i>Data ONTAP Block Access Management Guide for FCP</i>, which shipped with your filer

Selecting a SnapDrive configuration

Factors for choosing a configuration

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

- ◆ LUN access protocol—iSCSI or FCP
- ◆ Host operating system—Windows 2000 Server (or Advanced Server for Windows cluster configurations) or Windows Server 2003 (Standard Edition or Enterprise Edition)
- ◆ Host operating system Service Pack level
 - ❖ For Windows 2000 Server: SP3 or SP4
 - ❖ For Windows Server 2003: (no Service Pack required)
- ◆ Host operating system hotfix level (various combinations of mandatory and optional hotfixes, which are determined by host operating system, Service Pack level, and special SnapDrive options. See “[Understanding feature availability](#)” on page 23.)
- ◆ Special options (Windows clustering, filer cluster failover, MPIO)

Guidelines for choosing a configuration

When selecting your SnapDrive configuration, keep the following points in mind:

- ◆ Network Appliance recommends that any filer connected to a host reside in the same broadcast domain as that host, so that virtual disk I/O commands do not need to traverse router hops.
- ◆ For Windows cluster configurations, do not permit internal cluster traffic on a GbE network used for host-filer data transfer. Instead, use a FastEthernet connection for all cluster traffic. This practice 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 pictured in the following sections, consult your NetApp Sales Engineer.

Understanding feature availability

Examine the following matrix to determine which SnapDrive features are available for supported combinations of host operating system and virtual disk access type.

Host operating system		Feature availability by virtual disk access type	
		iSCSI	FCP
Windows 2000 Server with...	SP3 + hotfixes 816990, 822831, and 815616/325040	Standard features	Standard features
	SP3 + hotfixes 816990, 815198, 822831, and 815616/325040	Standard features	Standard features, MPIO
	SP4 + hotfix 822831	Standard features	Standard features, MPIO
Windows 2000 Advanced Server with...	SP3 + hotfixes 816990, 815616/325040, and 822831	Standard features, Windows cluster	Standard features, Windows cluster
	SP3 + hotfixes 816990, 815198, 815616/325040, and 822831	Standard features, Windows cluster	Standard features, Windows cluster, MPIO
	SP4 + hotfix 822831	Standard features, Windows cluster	Standard features, Windows cluster, MPIO
Windows Server 2003, Standard Edition		Standard features	Standard features, MPIO
Windows Server 2003, Enterprise Edition	Hotfix 824354	Standard features, Windows cluster	Standard features, Windows cluster, MPIO

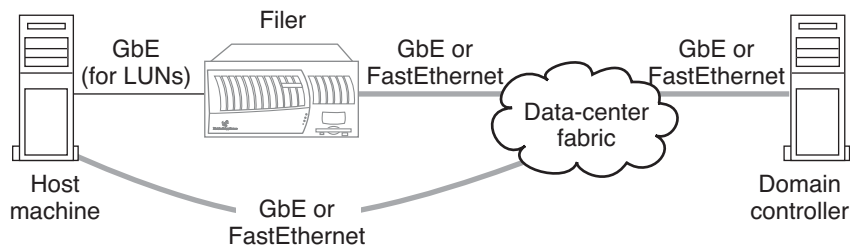
iSCSI configurations

Single host direct-attached to a single filer

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

Note

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



Windows requirements: This configuration supports the following operating system edition, service pack, and hotfix combinations:

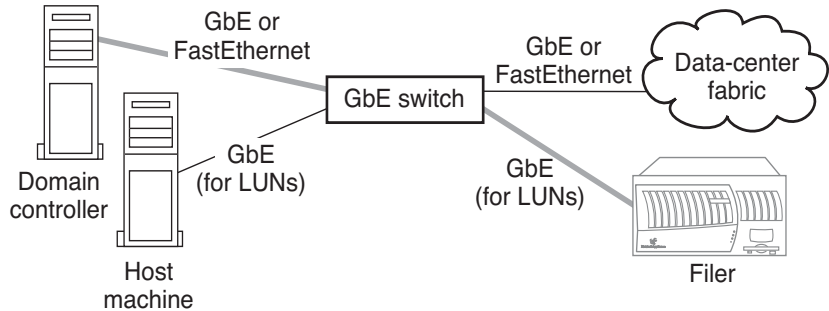
- ◆ Windows 2000 Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Server + SP4 + hotfix 822831
- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Standard Edition
- ◆ Windows Server 2003 Enterprise Edition

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

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

Single host attached to a single filer through a GbE switch

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



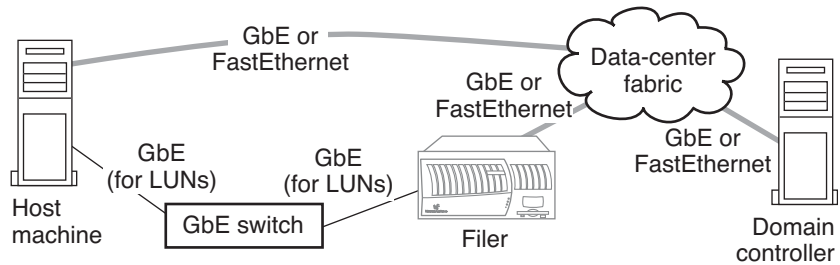
Windows requirements: This configuration supports the following operating system edition, service pack, and hotfix combinations:

- ◆ Windows 2000 Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Server + SP4 + hotfix 822831
- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Standard Edition
- ◆ Windows Server 2003 Enterprise Edition

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

Single host attached to a single filer through a dedicated switch

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



Windows requirements: This configuration supports the following operating system edition, service pack, and hotfix combinations.

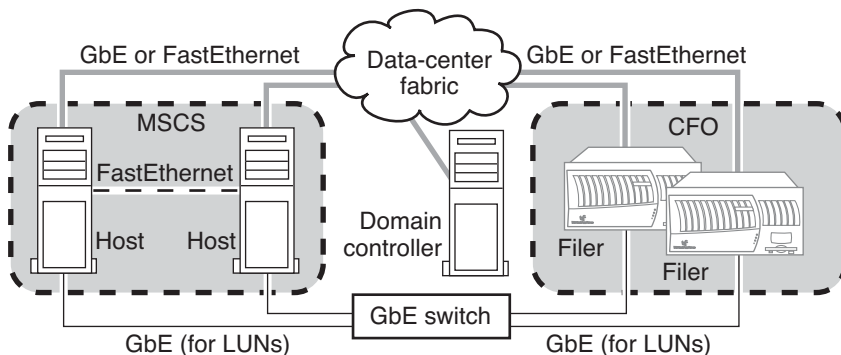
- ◆ Windows 2000 Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Server + SP4 + hotfix 822831
- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Standard Edition
- ◆ Windows Server 2003 Enterprise Edition

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

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

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

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



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

Windows requirements: This configuration supports the following operating system edition, service pack, and hotfix combinations:

- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Enterprise Edition + hotfix 824354

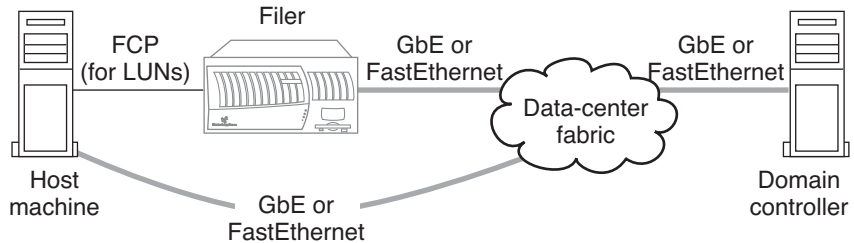
The host and filer in this configuration each use the following connection hardware:

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

FCP configurations

Single host direct-attached to a single filer

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



Caution

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

Windows requirements: This configuration supports the following operating system edition, service pack, and hotfix combinations:

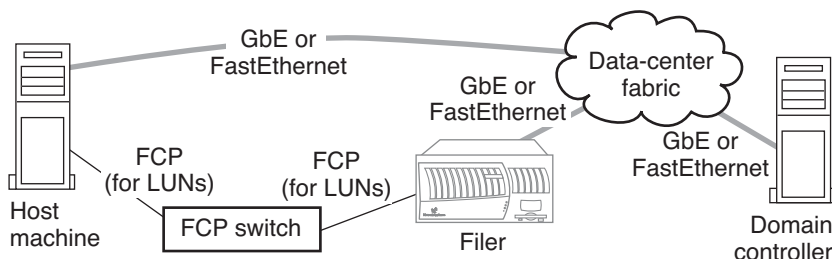
- ◆ Windows 2000 Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Server + SP4 + hotfix 822831
- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Standard Edition
- ◆ Windows Server 2003 Enterprise Edition

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

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

Single host attached to a single filer through a FCP switch

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



Windows requirements: This configuration supports the following operating system edition, service pack, and hotfix combinations:

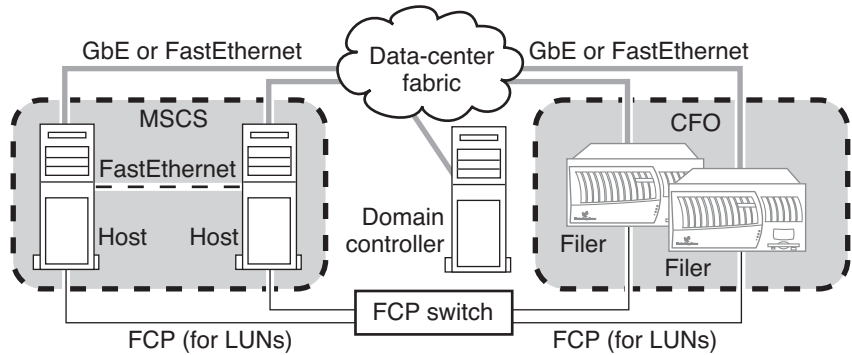
- ◆ Windows 2000 Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Server + SP4 + hotfix 822831
- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Standard Edition
- ◆ Windows Server 2003 Enterprise Edition

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

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

Windows cluster attached to a filer cluster through an FCP switch

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



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

Windows requirements: This configuration supports the following operating system edition, service pack, and hotfix combinations:

- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, and 815616/325040
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Enterprise Edition + hotfix 824354

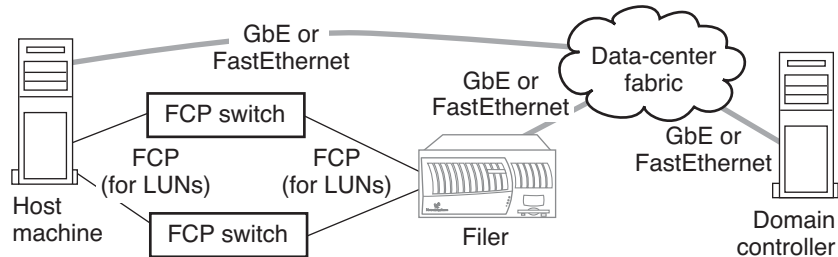
Each host in this configuration uses the following connection hardware:

- ◆ 1 HBA to transfer LUN data between filer and host
- ◆ 1 FastEthernet or GbE NIC to connect to the data-center fabric
- ◆ 1 optional Fast Ethernet NIC for internal cluster traffic

MPIO configurations

Single host direct-attached to single filer

This configuration uses dual FCP cables to support MPIO between a host and a filer. The host has two HBAs, and the filer has two FCP adapters.



Windows requirements: This configuration supports the following operating system edition, service pack, and hotfix combinations:

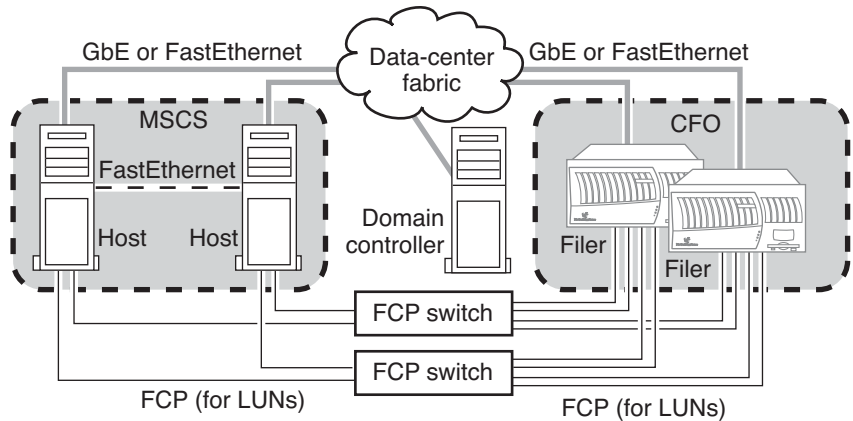
- ◆ Windows 2000 Server + SP3 + hotfixes 816990, 822831, 815616/325040, and 815198
- ◆ Windows 2000 Server + SP4 + hotfix 822831
- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, 815616/325040, and 815198
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Standard Edition
- ◆ Windows Server 2003 Enterprise Edition

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

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

Windows cluster attached to filer cluster through an FCP switch

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



Windows requirements: This configuration must use one of the following configurations:

- ◆ Windows 2000 Advanced Server + SP3 + hotfixes 816990, 822831, 815616/325040, and 815198
- ◆ Windows 2000 Advanced Server + SP4 + hotfix 822831
- ◆ Windows Server 2003 Enterprise Edition + hotfix 824354

Each host in this configuration uses the following connection hardware:

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

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

Preparing hosts

Tasks for 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 for your SnapDrive configuration.
- ◆ Install on each host the proper operating system edition, service pack, and hotfixes for your SnapDrive configuration.
- ◆ Make sure that name resolution (for example, DNS, WINS) is enabled on the Windows host such that SnapDrive can resolve a filer hostname to a reachable IP address, and an IP address to a hostname.

Verifying minimum requirements

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

Component	Requirement
CPU	500 MHz Pentium® III
Memory	256 MB RAM
HBAs	Emulex® LP9002L-F2 host bus adapters (for FCP)
Operating system	Windows 2000 Server (with SP3 or SP4) Windows 2000 Advanced Server (with SP3 or SP4) Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition (with hotfix 824354 for MSCS configurations only)

Component	Requirement
Microsoft Windows 2000 Server Post Service Pack 3 hotfixes	816990, 822831, and 815616/325040 (must be installed with SP3) 815198 (must be installed with SP3 if MPIO is deployed) 822831 (must be installed with SP4)

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

Interface drivers: Obtain the latest firmware and drivers for the HBAs and NICs you are using, to ensure high network bandwidth and ease of configuration.

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

Service Packs: You must install SP3 or SP4 before installing SnapDrive on a Windows 2000 system.

Hotfixes: You must install the following hotfixes on your hosts before you install SnapDrive. You must request these hotfixes directly from Microsoft Product Support Services at <http://support.microsoft.com>.

- ◆ If your Windows 2000 host is running SP3, you must install hotfixes 816990, 822831, and 815616/325040.
- ◆ If your Windows 2000 host is running SP4, you must install hotfix 822831.
- ◆ If your host is running MPIO on either Windows 2000 Server or Windows Advanced Server with SP3, you must install hotfixes 816990, 815616/325040, and 815198.
- ◆ If your host is running Windows Server 2003 Enterprise Edition in an MSCS configuration, you must install hotfix 824354.

Preparing filers

Conditions for filer preparation

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

- ◆ The filers are online.
- ◆ The filers are running Data ONTAP 6.4.2.
- ◆ The HBAs and NICs in your filers meet the requirements for your particular host-target SnapDrive configuration.
- ◆ The filers permit rsh access from the hosts.

Note

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

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

Verifying minimum filer requirements

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

Component	Minimum Requirement
Operating system	Data ONTAP 6.4.2
Licenses	◆ iSCSI, if you plan to use iSCSI-accessed virtual disks ◆ FCP, if you plan to use FCP-accessed virtual disks ◆ SnapRestore™ license, which is required only for restoring virtual disks from snapshots ◆ SnapMirror® license, if you plan to use the SnapMirror option

Note

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

Checking filer licences

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

Volume and filer options set by SnapDrive

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

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

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

Caution

Network Appliance *strongly recommends* that you do not change these values.

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

Option type	Parameter	SnapDrive setting	When
Volume	create_ucose	On	◆ Disk creation ◆ Disk connection
Volume	convert_ucose	On	◆ Disk creation ◆ Disk connection
Volume	nosnapdir	Off	◆ Disk creation ◆ Disk connection
Filer	Snapshot schedule	Off	◆ Disk creation ◆ Disk connection

Note

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

SnapDrive-specific limitations

SnapDrive has the following limitations:

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

Cautions and recommendations

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

- ◆ Use SnapDrive to create and manage all the virtual disks on your filer.
- ◆ *Never* disable the space reservation setting for any virtual disk managed by SnapDrive.
- ◆ Do set the snap reserve setting on the filer to 0%.

- ◆ Place all virtual disks connected to the same host on a dedicated volume accessible by just that host.
- ◆ Unless you can be sure that name resolution publishes only the filer interface you intend, configure each network interface by *IP address*, rather than by name.

Alternatively, prevent network interfaces from publishing to WINS by entering the following command at the filer prompt.

ifconfig *interfacename* -wins

interfacename is the name of the filer interface, such as e0, e4, or e4a.

- ◆ If you use snapshots, you cannot use the entire space on a filer volume to store your virtual disk.
The filer volume hosting the virtual disk should be at least twice the combined size of all the virtual disks on the volume.
- ◆ Do not create any LUNs in /vol/vol0.
This volume is used by Data ONTAP to administer the filer and should not be used to contain any LUNs.

Preparing a volume for SnapDrive

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

- ◆ Create a filer volume
- ◆ Create a qtree (only necessary if you plan to store virtual disks at a qtree root, rather than at the dedicated volume root)
- ◆ Create a CIFS share so that your host can access the volume or qtree holding the virtual disks attached to that host
- ◆ Reset the snap reserve option to 0% on the volume holding all the virtual disks attached to the host (optional, but highly recommended)

Note

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

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

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

- ◆ You can create multiple virtual disks on a filer volume

- ◆ A virtual disk must reside at either the root of a volume or the root of a qtree

Note

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

Recommendations for configuring filer volumes: You can optimize your filer volumes in the following ways:

- ◆ When multiple hosts share the same filer, each host should have its own dedicated volume on that filer to hold all the virtual disks connected to that host.
For more information about this recommendation, see “[Reasons for creating snapshots using SnapDrive](#)” on page 180.
- ◆ When multiple virtual disks exist on a filer volume, the dedicated volume on which the virtual disks reside must contain the virtual disks for just one host—and must *not* contain any other files or directories.

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

Step	Action
1	Using your Web browser, open a FilerView session to the filer where you are creating the volume. Example: Enter http://accounting-filer2/na_admin/ in the Address field of your Web browser.
2	From the main FilerView menu, navigate to Volumes > Add.
3	In the New Volume Name field, enter an easy-to-remember name for the volume. Example: Winsrvr5-Mfg indicates that the volume holds SnapDrive virtual disks connected to the host Winsrvr5 that contain data for the manufacturing department. (See your Data ONTAP documentation for specific volume-naming conventions.)
4	Complete the remaining fields on the panel, or accept the defaults, as appropriate. (See your Data ONTAP documentation for information about completing the fields.)
5	When you are satisfied with the entries in all the fields on the Add New Volume panel, click Add to execute the operation.

Step	Action
6	Create a CIFS share to the root of the volume you created in Step 5 , making sure that no other shares exist for this volume. (See “ Creating a CIFS share ” on page 43.) Network Appliance also recommends that you reset the snap reserve option for this dedicated virtual disk-storage volume to 0%. (See “ Resetting the snap reserve option ” on page 47.)

Alternatively, you can create a filer volume by completing the following procedure, which involves a Telnet session and the command prompt on the filer.

Step	Action
1	Open a Telnet session from your host to your filer by selecting Start Menu > Run, then entering the following command: <pre>telnet <i>filename</i></pre> <i>filename</i> is the name of the filer or the IP address of the filer. Examples: <pre>telnet accounting-filer2 telnet 122.48.50.52</pre>
2	At the filer prompt, create the volume by entering the following command: <pre>vol create <i>volname number</i></pre> <i>volname</i> is the name of the volume. <i>number</i> is the number of disks in the volume. Example: <pre>vol create winsrvr5-mfg 8</pre>
3	Create a CIFS share to the root of the volume you created in Step 2 , making sure that no other shares exist for this volume. (See “ Creating a CIFS share ” on page 43.) Network Appliance also recommends that you reset the snap reserve option for this dedicated virtual disk-storage volume to 0%. (See “ Resetting the snap reserve option ” on page 47.)

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

Note

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

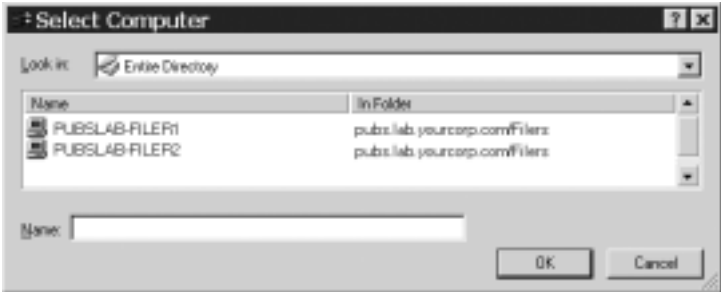
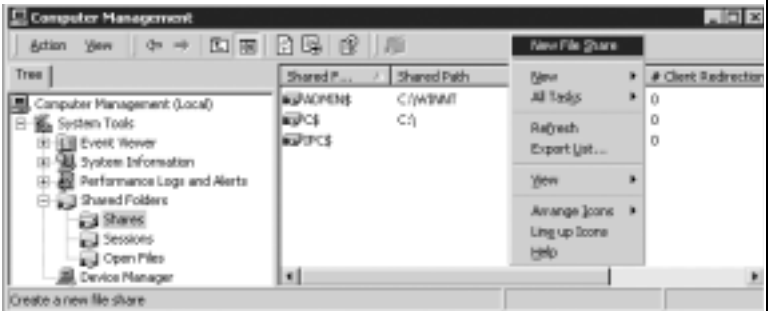
Step	Action
1	Using your Web browser, open a FilerView session to the filer where you are creating the volume. Example: Enter http://accting-filer2/na_admin/ in the Address field of your Web browser.
2	From the main FilerView menu, navigate to Volumes > Qtrees > Add.
3	In the Volume field, select the volume that will hold the qtree.
4	In the Qtree Name field, enter an easy-to-remember name for the qtree. Example: Winsrvr5-Mfg indicates that the qtree holds SnapDrive virtual disks connected to the host "Winsrvr5" that also contain data for the manufacturing department. (See your Data ONTAP documentation for specific volume-naming conventions.)
5	Complete the remaining fields on the panel, or accept the defaults, as appropriate. (Consult your Data ONTAP documentation for information on completing the fields.)
6	When you are satisfied with the entries in all the fields on the Add Qtree panel, click Add to execute the operation.

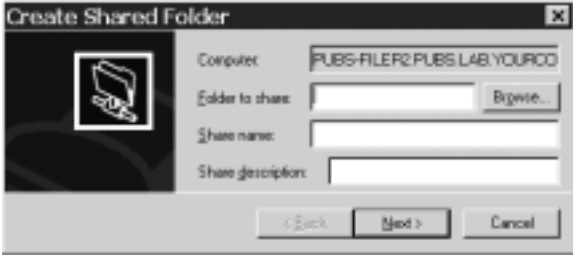
Alternatively, you can create a qtree by completing the following procedure, which involves a Telnet session and the command prompt on the filer.

Step	Action
1	Open a Telnet session from your host to your filer by selecting Start Menu > Run, then entering the following command: telnet <i>filename</i> <i>filename</i> is the name of the filer or the IP address of the filer. Examples: <pre>telnet accounting-filer2</pre> <pre>telnet 122.48.50.52</pre>
2	At the filer prompt, enter the following command: qtree create <i>path</i> <i>path</i> is the path name of the qtree. If you want to create the qtree on a volume other than the root volume, include the volume name between the root volume and the qtree name. Example: <pre>qtree create /vol/corphq/accounting</pre> <i>vol</i> indicates the root volume. <i>corphq</i> indicates the volume name. <i>accounting</i> indicates the qtree name.

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

Step	Action
1	Make sure CIFS is enabled and configured (through the <code>cifs setup</code> command) on the filer. For SnapDrive to operate properly, the filer's CIFS (NetBIOS) name must exactly match the filer listed (UNIX host name). For more information about running CIFS setup, see your Data ONTAP <i>File Access Management Guide</i>.

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

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

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

As an alternative to the preceding Windows-initiated procedure, you can use the Web-based FilerView utility to create a CIFS share for a filer volume or qtree, as detailed in the following procedure table.

Step	Action
1	Using your Web browser, open a FilerView session to the filer containing the volume or qtree for which you are creating the CIFS share. Example: Enter <code>http://accounting-filer2/na_admin/</code> in the Address field of your Web browser.
2	From the main FilerView menu, navigate to CIFS > Shares > Add.
3	In the Share Name field, enter an easy-to-remember name for the share. Example: Use the volume or qtree name as the name of your new share, such as <code>WinSrvr5-Mfg</code>.

Step	Action
4	In the Mount Point field, enter the path to the share. Example: /vol/corpha/accounting/
5	Complete the remaining fields on the panel, or accept the defaults, as appropriate. (Consult your Data ONTAP documentation for information about completing the fields.)
6	When you are satisfied with the entries in all the fields on the Add a CIFS Share panel, click Add to execute the operation.

Resetting the snap reserve option: By default, the snap reserve option for Data ONTAP 6.4.2 is 20%. Network Appliance strongly recommends that you reset the snap reserve option to 0% on all volumes holding SnapDrive virtual disks. To reset the snap reserve option, complete the following steps.

Step	Action
1	Open a FilerView session to the filer holding the volume whose snap reserve setting is to be changed.
2	From the main FilerView menu, navigate to Volumes > Snapshots > Configure.
3	In the Volume field, select the volume whose snap reserve setting is to be changed
4	In the space reservation field, enter “0.”
5	Click Apply at the bottom of the panel.

Preparing the SnapDrive service account

Reason to prepare the service account

Before installing SnapDrive, you must establish a SnapDrive service account. You must log in to this account whenever you need to perform SnapDrive-related functions on either a host or a filer.

Types of access to establish

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

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

Note

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

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

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

Next, add the service account to the Administrators group. (One way to do this is by clicking My Computer, right-clicking Manage on the drop-down menu, then navigating to System Tools > Local Users and Groups > Groups > Administrators.)

- ◆ The service account must have rsh (remote shell access) to the filer.

SnapDrive requires this type of access for certain operations. You enable rsh access by editing two files on the filer; see “[Enabling rsh access](#)” on page 49.

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

You enable such access by creating a share on the filer for each volume or qtree you want the host to access. This can only be done after you create the volumes or qtrees. The procedure is covered in the section “[Creating a CIFS share](#)” on page 43.

Enabling rsh access

If you can access your filer from your host through the rsh command, you do not have to perform the tasks described in this section. However, if your SnapDrive service account cannot access your filer by running rsh, you must enable rsh by editing the /etc/hosts and /etc/hosts.equiv files, which are on the filer.

Note

As an alternative to the steps described in the following sections, you can use FilerView to modify the /etc/hosts and /etc/hosts.equiv files.

- ◆ Edit the /etc/hosts file
- ◆ Edit the /etc/hosts.equiv file
- ◆ Test remote operation

File functions: The functions supported by the /etc/hosts and /etc/hosts.equiv files appear in the following table.

Note

The entries in these files are case-sensitive.

File	Function
/etc/hosts	Provides a local mapping of host names to IP addresses.
/etc/hosts.equiv	Lists all the Windows users capable of sending rsh commands to the filer.

Editing the /etc/hosts file: To edit the etc/hosts file, complete the following steps.

Step	Action
1	Using a text editor such as WordPad, open the /etc/hosts file on the filer.
2	Add the following line to the file: <i>ip_address hostname</i> <i>ip_address</i> is the IP address of the host. <i>hostname</i> is the name of the host. Use spaces or tabs to separate the items. Note_____ The /etc/hosts file entry for the host name must match the corresponding entry for the host name in the /etc/hosts.equiv file. _____
3	Save and close the file.

Example: In the following edited /etc/hosts file, the line 122.28.50.42 WinSrvr2 was added to map the IP address 122.28.50.42 to the host named WinSrvr2:

122.28.50.41 WinSrvr1

122.28.50.42 WinSrvr2

122.28.50.43 WinSrvr3

122.28.50.44 WinSrvr4

Editing the /etc/hosts.equiv file: To edit the etc/hosts.equiv file so that the filer responds to administrator commands, complete the following steps.

Step	Action
1	Using a text editor such as Wordpad, open the /etc/hosts.equiv file on the filer.

Step	Action
2	Add the following lines to the file: <pre>hostname Username hostname username</pre> <i>hostname</i> is the name of the host. It must match the entry for the host name in the /etc/hosts file. <i>Username</i> (with an initial capital), or <i>username</i> (all lowercase), is the name of the owner of the account on the host. Note _____ Entering the name of the account in both uppercase and lowercase prevents case-sensitivity oversights by users during login.
3	Save and close the file.
4	Verify that you edited this file properly by testing the remote command ability, as discussed in “ Verifying remote command ability ” on page 51.

Example: In the following edited /etc/hosts.equiv file, the host named WinSrvr1 is mapped to the filer and the SnapDrive service account for the host:

```
WinSrvr1 administrator
WinSrvr1 Administrator
WinSrvr1 domainname\administrator
WinSrvr1 domainname\Administrator
```

Verifying remote command ability

To test whether the filer accepts commands from the host, complete the following steps.

Step	Action
1	Log into the host using the SnapDrive service account.

Step	Action	
2	Open a Telnet session to the filer. 	
3	Open a Windows command prompt window and enter the following command: rsh filename version <i>filename</i> is the name of your filer. Result: The filer returns the Data ONTAP version it is currently running. 	
4	If the filer...	Then...
	Returned a version number (as pictured in the preceding illustration)	The /etc/hosts and /etc/hosts.equiv files are set up correctly. You do not need to edit the files.
	Returned an error message	The /etc/hosts and /etc/hosts.equiv files are not set up correctly; continue to Step 5 .

Step	Action	
5	View any error messages in the Telnet window you opened in Step 2 .	
	If...	Then...
	You see an IP address in the error message	You must edit the /etc/hosts file. See “ Editing the /etc/hosts file ” on page 50.
	You see an account name in the error message	You must edit the /etc/host.equiv file. See “ Editing the /etc/hosts.equiv file ” on page 50.
	You see both an IP address and an account name in the error message	You must edit both the /etc/hosts and the /etc/hosts.equiv files.

About this chapter

This chapter explains the procedures you must follow to install or upgrade to SnapDrive 3.0.

Procedures in this chapter

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 directions under “[Upgrading to SnapDrive 3.0](#)” on page 56.
- ◆ If no version of SnapDrive is installed, follow instructions under “[Installing SnapDrive for the first time](#)” on page 100.

Upgrading to SnapDrive 3.0

- When to use this section

Use this section if a previous version of SnapDrive is installed on your system.
- Which releases you can upgrade to 3.0

You can upgrade to SnapDrive 3.0 from SnapDrive 2.1 or 2.0.1. If you are running an earlier release (or the VLD Manager application) you must first upgrade to 2.0.1 or 2.1, then upgrade to 3.0.

You can confirm what version of SnapDrive your system is running by selecting SnapDrive in the Microsoft Management Console (MMC), pulling down the Action menu, and selecting SnapDrive Info.
- If you are using VLD-type virtual disks

VLD-type virtual disks cannot be restored using SnapDrive 3.0. If you are using VLDs, upgrade from 2.0.1 or 2.1 using the upgrade-and-conversion process described in [“Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks”](#) on page 60 or [“Upgrading a single system to SnapDrive 3.0 and converting VLD-type virtual disks”](#) on page 65. If the conversion process fails, you can reinstall a previous version of SnapDrive to restore the VLD-type virtual disk from snapshot.
- Which procedure to follow

How you upgrade to SnapDrive 3.0 depends on what components of SnapDrive you are currently using, and on your Windows configuration.

To upgrade...	Follow procedures under...
A single system with VLD-type virtual disks connected	“Upgrading a single system to SnapDrive 3.0 and converting VLD-type virtual disks” on page 65
A single system with only LUN-type virtual disks connected	“Upgrading a single system to SnapDrive 3.0 if you have no VLD-type virtual disks” on page 99

To upgrade...	Follow procedures under...
A Microsoft Windows server cluster with VLD-type virtual disks connected	“Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks” on page 60
A Microsoft Windows server cluster with only LUN-type virtual disks connected	“Upgrading a server cluster to SnapDrive 3.0 if you have no VLD-type virtual disks” on page 96
A single system or server cluster to SnapDrive 3.0 and Microsoft Server 2003 Edition	“Upgrading to SnapDrive 3.0 and Microsoft Windows Server 2003” on page 58

Upgrading to SnapDrive 3.0 and Microsoft Windows Server 2003

When to use this section

Use this section if you intend to upgrade a single Windows system or server cluster to SnapDrive 3.0 and Windows Server 2003.

Caution

If you are running Microsoft Exchange 2000 and SnapManager for Exchange 2000, DO NOT upgrade your Windows server or server cluster to Windows Server 2003 now. Neither Exchange 2000 nor SnapManager for Exchange 2000 version 1.1 runs on Windows Server 2003.

Note

If you plan to configure a Majority Node Set (MNS) cluster under Windows Server 2003, do not upgrade from Windows 2000 Server. You will need to do a fresh install of Windows Server 2003, then install SnapDrive 3.0.

Upgrade process

Follow this process to upgrade a Windows 2000 Server system or server cluster to SnapDrive 3.0 and Windows Server 2003.

Note

Perform these actions in the order given.

Stage	Process
1	Upgrade to SnapDrive 3.0. Choose one of the following options. ◆ To upgrade a single system that has VLD-type virtual disks, see “Upgrading a single system to SnapDrive 3.0 and converting VLD-type virtual disks” on page 65. ◆ To upgrade a single system that has only LUN-type virtual disks, see “Upgrading a single system to SnapDrive 3.0 if you have no VLD-type virtual disks” on page 99. ◆ To upgrade a server cluster with VLD-type virtual disks connected, see “Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks” on page 60. ◆ To upgrade a server cluster with only LUN-type virtual disks connected, see “Upgrading a server cluster to SnapDrive 3.0 if you have no VLD-type virtual disks” on page 96.
2	Uninstall the VLD driver. See “Uninstalling old components” on page 113.
3	Upgrade to Windows Server 2003 Standard Edition or (for a server cluster) Windows Server 2003 Enterprise Edition, using Microsoft documentation.

Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks

When to use this section

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

Upgrade and conversion process

Follow this process to upgrade a server cluster with VLD-type virtual disks.

Stage	Process
1	Plan and announce downtime. You will need to take offline the cluster groups that have VLD-type virtual disks as physical disk resources, thus stopping resources in that group that require the disk resource (see “Converting VLDs in a cluster group” on page 92). Note————— Taking the cluster groups offline shuts down the applications that use them. To ensure a graceful shutdown of an application, make sure you take offline all the cluster groups that the application uses. For example, if a Microsoft Exchange installation consists of two Exchange virtual servers in two cluster groups, you will need to take both cluster groups offline. You will also need to shut down the cluster nodes themselves if you have not yet upgraded your NetApp filer (see “Upgrading the filer” on page 112) or if the cluster needs to be upgraded to the required service pack and hotfix level (see “Selecting a SnapDrive configuration” on page 23). Pick a time for the upgrade when loss of access will have the least effect on your users.
2	When the time you have set arrives, make sure that no users are using the system and no SnapDrive operations are running.

Stage	Process
3	Check that the cluster is functioning properly. Make sure that the Cluster Groups are online and that you can do a “move group” back and forth between nodes.
4	Prepare your cluster for the upgrade and VLD conversion. See “Preparing for the upgrade and VLD conversion” on page 63.
5	If necessary, upgrade Data ONTAP on the filer. If an upgrade is necessary, you will have to reboot the filer and then the cluster nodes. See “Upgrading the filer” on page 112.
6	Install the components you need for FCP or iSCSI (see “Selecting a SnapDrive configuration” on page 23 for supported configurations). Choose one of the following options: ◆ If you will be creating and managing LUNs using the iSCSI protocol, download and install the Microsoft iSCSI Software Initiator 1.0 on both nodes. ❖ For download instructions, see the iSCSI Microsoft Windows Initiator Support Kit 1.0 Description Page on the NOW site (http://now.netapp.com). ❖ For detailed installation instructions, see “Installing the iSCSI Software Initiator” on page 102. ◆ If you will be creating and managing LUNs using the FCP protocol, install or upgrade the FCP components on both nodes. See the <i>Host Bus Adapter Installation and Setup Guide 1.1 for Fibre Channel Protocol on Windows</i>. This document is on the NOW site (http://now.netapp.com).

Stage	Process
7	Install SnapDrive 3.0 on both nodes, starting with the node that does not own the SnapDrive resources. See “Installing the new SnapDrive components” on page 104. The upgrade could require a reboot on both nodes, depending on whether new versions of underlying drivers need to be installed. Note— If you try to use the MMC after upgrading SnapDrive on the first node and before upgrading SnapDrive on the second node, you will get an error message indicating that the SnapDrive service is unavailable owing to an invalid tag. This message 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. Note— You will see messages warning you to convert VLD-type virtual disks. This is expected behavior at this point, because you have not yet done the conversion.
8	Convert the cluster’s VLD-type virtual disks. See “ Converting VLD-type virtual disks for MSCS ” on page 89.
9	Using the information you collected earlier (see “ Preparing for the upgrade and VLD conversion ” on page 63), verify that all converted virtual disks still have the same drive letter as they did before the upgrade.
10	When all the VLD-type virtual disks are converted to LUNs, make sure that the cluster is functional by doing several “move group” operations back and forth for each cluster group.
11	Remove the VLD driver. See “ Uninstalling old components ” on page 113.
12	Back up your application data. If you use SnapManager, use SnapManager rather than SnapDrive to create the backup.

Stage	Process
13	When all the VLD-type virtual disks are converted to LUNs, and you are satisfied that everything is working correctly, remove the VLD driver. See “Uninstalling old components” on page 113.

Preparing for the upgrade and VLD conversion

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

Step	Action
1	For each VLD-type virtual disk in your installation, record the drive letter and UNC path to the virtual disk object on the filer. Use the SnapDrive MMC snap-in to get this information. Recording this information helps you ensure that no drive letters are changed by the conversion, so that all scripts and applications function correctly after the conversion.
2	If you use SnapManager, make sure that you have an up-to-date and valid SnapManager backup, and that no SnapManager backups are scheduled to occur while you are upgrading. If backups are scheduled, cancel those scheduled jobs.
3	If necessary, upgrade the operating systems on the cluster nodes to the required service pack and hotfix level. See “Preparing hosts” on page 34. If you need to apply a new service pack or hotfix, you will have to reboot the cluster.
4	Network Appliance strongly recommends that you create a system backup and an Emergency Repair Disk for each node before upgrading to SnapDrive 3.0.

Step	Action
5	Using your current version of SnapDrive, take a snapshot of all VLD-type virtual disks. This creates a backup that can be restored by your current version of SnapDrive, in case the upgrade does not complete for any reason. Note— Taking a snapshot of a virtual disk creates a single, consistent snapshot of all the virtual disks that share this filer volume and are connected to this Windows host. (You can check this by clicking each virtual disk in turn in the left frame of the MMC window; the same snapshot shows up for each virtual disk that shares the filer volume.)

Upgrading a single system to SnapDrive 3.0 and converting VLD-type virtual disks

Upgrade overview

Because VLD-type virtual disks are no longer supported in SnapDrive 3.0, the upgrade to SnapDrive 3.0 includes extra steps if you are currently using VLD-type virtual disks. Network Appliance recommends that you read over the upgrade process that follows before you start the upgrade, to familiarize yourself with the requirements and upgrade steps.

Note

For more information about the VLD-to-LUN conversion, see “[VLD-to-LUN conversion](#)” on page 73.

SnapDrive 3.0 upgrade and conversion process

Upgrade process

To upgrade to SnapDrive 3.0 when your Windows host has VLD-type virtual disks connected, complete the following steps.

Step	Action
Prepare your system for the upgrade and VLD conversion	
1	For each VLD-type virtual disk in your installation, record the drive letter and the UNC path to the virtual disk object on the filer. Use the SnapDrive MMC snap-in to get this information. Recording this information helps you ensure that no drive letters are changed by the conversion, so that all scripts and applications function correctly after the conversion.
2	Bearing in mind that you will need to stop any application(s) that access VLD-type virtual disks, pick a time for the upgrade when loss of access to the virtual disks will have the least effect on your users.
3	If you use SnapManager, make sure that you have a valid SnapManager backup, and that no SnapManager backups are scheduled to occur while you are upgrading. If backups are scheduled, cancel those scheduler jobs.
4	Network Appliance strongly recommends that you create a system backup and an Emergency Repair Disk before upgrading to SnapDrive 3.0.

Step	Action	
5	If your applications access VLD-type virtual disks, determine the correct application-specific instructions to use to stop your applications. If the VLD-type virtual disks are accessed by more than one application, make sure you follow the instructions for all applicable applications.	
	If you have VLD-type virtual disks that store data used by...	Then...
	Microsoft Exchange	Follow the instructions in “Stopping Microsoft Exchange services for VLD conversion” on page 70.
	Microsoft SQL Server	Follow the instructions in “Stopping Microsoft SQL Server services for VLD conversion” on page 70.
	Domino	Follow the instructions in “Stopping Domino services for VLD conversion” on page 71.
	SnapManager remote verification servers	Make sure that the verification server will not be doing a verification during the conversion process. Check for scheduled commands and processes both on the verification server and on the production server. (Remote verification is performed as an option during backups that are scheduled and executed on the production server.)
	All other applications	Follow the instructions “Stopping all other applications for VLD conversion” on page 71.

Step	Action
6	Using your current version of SnapDrive, take a snapshot of all VLD-type virtual disks. This creates a backup that your current version of SnapDrive can restore, in case the upgrade does not complete for any reason. Note Taking a snapshot of a virtual disk creates a single, consistent snapshot of all the virtual disks that share this filer volume and are connected to this Windows host. (You can check this by clicking each virtual disk in turn in the left frame of the MMC window; the same snapshot shows up for each virtual disk that shares the filer volume.)
7	Install the components you need for FCP or iSCSI (see “Selecting a SnapDrive configuration” on page 23 for supported configurations). Choose one of the following options: ◆ If you will be creating and managing LUNs using the iSCSI protocol, download and install the Microsoft iSCSI Software Initiator on both nodes. ❖ For download instructions, see the iSCSI Microsoft Windows Initiator Support Kit 1.0 Description Page on the NOW site (http://now.netapp.com). ❖ For detailed installation instructions, see “Installing the iSCSI Software Initiator” on page 102. ◆ If you will be creating and managing LUNs using the FCP protocol, install or upgrade the FCP components. See the <i>Host Bus Adapter Installation and Setup Guide 1.1 for Fibre Channel Protocol on Windows</i>. This document is on the NOW site (http://now.netapp.com).

Step	Action
Upgrade SnapDrive and convert your VLDs	
8	Upgrade to SnapDrive 3.0. See “Installing the new SnapDrive components” on page 104. Note— You will see messages warning you to convert VLD-type virtual disks. This is expected behavior at this point, since you have not yet done the conversion.
9	Create a small test LUN of about 100 MB and connect to it before attempting the conversion. Repeat this step for every filer containing VLDs. Caution— If this step is unsuccessful, and you continue with the upgrade, you will not be able to access any of your converted LUNs. Do not proceed until you have found and fixed the problem,
10	Convert your VLD-type virtual disks to LUNs. See “VLD-to-LUN conversion” on page 73.
Validate upgrade and return system to production	
11	Using the information you collected in Step 1 , verify that all converted virtual disks still have the same drive letter as they did before the upgrade.
12	If you do not use SnapManager, use SnapDrive to take snapshots of all virtual disks. This creates a backup that SnapDrive 3.0 can restore.
13	If you stopped any applications, restart those applications.
14	If you use Microsoft Exchange, Microsoft SQL Server, or Lotus Domino, verify that all the application databases are mounted correctly after the application is restarted.
15	If you use SnapManager, create a valid SnapManager backup.

Step	Action
16	When all the VLD-type virtual disks are converted to LUNs, and you are satisfied that everything is working correctly, remove the VLD driver. See “Uninstalling old components” on page 113.

Stopping Microsoft Exchange services for VLD conversion

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

Note

This procedure is for single systems, not MSCS clusters. See [“Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks”](#) on page 60.

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

Stopping Microsoft SQL Server services for VLD conversion

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

Note

This procedure is for single systems, not MSCS clusters. See [“Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks”](#) on page 60.

Step	Action
1	Close the SnapManager application, if it is open.

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

Stopping Domino services for VLD conversion

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

Note

This procedure is for single systems, not MSCS clusters. See “[Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks](#)” on page 60.

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

Stopping all other applications for VLD conversion

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

Note

This procedure is for single systems, not MSCS clusters. See “[Upgrading a server cluster to SnapDrive 3.0 and converting VLD-type virtual disks](#)” on page 60.

Step	Action
1	Close the SnapManager application if it is open.

Step	Action
2	Stop all instances of any application that is accessing the VLD-type virtual disks to be converted.

VLD-to-LUN conversion

About this section

This section contains the following procedures:

- ◆ [“Converting a connected VLD-type virtual disk”](#) on page 73
- ◆ [“Converting an unconnected VLD-type virtual disk”](#) on page 81
- ◆ [“Converting VLD-type virtual disks for MSCS”](#) on page 89
- ◆ [“Converting VLDs in a cluster group”](#) on page 92
- ◆ [“Converting a VLD-type quorum disk”](#) on page 93

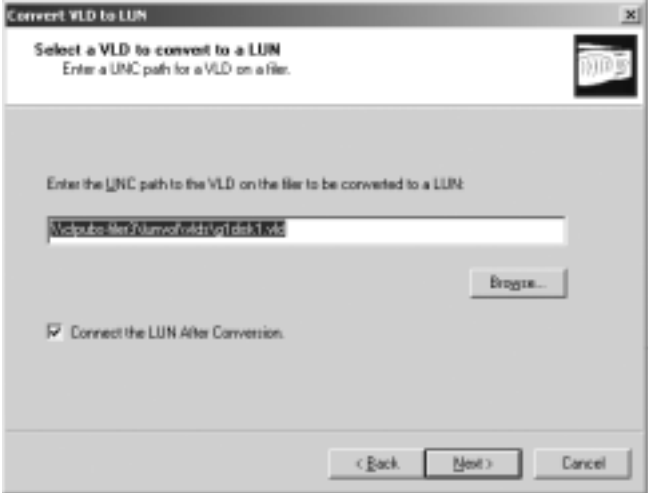
VLD conversion requirement

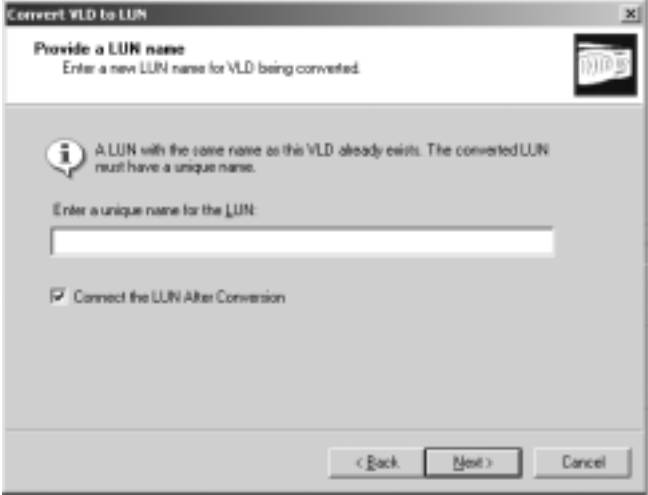
VLD-type virtual disks are not supported in SnapDrive 3.0. To manage the data on your VLD-type virtual disks, you must convert all VLD-type virtual disks to LUNs. SnapDrive 3.0 provides a Virtual Disk Conversion Wizard to assist you with this process.

Converting a connected VLD-type virtual disk

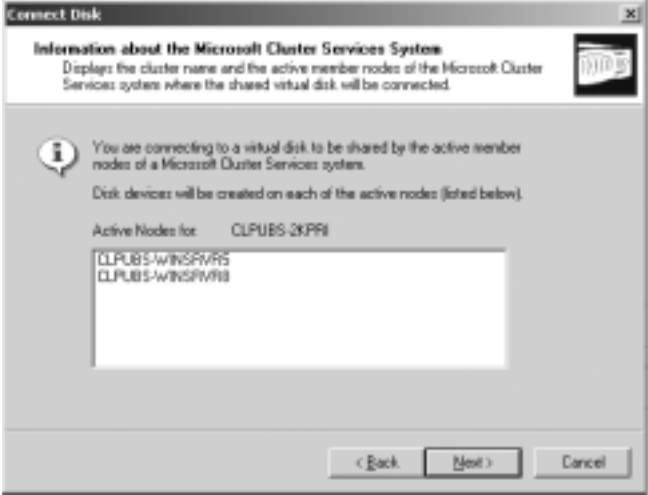
To convert a connected VLD-type virtual disk to a LUN, complete the following steps.

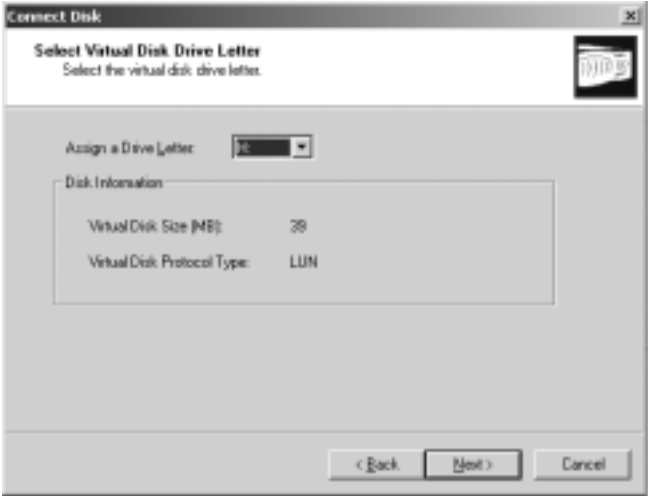
Step	Action
1	Make sure that your environment is prepared for the conversion and that no applications are accessing the VLD-type virtual disk to be converted. For more information, see “Upgrade and conversion process” on page 60. Note_____ The VLD-type virtual disk to be converted is disconnected during the conversion procedure. If applications are accessing the virtual disk when the disconnect happens, the conversion will fail. _____
2	Select Start > Programs > Administrative Tools > Computer Management to open the Computer Management window.
3	In the Computer Management window, select Storage > SnapDrive > Disks, and then select the VLD-type virtual disk you want to convert.
4	Right-click and select Convert VLD to LUN.

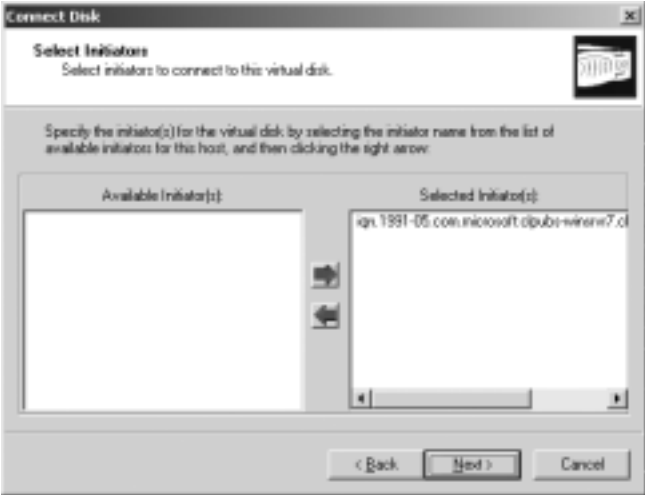
Step	Action
5	After the VLD-to-LUN Conversion Wizard appears, click Next. Result: The Select a VLD to Convert to a LUN panel is displayed, with the UNC path to the VLD-type virtual disk you selected already filled in. The converted LUN will have the same name as the VLD-type virtual disk you are converting.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

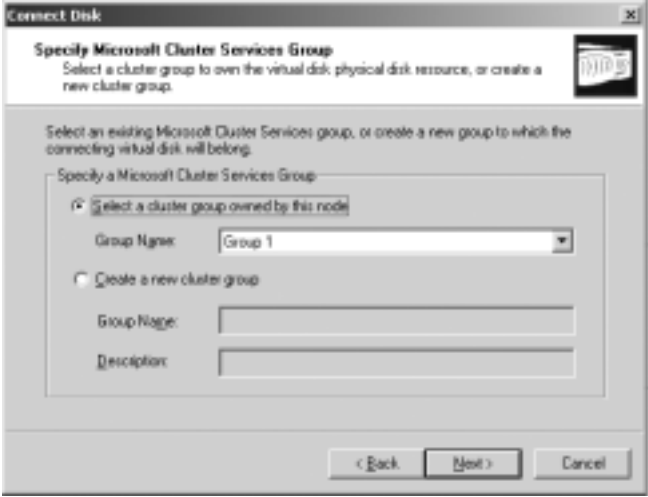
Step	Action
7	If a LUN-type virtual disk exists with the same name as the VLD-type virtual disk you are converting, a panel is displayed prompting you to specify a different name for the converted disk. 
8	If you did not leave the Connect the LUN After Conversion check box selected, skip to Step 14.

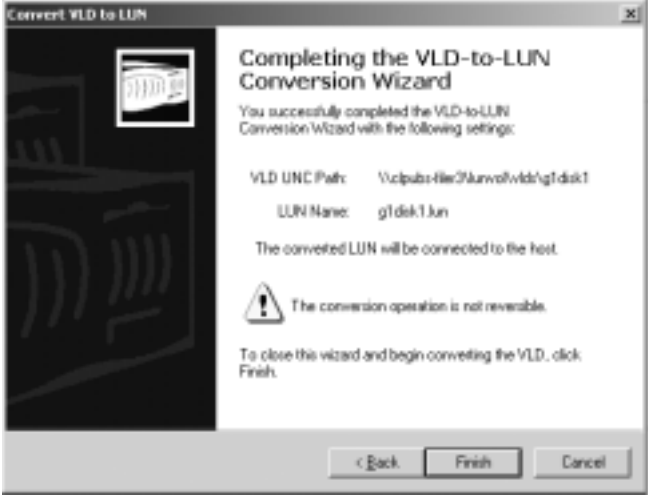
Step	Action	
9	In the Select a Virtual Disk Type panel, verify that the preselected virtual disk type is correct for your configuration.	
	If...	Then...
	The VLD-type virtual disk being converted will be connected to a single-host system	Select Dedicated, click Next, and then skip to Step 11 .
	The VLD-type virtual disk being converted is an MSCS cluster resource	Select Shared, and click Next.
		

Step	Action
10	In the Information about Microsoft Cluster Services System panel, verify that you want the disk to be shared by the nodes listed, and then click Next.  The screenshot shows a 'Connect Disk' dialog box. At the top, it says 'Information about the Microsoft Cluster Services System' and 'Displays the cluster name and the active member nodes of the Microsoft Cluster Services system where the shared virtual disk will be connected.' Below this, an information icon states: 'You are connecting to a virtual disk to be shared by the active member nodes of a Microsoft Cluster Services system. Disk devices will be created on each of the active nodes (listed below).' The 'Active Nodes for:' field shows 'CLPUBS-2KPR8'. A list box contains two entries: 'CLPUBS-WINSPVRS' and 'CLPUBS-WINSPVRS'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a mouse cursor.

Step	Action
11	In the Select Virtual Disk Drive Letter panel, make sure that the drive letter for the converted LUN is the same as the drive letter previously used by the VLD-type virtual disk being converted, and then click Next. 

Step	Action
12	Select the desired initiator, click the right arrow, and then click Next.  Note _____ If you are using MSCS or MPIO, you must select an initiator for each path to the filer. _____

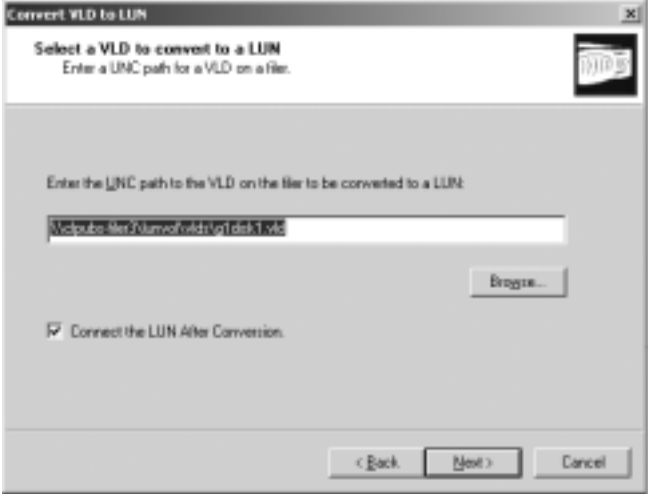
Step	Action
13	If you are connecting the converted LUN to an MSCS cluster, the following screen is displayed. Verify that the disk will be connected to the correct cluster group. If you want to create a new cluster group and add the converted LUN to the new group, select Create a New Cluster Group. However, that results in a different cluster configuration than you had before the conversion. 

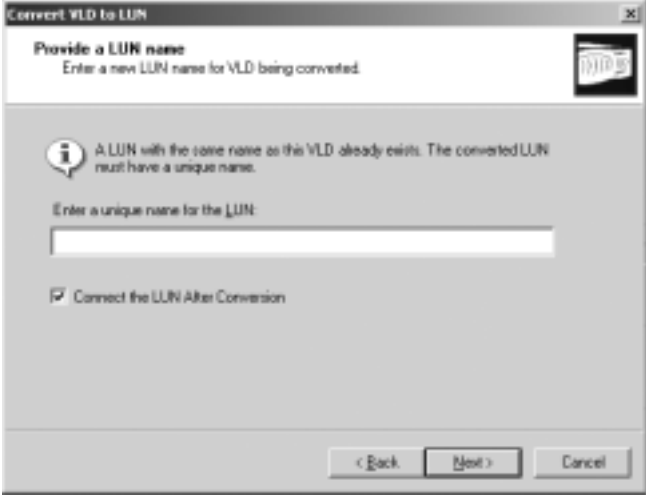
Step	Action
14	In the Completing the VLD-to-LUN Conversion Wizard panel, check the settings you selected for your new LUN, and then click Finish to start the conversion. 

Converting an unconnected VLD-type virtual disk

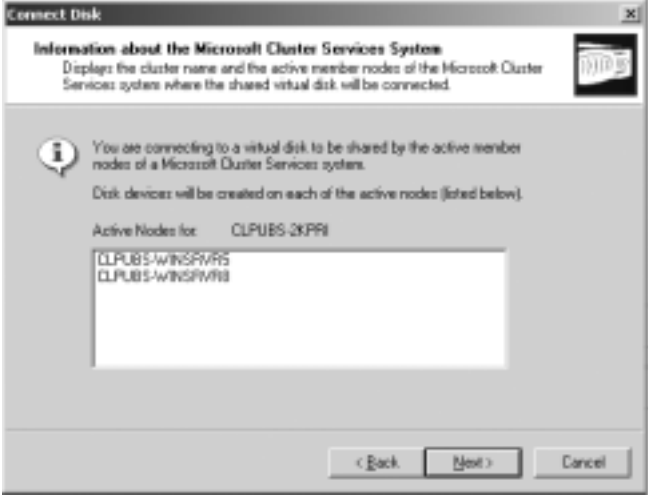
To convert an unconnected VLD-type virtual disk to a LUN, complete the following steps.

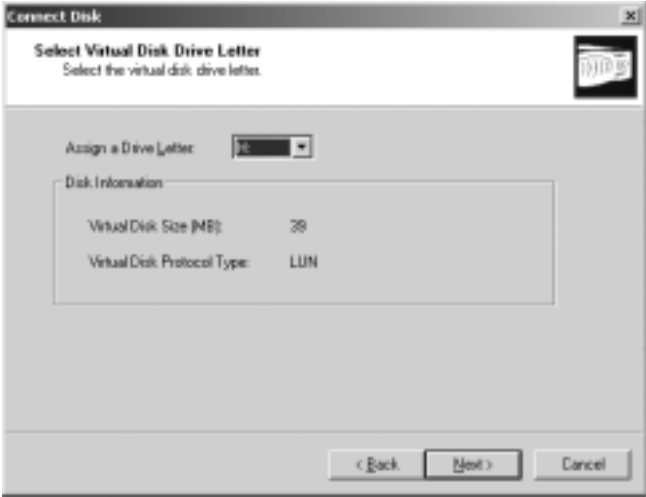
Step	Action
1	Make sure that your environment is prepared for the conversion.
2	Select Start > Programs > Administrative Tools > Computer Management to open the Computer Management window.
3	In the Computer Management window, select Storage > SnapDrive > Disks.
4	Right-click and select Convert VLD to LUN.
5	After the VLD-to-LUN Conversion Wizard appears, click Next. Result: The Select a VLD to Convert to a LUN panel is displayed.

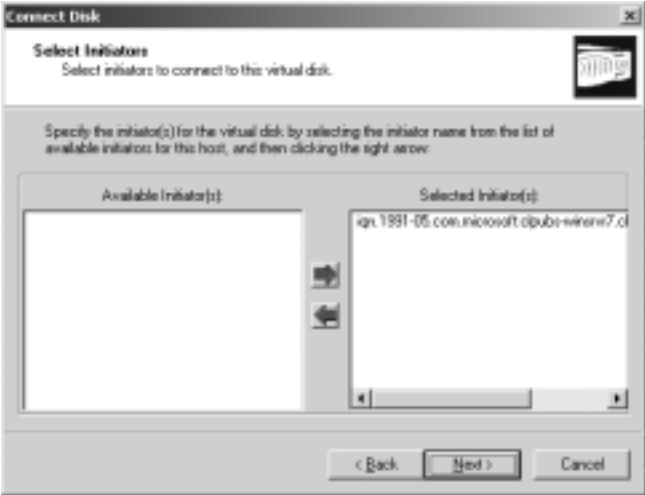
Step	Action
6	Enter the UNC path or browse to the VLD-type virtual disk you want to convert. The converted LUN will have the same name as the VLD-type virtual disk you are converting. Example: \\clpubs-filer3\lunvol\vlds\g1disk1.vld becomes a LUN named g1disk1.lun. 
7	To automatically connect the LUN after it is converted, select the Connect the LUN After Conversion check box. Click Next.

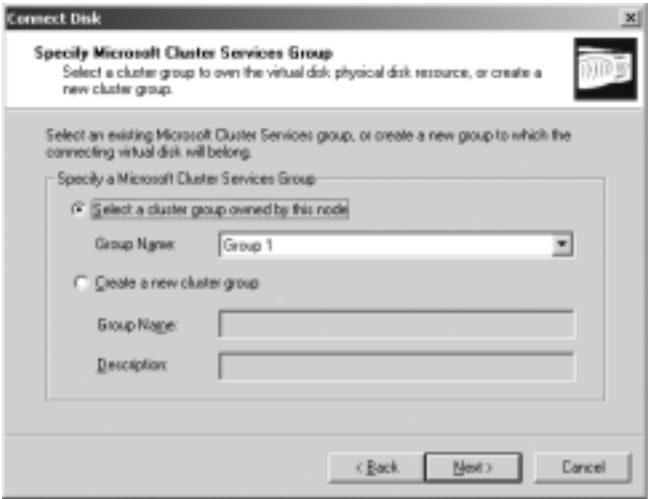
Step	Action
8	If a LUN-type virtual disk exists with the same name as the VLD-type virtual disk you are converting, a panel is displayed prompting you to specify a different name for the converted disk. 
9	If you did not select the Connect the LUN After Conversion check box, skip to Step 15.

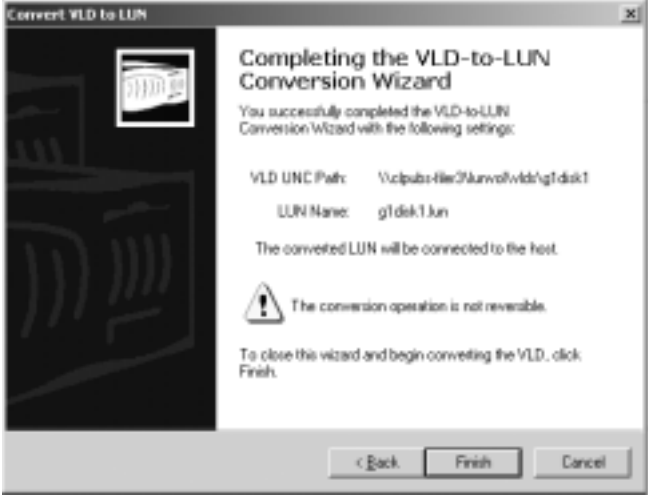
Step	Action	
10	In the Select a Virtual Disk Type panel, verify that the preselected virtual disk type is correct for your configuration.	
	If...	Then...
	The VLD-type virtual disk being converted will be connected to a single-host system	Select Dedicated, click Next, and then skip to Step 12 .
	The VLD-type virtual disk being converted is an MSCS cluster resource	Select Shared, and click Next.
		

Step	Action
11	In the Information about Microsoft Cluster Services System panel, verify that you want the disk to be shared by the nodes listed, and then click Next.  The screenshot shows a 'Connect Disk' dialog box. At the top, it says 'Information about the Microsoft Cluster Services System' and 'Displays the cluster name and the active member nodes of the Microsoft Cluster Services system where the shared virtual disk will be connected.' Below this, an information icon states: 'You are connecting to a virtual disk to be shared by the active member nodes of a Microsoft Cluster Services system. Disk devices will be created on each of the active nodes (listed below).' The 'Active Nodes for:' field shows 'CLPUBS-2KPR8'. A list box contains two entries: 'CLPUBS-WINSPVRS' and 'CLPUBS-WINSPVRS'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted.

Step	Action
12	In the Select Virtual Disk Drive Letter panel, select the same drive letter for the converted LUN as the drive letter previously used by the VLD-type virtual disk being converted, and then click Next. 

Step	Action
13	Select the desired initiator, click the right arrow, and then click Next.  Note _____ If you are using MSCS or MPIO, you must select an initiator for each path to the filer. _____

Step	Action
14	If you are connecting the converted LUN to an MSCS cluster, the following screen is displayed. Select the cluster group that you want the newly converted LUN to be connected to. If you want to create a new cluster group and add the converted LUN to the new group, select Create a New Cluster Group. 

Step	Action
15	In the Completing the VLD-to-LUN Conversion Wizard panel, check the settings you selected for your new LUN, and then click Finish to start the conversion. 

Converting VLD-type virtual disks for MSCS

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

Note

The following procedure assumes extensive knowledge of MSCS administration.

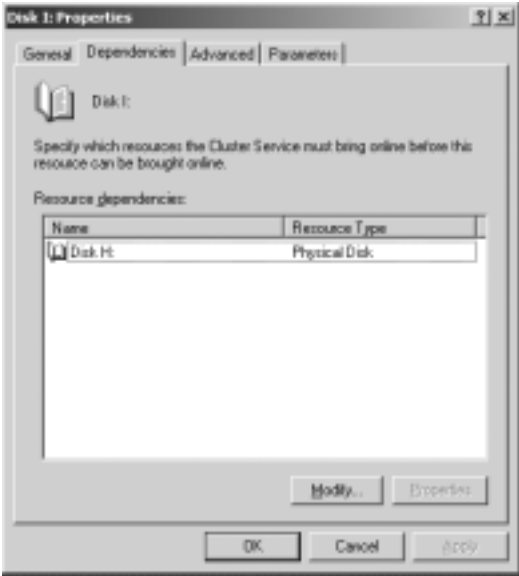
Step	Action
Prepare the cluster for conversion	
1	Determine the order in which you will convert your cluster groups. Each group should be completely converted before you move on to the next group. The main cluster group (the group that contains the quorum disk) should be converted last.

Step	Action
2	Create a new shared LUN for temporary use during the conversion. The size of this LUN should be at least 200 MB. Place the temporary LUN in the first cluster group to be converted. This temporary LUN will be used to shift resource dependencies and as a quorum disk while the current quorum disk is being converted. For more information, see “Creating a virtual disk” on page 131.
3	If you have only one cluster group, skip to Step 6 .
Convert cluster groups that do not contain the quorum disk	
4	For each cluster group other than the one that contains the quorum disk, if the group contains VLD-type virtual disks, perform the following steps: - Open Cluster Administrator on the node that owns the cluster group. - Right-click the cluster group and select Take Offline. - Right-click each physical disk resource in the cluster group and select Bring Online. - Using SnapDrive, create a snapshot of every VLD-type virtual disk in the cluster group. Name the snapshots using the name of the cluster group and the drive letter. For more information on creating snapshots, see “Creating snapshots” on page 180. - Right-click the cluster group and select Take Offline again to bring all of the disks back offline. - Convert each VLD-type virtual disk in the cluster group. See “Converting VLDs in a cluster group” on page 92.
Convert the main cluster group	
5	Open Cluster Administrator on the node that owns the main cluster group.

Step	Action
6	If your quorum disk is a VLD-type virtual disk, convert it to a LUN. See “Converting a VLD-type quorum disk” on page 93.
7	Using SnapDrive, create a snapshot of every VLD-type virtual disk in the main cluster group. Name the snapshots using the name of the main cluster group and the drive letter. For more information on creating snapshots, see “Creating snapshots” on page 180.
8	For each remaining VLD-type virtual disk in the main cluster group, right-click the resource in Cluster Administrator and select Take Offline.
9	Convert any remaining VLD-type virtual disks in the main cluster group. See “Converting VLDs in a cluster group” on page 92.
Delete the temporary LUN	
10	On the node that currently owns the cluster group containing the temporary LUN, open the Computer Management window and select SnapDrive > Disks.
11	Select the temporary LUN, right-click, and select Delete Disk to delete the temporary LUN. Note _____ After deleting the temporary LUN, you may see an Unsafe Removal of Device notification on the other node. This is not a problem; click OK to dismiss the dialog box. _____

Converting VLDs in a cluster group

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

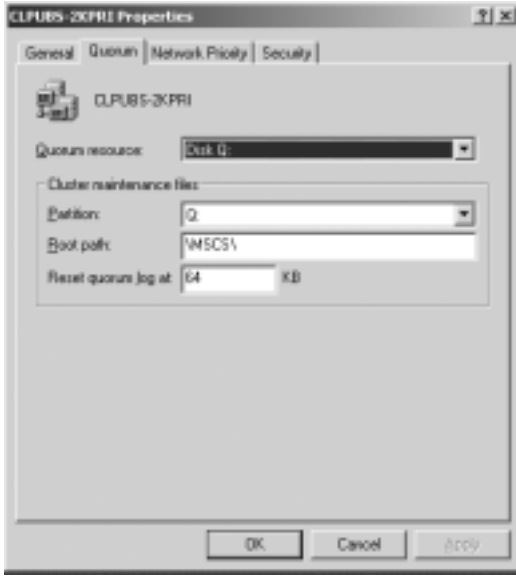
Step	Action
1	For each resource in this cluster group, record all dependencies and remove any dependencies on VLD-type virtual disks. a. Right-click the resource and select Properties. b. Select the Dependencies tab. c. Record all dependencies for the resource. d. If the resource has a dependency on any VLD-type virtual disk, remove the dependency. e. If you cannot remove the last dependency, move the dependency to the temporary LUN. Some services, for example Microsoft Exchange System Attendant, do not allow all physical disk dependencies to be removed. 

Step	Action
2	After all dependencies on the VLD-type virtual disks are removed, convert every VLD-type virtual disk in this cluster group to a LUN-type virtual disk. For more information, see “Converting a connected VLD-type virtual disk” on page 73.
3	Using Cluster Administrator, reestablish the original dependencies on the newly converted LUNs, and remove any dependencies you placed on the temporary LUN.
4	Drag and drop the temporary LUN into the next cluster group to be converted.
5	Right-click the cluster group that you just converted and select Bring Online.
6	Verify the status of your cluster by performing a move group back and forth. a. Right-click the cluster group that contains the quorum and select Move Group. b. After the cluster group comes back online after the move group, repeat the move group to return the cluster group to its original owning node.
7	After all dependencies on the VLD-type virtual disks are removed, convert every VLD-type virtual disk in this cluster group to a LUN-type virtual disk. For more information, see “Converting a connected VLD-type virtual disk” on page 73.

Converting a VLD-type quorum disk

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

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

Step	Action
1	In Cluster Administrator, right-click the top-level cluster name and select Properties.
2	In the Properties dialog box, select the Quorum tab. Result: 
3	Select the temporary LUN from the list of available drives, and then click OK. Result: The temporary LUN is now the quorum disk.
4	Convert the original (VLD-type virtual disk) quorum disk to a LUN-type virtual disk. See “Converting a connected VLD-type virtual disk” on page 73.
5	Reopen the cluster Properties dialog box. This time, select the newly converted LUN to be the quorum disk. Result: The quorum disk is the same drive letter as it was before, but now it is a LUN-type virtual disk.

Step	Action
6	Verify the status of your cluster by performing a move group back and forth. a. Right-click the cluster group that contains the quorum and select Move Group. b. After the cluster group comes back online after the move group, repeat the move group to return the cluster group to its original owning node.

Upgrading a server cluster to SnapDrive 3.0 if you have no VLD-type virtual disks

When to use this section

Use this section only if your Microsoft server cluster is currently running an earlier version of SnapDrive and you are not using VLD-type virtual disks.

Upgrade process

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

Stage	Process
1	Plan and announce downtime. You will need to shut down the cluster nodes if you have not yet upgraded your NetApp filer (see “Upgrading the filer” on page 112) or if the cluster needs to be upgraded to the service pack and hotfix level required by SnapDrive 3.0 (see “Selecting a SnapDrive configuration” on page 23). Pick a time for the upgrade when loss of access will have the least effect on your users.
2	When the time you have set arrives, make sure no users are using the system and no SnapDrive operations are running.
3	Check that the cluster is functioning properly. Make sure that the Cluster Groups are online and that you can do a “move group” back and forth between nodes.
4	Prepare your cluster for the upgrade. See “Preparing for the upgrade” on page 98.
5	If necessary, upgrade Data ONTAP on the filer. If an upgrade is necessary, you will have to reboot filer, then the cluster nodes. See “Upgrading the filer” on page 112.

Stage	Process
6	Install the components you need for FCP or iSCSI (see “Selecting a SnapDrive configuration” on page 23 for supported configurations). Choose one of the following options. ◆ If you will be creating and managing LUNs using the iSCSI protocol, download and install the Microsoft iSCSI Software Initiator version 1.0 on both nodes. ❖ For download instructions, see the iSCSI Microsoft® Windows® Initiator Support Kit 1.0 Description Page on the NOW site (http://now.netapp.com). ❖ For detailed installation instructions, see “Installing the iSCSI Software Initiator” on page 102. ◆ If you will be creating and managing LUNs using the FCP protocol, install or upgrade the FCP components on both nodes. See the <i>Host Bus Adapter Installation and Setup Guide 1.1 for Fibre Channel Protocol on Windows</i>. This document is on the NOW site (http://now.netapp.com).
7	Install SnapDrive 3.0 on both nodes, starting with the node that does not own the SnapDrive resources. See “Installing the new SnapDrive components” on page 104. The upgrade could require a reboot on both nodes, depending on whether new versions of underlying drivers need to be installed. Note If you try to use the MMC after upgrading SnapDrive on the first node and before upgrading SnapDrive on the second node, you will get an error message indicating that the SnapDrive service is unavailable owing to an invalid tag. This message 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.
8	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 113.

Stage	Process
9	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 those scheduled jobs.
2	If necessary, upgrade the operating systems on the cluster nodes to the required service pack and hotfix level. See “Preparing hosts” on page 34. If you need to apply a new service pack or hotfix, you will have to reboot the cluster.
3	Network Appliance strongly recommends that you create a full backup, including system state, and create an Emergency Repair Disk for each node before upgrading to SnapDrive 3.0.

Upgrading a single system to SnapDrive 3.0 if you have no VLD-type virtual disks

When to use this section

Use this section only if you are currently running an earlier version of SnapDrive and you are not using VLD-type virtual disks.

Upgrade process

To upgrade a system without VLD-type virtual disks to SnapDrive 3.0, you need to do the following.

Stage	Process
1	Install the required version of the iSCSI Software Initiator or FCP driver. See “Installing the FCP or iSCSI components” on page 101.
2	Network Appliance strongly recommends that you create a full backup, including system state, and create an Emergency Repair Disk before upgrading to SnapDrive 3.0.
3	Install SnapDrive 3.0. See “Installing the new SnapDrive components” on page 104.
4	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 113.

Installing SnapDrive for the first time

When to use this section Use this section to install SnapDrive 3.0 if no previous version of SnapDrive or VLD Manager is installed on your system.

Installation process To install SnapDrive 3.0, you need to do the following in the order given.

Stage	Process
1	Install the required version of the iSCSI Software Initiator or the FCP components. See “ Installing the FCP or iSCSI components ” on page 101.
2	Install SnapDrive 3.0. See “ Installing the new SnapDrive components ” on page 104. In a server cluster, install SnapDrive on all nodes.

Installing the FCP or iSCSI components

Supported protocols

SnapDrive 3.0 supports two protocols for creating and managing virtual disks (LUNs): iSCSI and FCP.

Note

You can use only one connection protocol from any one host.

What you need to do

Before you install SnapDrive 3.0, you need to do one of the following:

If...	Then...
You will be using the iSCSI protocol to create and manage LUNs	Install the Microsoft iSCSI Software Initiator. See “ Installing the iSCSI Software Initiator ” on page 102.
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>Host Bus Adapter Installation and Setup Guide 1.1 for Fibre Channel Protocol on Windows</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>Host Bus Adapter Installation and Setup Guide 1.1 for Fibre Channel Protocol on Windows</i>. This document is on the NOW site (http://now.netapp.com).

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. See the iSCSI Microsoft Windows Initiator Support Kit 1.0 Description Page on the NOW site (http://now.netapp.com) for instructions.
2	Click the Microsoft iSCSI Initiator Installer Package icon.
3	Click Next on the Welcome to the Microsoft iSCSI Initiator Setup Wizard screen.
4	Read the end-user license agreement, select I agree, and click Next.
5	On the Confirm Installation screen, click Next.
6	Choose a folder to install the Microsoft iSCSI Initiator into, and then click Next. Result: The Installing Microsoft iSCSI Initiator screen shows a progress bar.
7	Accept the option to Install Complete iSCSI Initiator by clicking OK in the pop-up window.
8	Select I agree on the license agreement.
9	On the Microsoft iSCSI Initiator Information screen, click Next.
10	On the Installation Complete screen, click Close.

Step	Action
11	Configure the iSCSI Initiator following the instructions in the iSCSI Microsoft Windows Initiator Support Kit 1.0.

Installing the new SnapDrive components

Installing the components

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

Note—————
In a cluster, install SnapDrive 3.0 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.

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

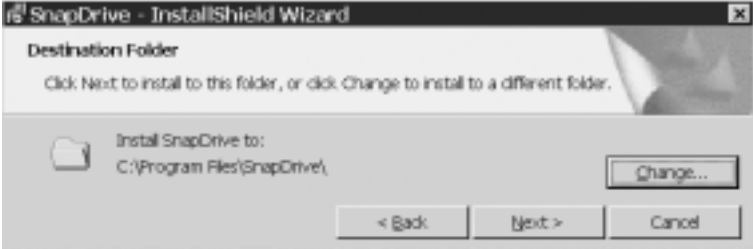
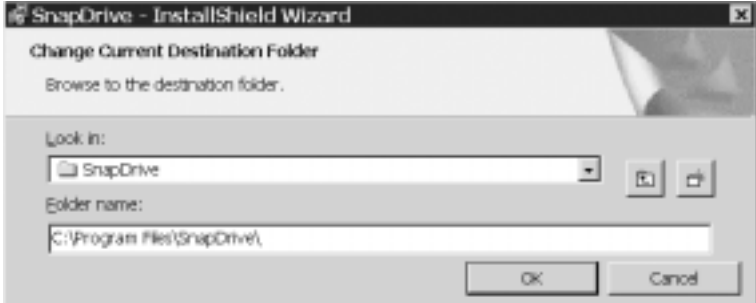
Step	Action
1	Make sure that you have installed the required FCP or iSCSI components. See “Installing the FCP or iSCSI components” on page 101. Note————— If you will be using the iSCSI initiator, you may see a message during the SnapDrive installation that SnapDrive will modify the maxrequestholdtime parameter. This message does not indicate an error
2	Make sure that the Microsoft Management Console (MMC) window is not open.
3	Browse to the location of the SnapDrive installation package and double-click SnapDrive3.0.exe.
4	Click Next on the “Welcome to the InstallShield Wizard for SnapDrive” screen.
5	If this is a new SnapDrive installation, accept the license agreement and click Next.

Step	Action
6	If you are upgrading SnapDrive, the Program Maintenance panel appears. Click Modify/Upgrade, and then click Next. 

Step	Action	
7	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 101), and then restart the SnapDrive InstallShield Wizard.
		

Step	Action	
8	On the SnapDrive Driver Installation screen, select Update MPIO drivers or Install MPIO drivers, if the FCP driver is installed and you want to install or upgrade the MPIO drivers, and then click Next. 	
9	If you selected Update MPIO drivers, two dialog boxes prompt you for permission to overwrite a newer file with an older one. These prompts are the result of a change in Microsoft's numbering scheme for these drivers and do not indicate a problem. Click Yes in both dialog boxes.	
10	If...	Then...
	If you are upgrading from SnapDrive 2.0.1 or later	Skip to Step 14 .
	If this is a new SnapDrive installation	Continue with the next step.

Step	Action
11	In the Customer Information screen, type your user name and organization name, and then click Next. 

Step	Action
12	The Destination Folder screen prompts you for a directory in which to install SnapDrive on the host. By default, this is C:\Program Files\SnapDrive. To accept the default, click Next, and then proceed to Step 13.  To specify a different location, click the Change button. In the Change Current Destination Folder screen, 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 screen, and then click Next. 

Step	Action
13	On the SnapDrive Service Credentials screen, click Browse and select Administrator from the drop-down list.  Type the account password in both the Password and Confirm Password text boxes, then click Next.
14	In the “Ready to...” screen, click Install. Result: The Installing SnapDrive screen appears, informing you that installation might take several minutes to complete. Note If you are upgrading from SnapDrive 2.1 and you have VLD-type virtual disks, a message warns you to convert the VLDs to LUNs. See “VLD-to-LUN conversion” on page 73.
15	When the InstallShield Wizard Complete screen appears, click Finish.
16	If you are installing or upgrading the MPIO drivers, the SnapDrive Installer Information pop-up screen appears. Click Yes to reboot the machine.

Step	Action
17	When the reboot process is complete, SnapDrive is successfully installed on your host. Note_____ If you are upgrading a server cluster and you try to use the MMC after upgrading SnapDrive on the first node and before upgrading SnapDrive on the second node, you get an error message indicating that the SnapDrive service is unavailable owing to an invalid tag. This message is the result of the temporary presence of two versions of SnapDrive on the same cluster. No corrective action is needed; just upgrade SnapDrive on the other node.
18	If you will be creating and managing LUNs using the iSCSI protocol, establish an iSCSI connection to the filer. See “Establishing an iSCSI connection to a target” on page 121.

Installing SnapDrive on SnapManager verification servers

If you are upgrading or installing SnapDrive to support a SnapManager installation, and you use verification servers, remember to install SnapDrive 3.0 on the verification servers as well as on the production systems.

If a verification server will be connecting to LUNs over an iSCSI connection, make sure you also install the Microsoft iSCSI Software Initiator on the verification server (see “[Installing the iSCSI Software Initiator](#)” on page 102) and establish a connection from the verification server to the iSCSI target on the filer where the database to be verified resides. This connection enables the verification server to connect to the snapshot LUN that contains the database, and you must create it explicitly before the verification server attempts to connect to the LUN.

For instructions for establishing an iSCSI connection, see “[Establishing an iSCSI connection to a target](#)” on page 121.

Note_____

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

Upgrading the filer

Upgrading the filer SnapDrive 3.0 requires Data ONTAP 6.4.2 on the filer. To upgrade the filer, complete the following steps.

Step	Action
1	Shut down the Windows server. In a server cluster, shut down both cluster nodes.
2	Upgrade the filer to Data ONTAP 6.4.2. See the Data ONTAP 6.4.2 <i>Upgrade Guide</i> for details.
3	When the filer upgrade is complete, bring the Windows system back up. In a server cluster, bring the cluster nodes back up one at a time.

Uninstalling old components

Uninstalling the VLD driver

After you have converted all VLD-type virtual disks to LUNs (see [“VLD-to-LUN conversion”](#) on page 73) and have taken 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, and remove the VLD driver if necessary, complete the following steps.

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

Uninstalling SnapDrive and MPIO drivers

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

- ◆ Uninstall SnapDrive 2.1 (rather than upgrade to 3.0)
- ◆ Uninstall SnapDrive 3.0
- ◆ Uninstall the MPIO drivers

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

Note

Do not attempt to uninstall the MPIO drivers through the Device Manager; you must use the SnapDrive InstallShield wizard to remove the MPIO drivers.

Uninstalling SnapDrive 2.0.1: If, for some reason, you want to uninstall SnapDrive 2.0.1 (rather than upgrade to 3.0), complete the following steps.

Step	Action	
1	If...	Then
	You want to uninstall a fresh (first-time) installation of SnapDrive 2.0.1	Skip to Step 7 .
	You want to uninstall an installation of SnapDrive 2.0.1 resulting from an upgrade from SnapDrive 2.0	Go to Step 2
2	Open a Windows command prompt by navigating to Start Menu > Run, typing cmd in the “Open:” field, then clicking OK.	
3	If the volume containing the SnapDrive installation package is not already mapped to a drive letter on your host, create that mapping. Select My Computer > Map Network Drive, select an available drive letter from the drop-down menu in the Drive field, type (or browse to) the UNC location where the installation package is located, select the “Reconnect at logon” check box, and then click Finish.	
4	Set the command prompt to the drive containing the installation package from which you originally installed SnapDrive 2.0.1. Example: G:	

Step	Action
5	Enter the following command at the prompt: cd <i>path</i> <i>path</i> is the fully qualified path to the setup package from which you originally installed SnapDrive 2.0.1. Example: \SD2.0.1\download\install
6	Enter the following command: wizardname /v "REINSTALLMODE=vomus REINSTALL=ALL" <i>wizardname</i> is one of the following: ◆ SnapDrive2.0.1.exe, if you downloaded the installation package for your most recent SnapDrive installation. ◆ Setup.exe, if you most recently installed SnapDrive from a CD-ROM. REINSTALLMODE=vomus re-caches the installation packages on the local system so you can use Add/Remove Programs to remove it (see next step).
7	Navigate to Start Menu > Settings > Control Panel > Add/Remove Programs, and then double-click the SnapDrive icon.
8	Click Remove to launch the SnapDrive Uninstall process.
9	Follow the prompts to uninstall SnapDrive 2.0.1.

Uninstalling the FCP driver

To remove the FCP driver if necessary, 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: right-click My Computer, then choose Properties > Hardware > Device Manager.
3	Open SCSI and RAID Controllers.

Step	Action
4	Select the entry for the Fibre Channel HBA, pull down the Action menu and select Uninstall, and then click OK in the dialog box to confirm that you want to uninstall the FCP driver.
5	Remove the HBA (the physical card) from the system.

Uninstalling or upgrading the iSCSI Software Initiator

To remove or upgrade the Microsoft iSCSI Software Initiator if necessary, complete the following steps.

Step	Action
1	If you are uninstalling the iSCSI Software Initiator, make sure that no virtual disks are connected to your Windows host by means of the iSCSI protocol.
2	Close the SnapDrive snap-in in the MMC.
3	Stop the SnapDrive Service.
4	Navigate to the folder containing the Microsoft iSCSI installation package.
5	Launch the InstallShield wizard, select Repair Microsoft iSCSI Initiator or Remove Microsoft iSCSI Initiator, and then click Finish.
6	Restart the SnapDrive service.

Reminder: SnapManager verification servers

If you are upgrading or installing SnapDrive to support a SnapManager installation, and you use verification servers, remember to install SnapDrive 3.0 on the verification servers as well as on the production systems.

If a verification server will be connecting to LUNs over an iSCSI connection, make sure you also install the Microsoft iSCSI Software Initiator on the verification server (see [“Installing the iSCSI Software Initiator”](#) on page 102) and establish a connection from the verification server to the iSCSI target on the filer where the database to be verified resides. This connection enables the

verification server to connect to the snapshot LUN that contains the database, and you must create it explicitly before the verification server attempts to connect to the LUN.

Note

For this purpose, create only an iSCSI connection; do not create a new LUN as well.

For information on establishing an iSCSI connection, see “[Establishing an iSCSI connection to a target](#)” on page 121.

About this chapter This chapter explains how to manage iSCSI connections that you use to access virtual disks on the targets (filers).

Topics in this chapter This chapter covers the following topics:

- ◆ [“Tasks for managing iSCSI connections”](#) on page 120
- ◆ [“Establishing an iSCSI connection to a target”](#) on page 121
- ◆ [“Disconnecting an iSCSI target from a Windows host”](#) on page 125
- ◆ [“Examining details of iSCSI connections”](#) on page 126

Tasks for managing iSCSI connections

Ways to establish iSCSI connections

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

- ◆ Establish iSCSI connections prior to creating virtual disks
For detailed information, see “[Establishing an iSCSI connection to a target](#)” on page 121.
- ◆ Establish iSCSI connections during the creation of a virtual disk
If an iSCSI connection does not exist to a target on which you create a virtual disk, SnapDrive collects the pertinent information about the connection from you when you step through the Create Disk Wizard and establishes the connection.
For detailed information, see .

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 125.
- ◆ Examine details about iSCSI connections
For detailed information, see “[Examining details of iSCSI connections](#)” on page 126.

Establishing an iSCSI connection to a target

About establishing an iSCSI connection

You need to have an iSCSI connection to a target on which you create a virtual disk. You establish this connection prior to creating a virtual disk, as explained in the procedure in this section.

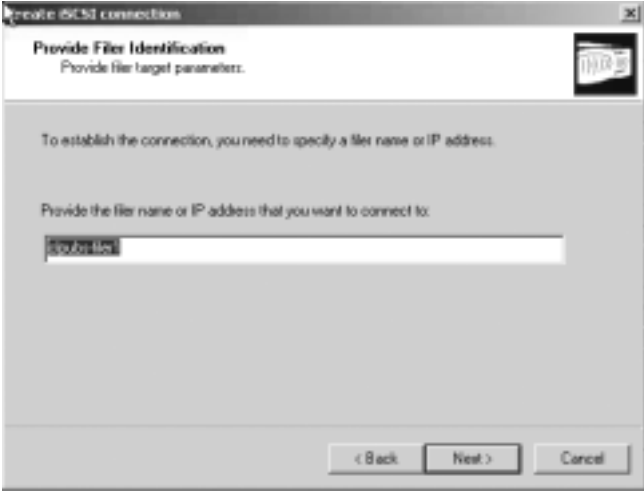
Note

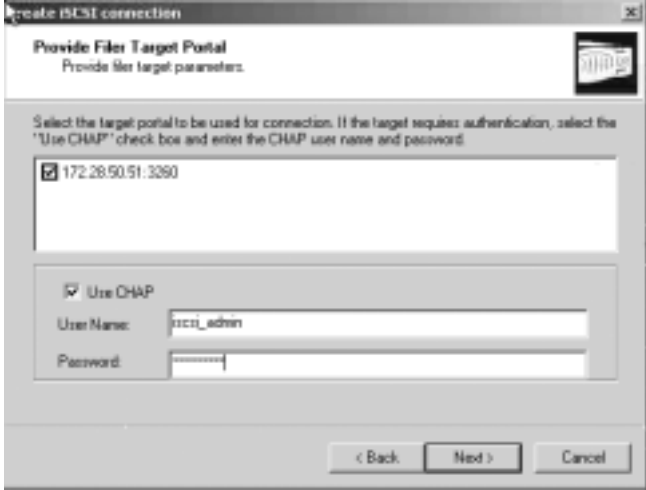
If you do not establish an iSCSI connection to a target prior to creating a virtual disk on it, SnapDrive prompts you for information it needs to establish the connection during the course of virtual disk creation. After you supply the information, the iSCSI connection is established during the virtual disk creation process. For detailed information, see “[Creating a virtual disk](#)” on page 131.

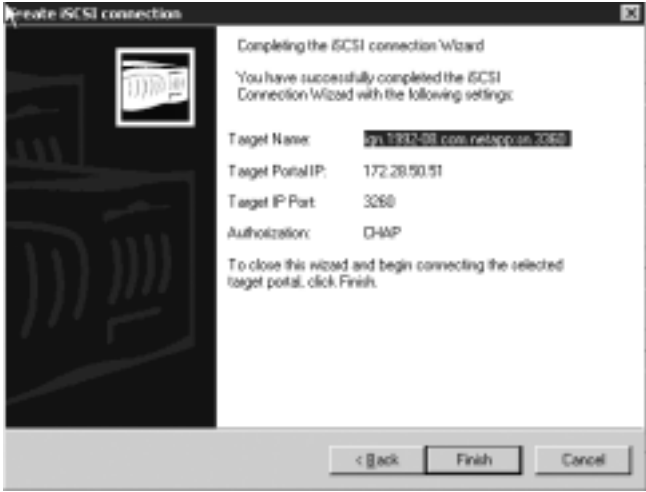
Establishing an iSCSI connection to a target

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

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	Perform the following actions to launch the Create iSCSI Connection 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 Connections. d. Click Action (from the menu choices on top of the MMC). e. Select Establish New Connection from the drop-down menu.
3	In the Create iSCSI Connection wizard, click Next. Result: The Provide Filer Identification panel is displayed.

Step	Action
4	In the Provide Filer Identification panel, enter the NetBIOS name or IP address of the target (filer) you want to establish the iSCSI connection with, and then click Next.  Result: The Provide Filer Target Portal panel is displayed.

Step	Action
5	In the Provide File Target Portal panel, perform the following actions:  - Select the target portal to which SnapDrive will establish the iSCSI connection. - 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. - Click Next. Result: The Completing the iSCSI Connection Wizard panel is displayed.

Step	Action
6	In the Completing the iSCSI Connection Wizard, perform the following actions:  - Review the information to make sure it is accurate. - If the information is not accurate, use Back to go back to previous panels of the wizard to modify information. - Click Finish. Result: An iSCSI connection to the target is established.

Disconnecting an iSCSI target from a Windows host

Disconnecting an iSCSI target from a Windows host

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

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	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 Connections. d. Select the iSCSI connection 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 disconnected.
3	Click Yes. Result: The selected iSCSI connection is disconnected from the Windows host.

Examining details of iSCSI connections

Details you can examine

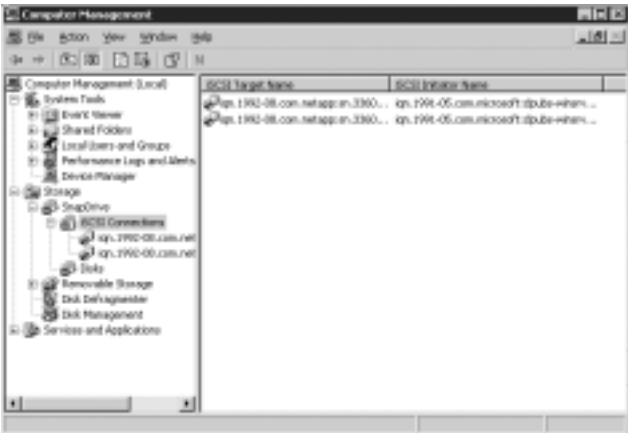
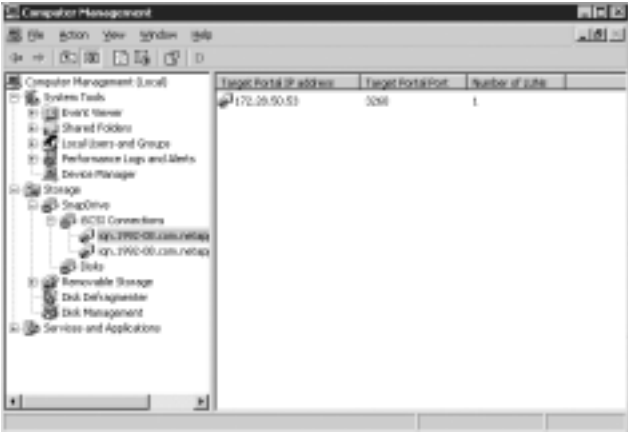
The following table describes the iSCSI connection details you can examine using the Computer Management (MMC) window on your Windows host.

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

Examining details of iSCSI connections

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

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	Perform the following actions: 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 Connections.

Step	Action	
3	If...	Then...
	You want to view the details of all iSCSI connections that exist on the Windows host	The details are displayed in the right panel of the MMC. 
	You want to view the details of a specific iSCSI connection that exists on the Windows host	- Double-click iSCSI Connections. - Select the iSCSI connection whose details you want to view. Result: The details are displayed in the right panel of the MMC. 

About this chapter

This chapter explains how to use SnapDrive to create virtual disks that you can access using FCP and iSCSI.

Topics in this chapter

This chapter covers the following topics:

- ◆ [“About virtual disk management”](#) on page 130
- ◆ [“Creating a virtual disk”](#) on page 131
- ◆ [“Creating a shared virtual disk on a Windows cluster”](#) on page 141
- ◆ [“Creating a virtual disk as a quorum disk on a new Windows cluster”](#) on page 142
- ◆ [“Creating a shared virtual disk on a Windows cluster”](#) on page 153

About virtual disk management

Rules about managing virtual disks

After you install SnapDrive to manage your virtual disks

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

Note

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

Creating a virtual disk

Rules for creating a virtual disk

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

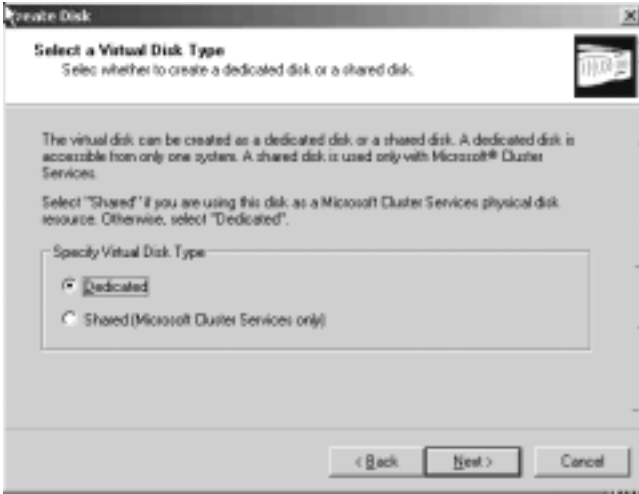
- ◆ If you are adding the virtual disk to a cluster, make sure to perform the following procedure on whichever node owns that cluster's physical disk resources.
- ◆ To avoid the possibility of unwritable files, do not attempt to create a virtual disk on a filer volume that holds anything other than virtual disks. Conversely, do not put anything other than virtual disks on a filer volume that contains virtual disks.

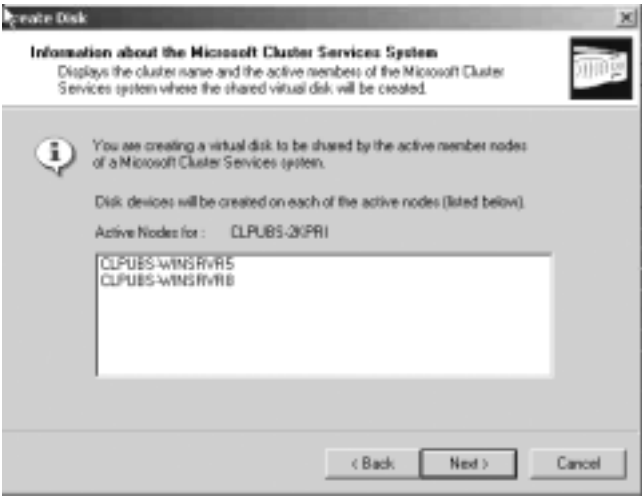
Creating a virtual disk

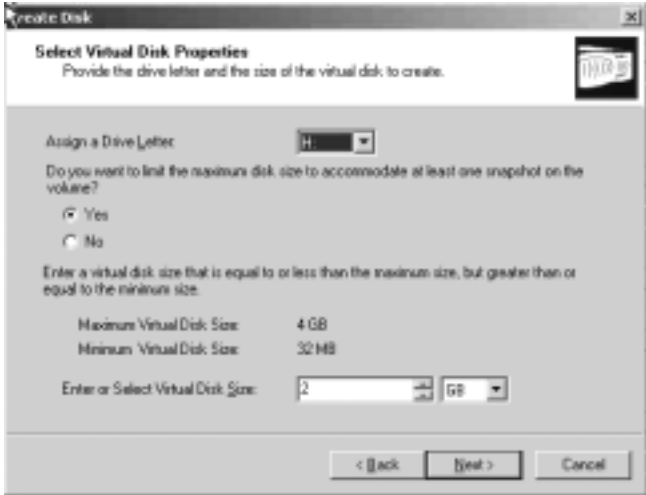
To create an FCP- or iSCSI-accessed virtual disk, complete the following steps.

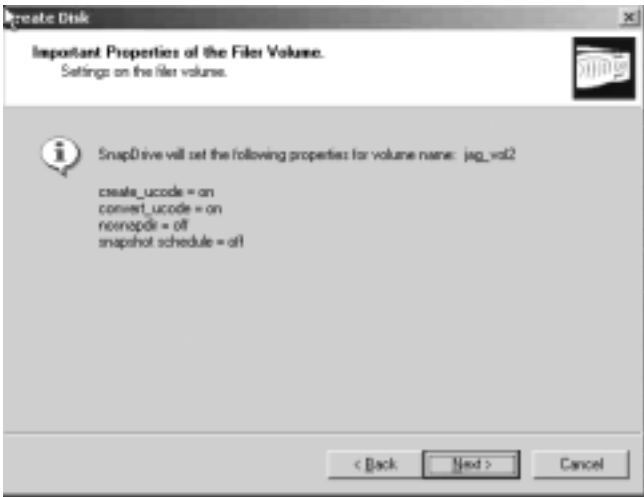
Step	Action
1	Create the dedicated volumes that will hold your virtual disks on the filer and create CIFS shares for those volumes. See “Creating a filer volume” on page 40 and “Creating a CIFS share” on page 43, and also consult the <i>Data ONTAP File Access Management Guide</i> .
2	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
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.
4	In the Create Disk wizard, click Next.

Step	Action
5	In the Provide a Path and Name panel, perform the following actions: ◆ In the Enter a Virtual Disk UNC Path to Filer Volume or Qtree field, type the filer location for the virtual disk. Alternatively, click Browse and navigate to that location. ◆ In the Enter a Name for the New Virtual Disk field, type in a descriptive name for the virtual disk; for example, “corporate billing” or “sunnyvale gym.” The name you enter in this field is automatically lowercased.  ◆ Click Next. Result: The Select a Virtual Disk Type panel is displayed.

Step	Action						
6	In the Select a Virtual Disk Type panel, perform one of the following actions: 						
	<table border="1"> <thead> <tr> <th data-bbox="229 822 655 876">If...</th><th data-bbox="655 822 1241 876">Then...</th></tr> </thead> <tbody> <tr> <td data-bbox="229 876 655 968">The virtual disk will belong to a single-host system</td><td data-bbox="655 876 1241 968">Select Dedicated, click Next, and then skip to Step 8.</td></tr> <tr> <td data-bbox="229 968 655 1046">The virtual disk will be a Windows cluster resource</td><td data-bbox="655 968 1241 1046">Select Shared, click Next, and then proceed to the next step.</td></tr> </tbody> </table>	If...	Then...	The virtual disk will belong to a single-host system	Select Dedicated, click Next, and then skip to Step 8 .	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 8 .						
The virtual disk will be a Windows cluster resource	Select Shared, click Next, and then proceed to the next step.						

Step	Action
7	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.  The screenshot shows a Windows XP-style window titled "Create Disk". Inside, there's a section titled "Information about the Microsoft Cluster Services System" with a sub-header "Displays the cluster name and the active members of the Microsoft Cluster Services system where the shared virtual disk will be created." Below this, an information icon (i) is next to the text: "You are creating a virtual disk to be shared by the active member nodes of a Microsoft Cluster Services system." Further down, it says "Disk devices will be created on each of the active nodes (listed below)." and "Active Nodes for : CLPUBS-2KSPRI". A list box contains two entries: "CLPUBS-WINSRVR5" and "CLPUBS-WINSRVR6". At the bottom, there are three buttons: "< Back", "Next >" (which is highlighted with a black border), and "Cancel".

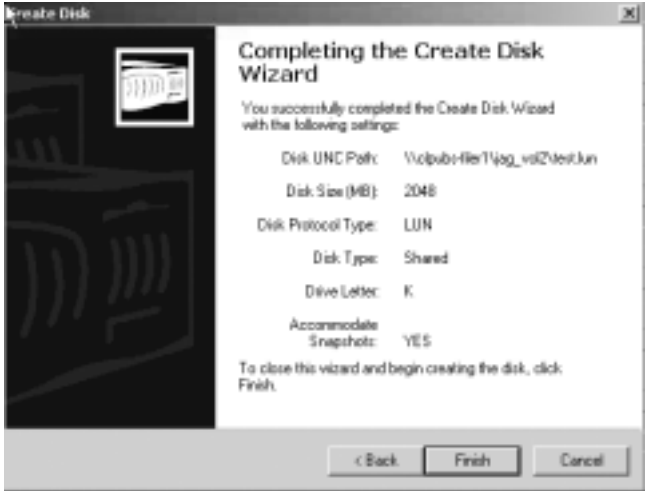
Step	Action
8	In the Select Virtual Disk Properties panel, perform the following actions: ◆ Select from the list of available drive letters a drive letter for the virtual disk you are creating. ◆ Select either the Yes or No radio button for “Do you want to limit the maximum disk size to accommodate at least one snapshot?”. When you select this option, the disk size limits displayed are accurate only when they first appear on the Select Virtual Disk Properties panel. When this option is selected, the following actions might interfere with the creation of at least one snapshot: ❖ The option to limit the maximum disk size to accommodate at least one snapshot is <i>not</i> selected when SnapDrive is used to create an additional virtual disk in the same filer volume. ❖ A virtual disk is created in the same filer volume <i>without</i> using SnapDrive. ❖ Data objects other than virtual disks are stored on this filer volume. ◆ Select a disk size, which must fall within the minimum and maximum values displayed in the panel. ◆ Click Next. Result: If the settings on the filer volume or qtree on which you are creating the virtual disk are not as required by SnapDrive for the create operation to proceed, the Important properties of the Filer Volume panel is displayed, as described in Step 9. Otherwise, Step 9 is skipped. 

Step	Action	
9	The Important Properties of the Filer Volume panel displays the settings that will be set for the volume or qtree you specified in Step 5 of this procedure. Note_____ The virtual disk creation process cannot proceed without SnapDrive configuring the settings that are displayed in this panel. Therefore, you must accept these settings. _____ Click Next.  Result: The Select Initiators panel is displayed.	
10	If...	Then...
	The virtual disk will belong to a single-host system	Go to Step 16 .
	The virtual disk will be a Windows cluster resource	Go to the next step.
11	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.	

Step	Action
12	In the Select Initiators panel, select the initiator for the virtual disk you are creating and use the arrows to move it back and forth between the two panes. If you select an iSCSI initiator and an iSCSI connection to the filer on which you are creating the virtual disk does <i>not</i> exist, you are prompted to select a target portal. Also, if your target requires authentication of hosts that connect to it, you can enter that information here. After you click OK, the iSCSI connection from the Windows host to the filer is established, even if you do not complete the Create Disk Wizard.

Step	Action
13	Repeat Step 11 and Step 12 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.
14	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 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.
15	Go to Step 18 .

Step	Action
16	In the Select Initiators panel, select the FCP or iSCSI initiator for the virtual disk you are creating, and use the arrows to move it back and forth between the two panes.  If you select an iSCSI initiator and an iSCSI connection to the filer on which you are creating the virtual disk does <i>not</i> exist, you are prompted to select a target portal. Also, if your target requires authentication of hosts that connect to it, you can enter that information here. After you click OK, the iSCSI connection from the Windows host to the filer is established, even if you do not complete the Create Disk Wizard. 

Step	Action
17	In the Select Initiators panel, click Next. Result: The Completing the Create Disk Wizard panel is displayed.
18	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

About creating shared virtual disks on a Windows cluster

The process that you must follow 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 142.

For information about how to create a shared virtual disk, which will *not* be used as a quorum disk, on a Windows cluster, see “[Creating a shared virtual disk on a Windows cluster](#)” on page 153.

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

Prerequisites

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

- ◆ You have one of the following:
 - ❖ Two host machines with Windows 2000 Advanced Server installed
 - ❖ Two to four host machines with Windows Server 2003 Standard Edition or Enterprise Edition installed
- ◆ Your filer is running Data ONTAP 6.4.2.
- ◆ Each node of the cluster contains the following:

If...	Then...
You want the quorum disk to be an iSCSI-accessed LUN	Each host node must have the following installed: ◆ A GbE NIC (as recommended in the iSCSI Microsoft Initiator Software Support Kit 1.0) ◆ The Microsoft Software Initiator driver ◆ (Optionally) A FastEthernet NIC dedicated to internal cluster traffic For information about the iSCSI Microsoft Initiator Software Support Kit, go to http://now.netapp.com.
You want the quorum disk to be an FCP-accessed LUN	Each host node must have the following installed: ◆ A NetApp qualified FCP HBA ◆ The driver and firmware for the FCP HBA For information about the qualified FCP HBAs, go to http://now.netapp.com.

Guideline to prevent resource competition in a Windows cluster

To ensure that all nodes of the cluster host never start simultaneously following a power failure, change the file time-out 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.

For more information

For detailed information about how to set up a virtual disk as a quorum disk, see the following topics:

- ◆ [“Creating a virtual disk as a quorum disk on a new Windows 2000 Server cluster”](#) on page 144.
- ◆ [“Creating a virtual disk as a quorum disk on a new Windows Server 2003 cluster”](#) on page 146

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

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

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

Note

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

Task	Procedure
1	Make sure that the following are installed on both nodes of the cluster: ◆ Appropriate FCP HBA drivers or the Microsoft iSCSI Software Initiator drivers For information about the drivers, see “Prerequisites” on page 142. ◆ SnapDrive 3.0 For information about installing SnapDrive, see “Installing or Upgrading SnapDrive” on page 55.
2	Create a shared virtual disk on node 2 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 131.
3	Disconnect the virtual disk from node 2. For information about how to disconnect a virtual disk, see “Disconnecting virtual disks” on page 164.
4	Using the drive letter you noted in Step 2, connect the virtual disk to node 1. For information about how to connect a virtual disk, see “Connecting virtual disks” on page 156.

Task	Procedure
5	Install and configure the Windows cluster services 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.
6	Reapply the service pack—SP3 or SP4—that was installed on node 1 before you began this procedure. After applying the service pack, reboot the node when directed by the service pack installation.
7	Install and configure the Windows cluster on node 2, and join node 2 to the cluster you created in Step 5.
8	From node 2, connect to the virtual disk you created in Step 2. See “Connecting virtual disks” on page 156 for instructions.
9	Reapply the service pack—SP3 or SP4—that was installed on your Windows host before you began this procedure. After applying the service pack, reboot the node when directed by the service pack installation.
10	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

About this procedure

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

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

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

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

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 or the Microsoft iSCSI Software Initiator drivers For information about the drivers, see “Prerequisites” on page 142. ◆ SnapDrive 3.0 For information about installing SnapDrive, see “Installing or Upgrading SnapDrive” on page 55.

Task	Procedure	
3	If...	Then...
	You are using the Microsoft iSCSI software	Establish iSCSI connections to the filer from all nodes of the cluster using the MMC window of each node. To go to the MMC, select Start > Programs > Administrative Tools > Computer Management. For information about how to establish iSCSI connections, see “Establishing an iSCSI connection to a target” on page 121.
4	Create a dedicated virtual disk on any node that will be part of the cluster, 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 131. 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	Disconnect the virtual disk from the node to which it is currently connected. For information about how to disconnect a virtual disk, see “Disconnecting virtual disks” on page 164.	

Task	Procedure	
6	Connect to the virtual disk from another node that will be part of the cluster, using the path and drive letter you noted in Step 4. For information about how to connect a virtual disk, see “Connecting virtual disks” on page 156. Note Choose the Dedicated option when stepping through the Connect Disk Wizard.	
7	If the virtual disk in Step 6 is...	Then...
	The last node of the cluster	Go to Step 8. That is, the last node of the cluster must remain connected to the virtual disk.
	Not the last node of the cluster	a. Disconnect the virtual disk from the node to which it is currently connected. For information about how to disconnect a virtual disk, see “Disconnecting virtual disks” on page 164. b. Go to Step 6.
8	On the node to which the virtual disk is connected now, launch the Windows Server 2003 Cluster Administrator. If the Cluster Administrator is launched for the first time on this node, you are prompted to specify the action to take. Select Create New Cluster from the Action drop-down list. If the Cluster Administrator is launched subsequently, it does not prompt you to specify the action to take. In that case, select File > New > Cluster from the Cluster Administrator. Result: The New Server Cluster Wizard is displayed.	

Task	Procedure	
9	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 window is displayed.	
10	If...	Then...
	The virtual disk you created in Step 4 is automatically selected as the quorum disk	Go to Step 11 .
	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.
11	Step through the remaining windows of the New Server Cluster Wizard. After you step through all of the New Server Cluster Wizard windows, the first node in the cluster is up and functional.	

Task	Procedure
12	Go to the Windows host that will be the next node in the cluster and connect to the virtual disk (as a shared disk this time) you created in Step 4 from this node, using the path and drive letter you noted in Step 4. Note Choose the Shared option when stepping through the Connect Disk Wizard at this point. For information about how to connect a virtual disk, see “Connecting virtual disks” on page 156. Result: The following error message is displayed when you go through the connect operation: “Unable to retrieve a list of virtual disk snapshots. Error: The system cannot find the file specified.” Note The preceding error message is expected because the node in Step 8 owns the virtual disk.
13	Click OK to clear the error message. Result: The connect operation is completed successfully.
14	Launch the Windows Server 2003 Cluster Administrator and perform the following actions: ◆ Select Add Nodes to Cluster. ◆ Enter the name of the cluster (as in Step 9). ◆ Click Next. Result: The Add Nodes Wizard is displayed with the name of the node on which you are currently working.

Task	Procedure	
15	In the Add Nodes Wizard, follow the prompts to enter the following information in the Wizard windows: ◆ 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. ◆ Password for the cluster service account. Note _____ This user name password should be the same as the one you entered in Step 9. _____ Result: After you enter the information, the Proposed Cluster Configuration window is displayed.	
16	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.
17	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	
18	If...	Then...
	The node you added to the cluster was the last node	Go to Step 19 .
	The node you added to the cluster was not the last node	Go to Step 12 .
19	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 virtual disk on a Windows cluster” on page 153.	

Creating a shared virtual disk on a Windows cluster

When to use this procedure

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

About creating a shared virtual disk on a Windows cluster

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

Creating a shared virtual disk

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

Step	Action
1	Make sure that the appropriate FCP HBA drivers or the Microsoft iSCSI Software Initiator drivers and SnapDrive are installed on all nodes in a cluster. See “Prerequisites” on page 142 for information about the drivers. See “Installing the new SnapDrive components” on page 104.
2	Create as many shared virtual disks as are necessary to hold your data. See “Creating a virtual disk” on page 131 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.

About this chapter This chapter explains how to use SnapDrive to manage virtual disks.

Topics in this chapter This chapter covers the following issues:

- ◆ “[Connecting virtual disks](#)” on page 156
- ◆ “[Disconnecting virtual disks](#)” on page 164
- ◆ “[Deleting a virtual disk](#)” on page 167
- ◆ “[Expanding virtual disks](#)” on page 168
- ◆ “[Examining and modifying virtual disk properties](#)” on page 172
- ◆ “[Administering SnapDrive remotely](#)” on page 174
- ◆ “[Enabling SnapDrive notification](#)” on page 175

Connecting virtual disks

Reason for connecting to virtual disks

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

Rule for connecting

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

Caution

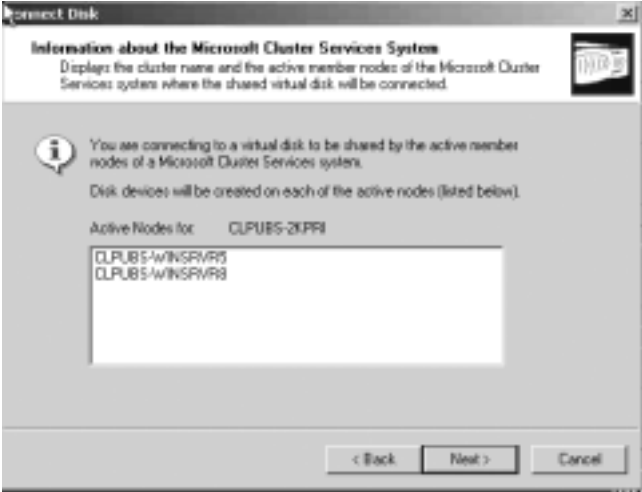
Do not try to connect to a virtual disk if it is already connected to another machine; SnapDrive does not support such simultaneous use.

Connecting a virtual disk

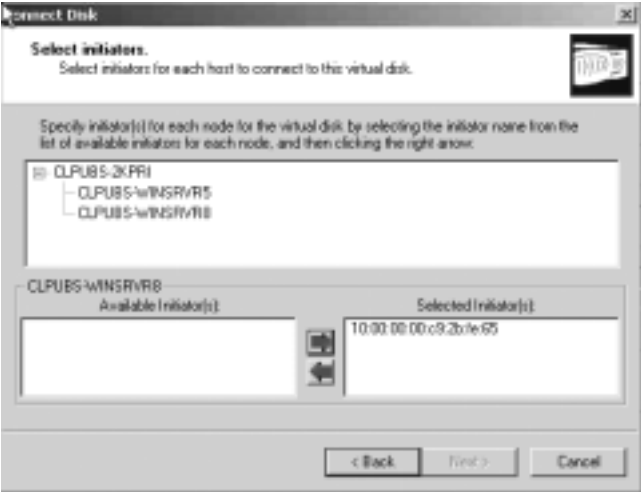
To connect your host to a virtual disk, complete the following steps.

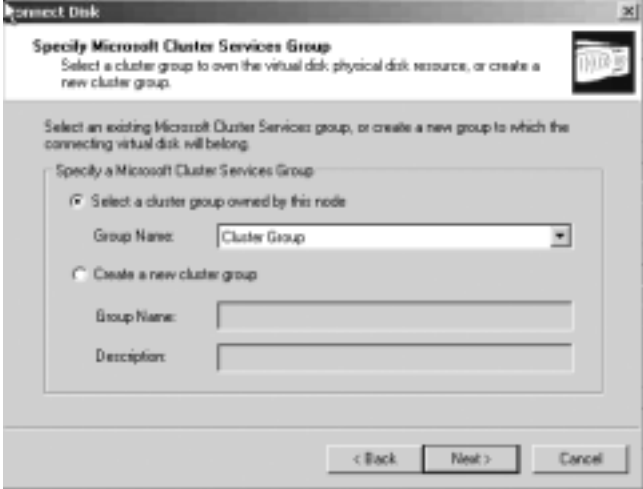
Step	Action
1	Close all Explorer windows on your host.
2	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
3	Perform the following actions to launch the Connect Disk wizard: a. Expand the Storage option in the left panel of 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.
4	In the Connect Disk Wizard, click Next.

Step	Action	
5	In the Provide Virtual Disk Location panel, perform the following actions. ◆ Click Browse. ◆ Navigate to the file volume on which the virtual disk resides. ◆ Select the virtual disk (LUN) with a .lun extension to which you want to connect. ◆ Click Next. Result: The Select a Virtual Disk Type panel is displayed.	
6	If...	Then...
	The virtual disk will belong to a single system	Select Dedicated, click Next, and then continue to Step 8 .
	The virtual disk will become a Windows cluster resource	Select Shared, click Next, and then continue to the next step.

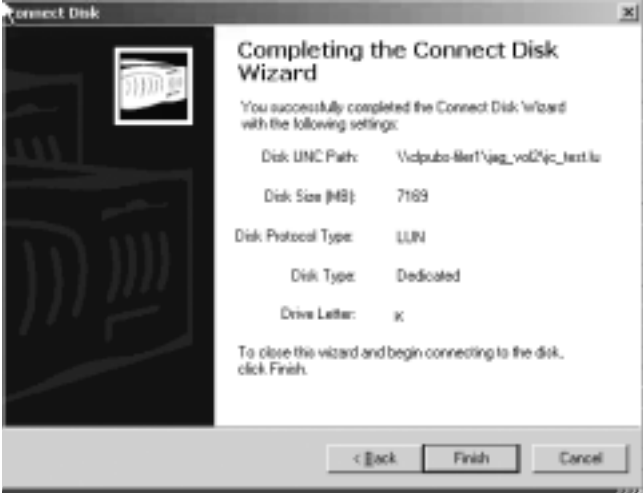
Step	Action
7	In the Information about the Microsoft Cluster Services System panel, verify that you want the disk to be shared by the nodes listed, and then click Next. 

Step	Action	
8	In the Select Virtual Disk Drive Letter panel, perform the following actions. ◆ Select from the list of available drive letters a drive letter for the virtual disk you are connecting. ◆ Click Next.	
9	If...	Then...
	The virtual disk will belong to a single-host system	Go to Step 13 .
	The virtual disk will be a Windows cluster resource	Go to the next step.

Step	Action
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. The list of Available Initiators for that host is displayed in the bottom-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 remains grayed out until initiators for all hosts of a cluster are selected. Result: The Specify Microsoft Cluster Services Group panel is displayed.

Step	Action
11	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.
12	Go to Step 14 .

Step	Action
13	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 If MPIO is installed on the system, two FCP initiator ports can be selected simultaneously. ◆ Click the right arrow to move the selected initiator to the Selected Initiators list on the right side. If you change your mind, you can move an initiator from the Selected Initiators list to the Available Initiators list by selecting the initiator and clicking the left arrow. ◆ Click Next. Result: The Completing the Connect Disk Wizard panel is displayed. Note See the <i>Data ONTAP Block Access Management Guide</i> for information about how to determine the port for your HBA.

Step	Action
14	In the Completing the Connect Disk Wizard panel, perform the following actions.  ◆ Verify all the settings. ◆ If you need to change any settings, click Back to go back to the previous Wizard panels. ◆ Click Finish. Result: The Computer Management window is displayed, with the newly connected virtual disk now appearing under SnapDrive > Disks in the left panel.

Disconnecting virtual disks

About disconnecting a virtual disk

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

Guidelines for disconnecting a virtual disk

The following guidelines apply to disconnecting a virtual disk:

- ◆ You must make sure that the virtual disk you are disconnecting is not monitored with the Windows Performance Monitor (perfmon).
- ◆ You can only disconnect a shared virtual disk (that is, a non-quorum disk) after removing the cluster resource dependencies from the virtual disk.
- ◆ You can disconnect a quorum disk only after replacing it with another disk that takes over as a quorum disk for the cluster.

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 164.
- ◆ By forcing a disconnect, as described in “[Forcing a disconnect](#)” on page 165.
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 that an application such as Windows Explorer or the Windows operation system is using. However, you can force a disconnect to override this protection.

Disconnecting a virtual disk

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

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

Step	Action
2	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
3	Double-click SnapDrive in the left panel 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 panel the disk that you want to disconnect.
5	Click Action (from the menu choices on top of the MMC), and then select Disconnect Disk.
6	When prompted by the pop-up window, 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.

Forcing a disconnect

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

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

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

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

Step	Action
3	Double-click SnapDrive in the left panel 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 panel 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 by the pop-up panel, 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 156.

Deleting a virtual disk

Guidelines for deleting a virtual disk

You must keep the following guidelines in mind when deleting a virtual disk:

- ◆ You must make sure that the virtual disk you are deleting is not monitored with the Windows Performance Monitor (perfmon).
- ◆ You must 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 must 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	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	Double-click SnapDrive in the left panel 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 panel the disk that you want to delete.
4	Click Action (from the menu choices on top of the MMC), and then select Delete Disk.
5	When prompted by the pop-up panel, click Yes to proceed with the operation. Result: The icons representing the deleted virtual disk disappear from both the left and right panels of the Computer Management window.

Expanding virtual disks

When to expand a virtual disk

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

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 filer storage](#)” on page 13 for more information.
- ◆ After you increase the size of a virtual disk, you cannot reduce it in size, except by restoring a snapshot taken prior to the expansion of the virtual disk. Such a restore causes the loss of any data added to the virtual disk after you expanded the virtual disk. (Conversely, restoring a snapshot of a virtual disk whose size has since been reduced enlarges the virtual disk to its former size.)
- ◆ You should ensure that you create a virtual disk that is a quorum disk of a size recommended by Microsoft for your Windows cluster setup because 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 171.

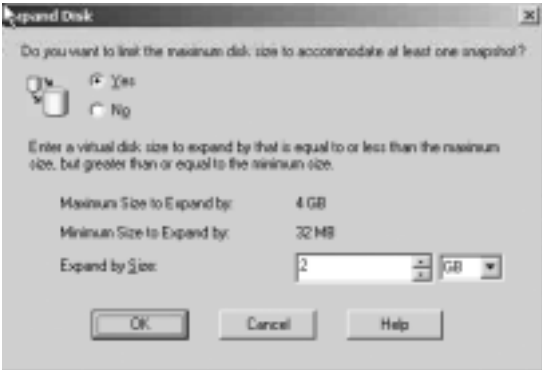
- ◆ When you expand a virtual disk that serves as a Windows cluster physical disk resource, that physical disk resource is momentarily taken offline and then brought back online to refresh the resource properties. Also taken offline are all the Windows cluster resources having direct or indirect dependency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

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	Select Start > Programs > Administrative Tools > Computer Management. Result: The MMC is launched.
2	Double-click SnapDrive in the left panel 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 panel the disk that you want to expand.
4	Click Action (from the menu choices on top of the MMC), and then select Expand Disk. Result: The Expand Disk panel is displayed. 

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

Expanding a quorum disk

To expand a virtual disk that is a quorum disk, 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 131. 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 167.
	You would like to keep the original quorum disk but expand it anyhow	1. Create a new virtual disk as described in “Creating a virtual disk” on page 131. 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 169. 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 167.

Examining and modifying virtual disk properties

Property you can examine

You can examine the Monitor Time Interval property for virtual disks. This property specifies how frequently SnapDrive monitors the snap reserve space on the filer volume for all virtual disks on the system. The default is every 60 minutes.

Guidelines about examining and modifying virtual disk property

Follow these guidelines when examining and modifying the virtual disk property:

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

Examining and modifying global virtual disk property

To examine or modify the virtual disk property, complete the following steps.

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	Double-click SnapDrive in the left panel of the MMC, then select Disks.
3	Click Action (from the menu choices on top of the MMC), then select Properties. Result: The SnapDrive Properties panel with the Virtual Disk Monitor tab selected is displayed. Note _____ Prior to SnapDrive 3.0, the Virtual Disk Monitor tab was labeled Snapshot Monitor in the SnapDrive GUI.

Step	Action
4	In the Virtual Disk Monitor tab, perform the following actions: ◆ Enter a value in the Monitor Time Interval field, in minutes. ◆ Click OK. The following values are valid: Default—60 minutes Minimum value—30 minutes Maximum value—10080 minutes (7 days) Note— You can also set the Monitor Time Interval value to 0 minutes, which disables periodic snapshot monitoring; however, after configuring the value when you click OK, SnapDrive runs a one-time scan to obtain the current snap reserve space on the filer volume. Additionally, every time you click OK in the Virtual Disk Monitor tab, SnapDrive runs a scan to obtain the current snap reserve space on the filer volume. The scan is also run every time the SnapDrive service starts.

Administering SnapDrive remotely

Remote administration requirements

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

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

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

Running remote administration

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

Note_____

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

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	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 window is displayed.
3	In the Select Computer window, 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.

Enabling SnapDrive notification

About notification settings

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

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

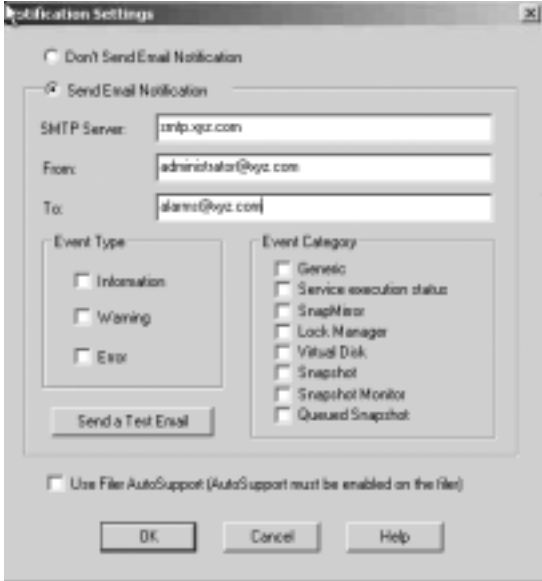
Note

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

Enabling SnapDrive notification

To enable email notification for selected SnapDrive events, complete the following procedure.

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	Select SnapDrive, click Action from the menu choices on top of the MMC, and then select Notification Settings. Result: The Notification Settings window is displayed.

Step	Action
3	In the Notification Settings panel, perform the following actions.  - Select Send Email Notification. - Enter the outgoing SMTP server, and the From and the To addresses. - Select one or more Event Types about which you want to be notified. - Select the Event Category items about which you want to be notified when the specified event types take place. - Select Use Filer Autosupport if you want to enable a subset of the Windows System Events for Autosupport on the filer. - Click OK.
4	You can verify the email output of the Event Notification feature by clicking Send a Test Email on the Notification Settings panel.

About this chapter

This chapter describes how to use the SnapDrive Snapshot™ feature to create snapshots for data backup and restore.

Additionally, this chapter provides an overview of the methods and media you can use to archive your virtual disk snapshots to tape or other offline media. For details about how to use those methods and media, see the documentation for the archiving application you use.

Topics in this chapter

This chapter discusses the following topics:

- ◆ [“How snapshots work”](#) on page 178
- ◆ [“Creating snapshots”](#) on page 180
- ◆ [“Connecting to LUNs in a snapshot”](#) on page 187
- ◆ [“Restoring virtual disks from snapshots”](#) on page 194
- ◆ [“Deleting snapshots”](#) on page 197
- ◆ [“Overview of archiving and restoring snapshots”](#) on page 199

How snapshots work

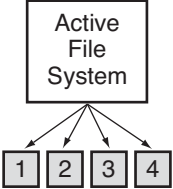
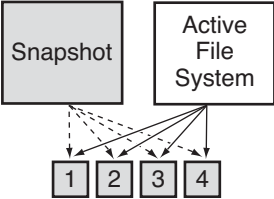
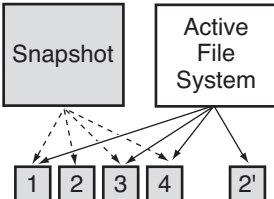
What a snapshot is

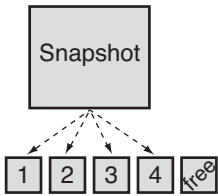
A snapshot is a point-in-time, read-only image of the filer volume. Snapshots can restore your databases rapidly if you encounter data corruption or other problems.

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

How snapshots work

The following figure illustrates how snapshots work.

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

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

Creating snapshots

Reasons for creating snapshots using SnapDrive

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

Note

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

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

Restrictions on snapshot creation

You need to be aware of the following facts:

- ◆ You can keep a maximum of 255 snapshots with Data ONTAP 6.4.2.
After the number of snapshots has reached the maximum limit, the Snapshot Create operation fails, and you must delete some of the old snapshots before you can take any more.
- ◆ SnapDrive does not support snapshots that are created from the filer console, because such a practice can lead to inconsistencies within the NTFS file system. Therefore, use only SnapDrive to create snapshots of virtual disks.

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

Note

Any snapshots inadvertently taken at the filer console or through FilerView are grayed out in the SnapDrive plug-in and are not usable by SnapDrive.

Snapshot requisites

The following requisites must be followed:

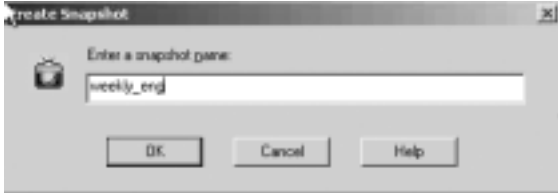
- ◆ Snapshots must be created through the SnapDrive MMC snap-in or through sdcli.exe, rather than the filer console or the volume snapshot schedule on the filer. This is because SnapDrive must first flush NTFS so that the virtual disk is consistent at the moment the snapshot is taken. This ensures the usability of the virtual disk file in the snapshot directory.
- ◆ You must create separate SnapDrive snapshot schedules for each volume that contains virtual disks.
- ◆ The SnapDrive service can perform one task at a time. Therefore, if you have multiple tasks scheduled to start at exactly the same time, only the first one will succeed, while others will fail.

Creating a snapshot

To create a snapshot using SnapDrive, 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 get to the Create Snapshot menu item: 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 Disks. d. Select the disk for which you want to create a snapshot. e. Click Action (from the menu choices on top of the MMC). f. Select Create Snapshot from the drop-down menu. Result: The Create Snapshot text box is displayed.

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

Scheduling snapshots

Make sure that you have read the snapshot requirements described in “[Snapshot requisites](#)” on page 181 before you proceed with the following procedure.

To schedule SnapDrive snapshots, complete the following steps.

Note

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

Step	Action
1	Create a batch file (a file with a .bat extension) containing the following command on the Windows host on which you are scheduling snapshots: <pre>sdcli snap create [-m <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 to be created. <i>DriveLetterList</i> is a list of space-separated drive letters. When -x flag is specified, it causes the snapshots to be created only for the drives specified by the -D flag. Otherwise, snapshots are created for all the disks on the filer volumes used by the listed drives. Example: <code>sdcli snap create -s Jun_13_03 -D j k l</code> The preceding example creates a snapshot named Jun_13_03 for each volume containing one or more of the virtual disks mapped to the specified drives (that is, J:, K:, and L:). The snapshots created are consistent for all virtual disks contained by those volumes.
2	Select Start Menu > Settings > Control Panel > Scheduled Tasks.
3	Double-click Add Scheduled Task. Result: The Scheduled Task Wizard is launched.
4	In the Scheduled Task Wizard appears, click Next.
5	After the next panel appears, click Browse, and navigate to the folder where the .bat file you created in Step 1 is located.
6	Select the batch (.bat) file.

Step	Action
7	After the following panel appears, select from the list of frequencies, then click Next. 
8	After the following panel appears, enter a start time and complete the detailed frequency parameters. The option details displayed on this panel vary depending on the snapshot frequency you picked in the previous panel. 

Step	Action
9	In the following panel, type the user name (the administrator account name and password (repeated for confirmation), then click Next. 

Note

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

Connecting to LUNs in a snapshot

About read/write connections

You can connect a host to a virtual disk in a snapshot in read/write mode. (This is useful for conducting tests, for example.)

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

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

For details, see your Data ONTAP documentation.

Snapshot cautions

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

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

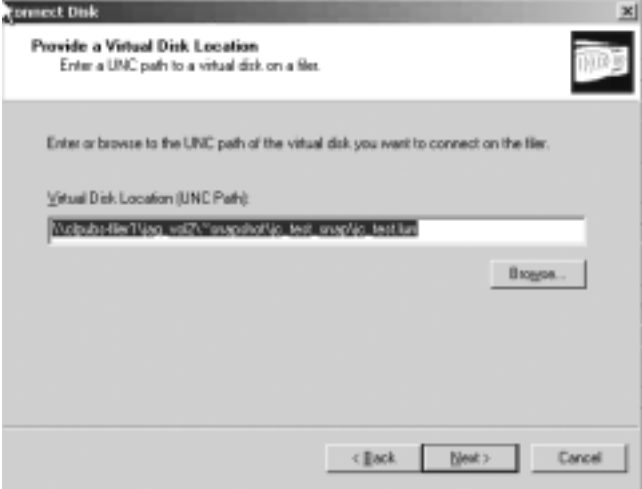
Connecting to a virtual disk (LUN) in a snapshot

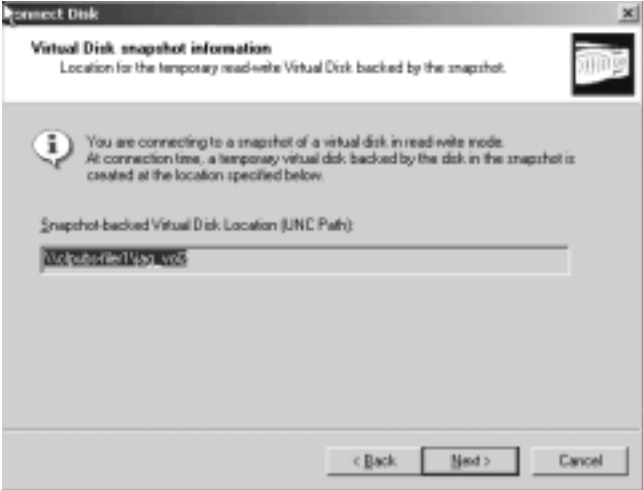
To connect to a virtual disk (LUN) in a snapshot using SnapDrive, complete the following steps.

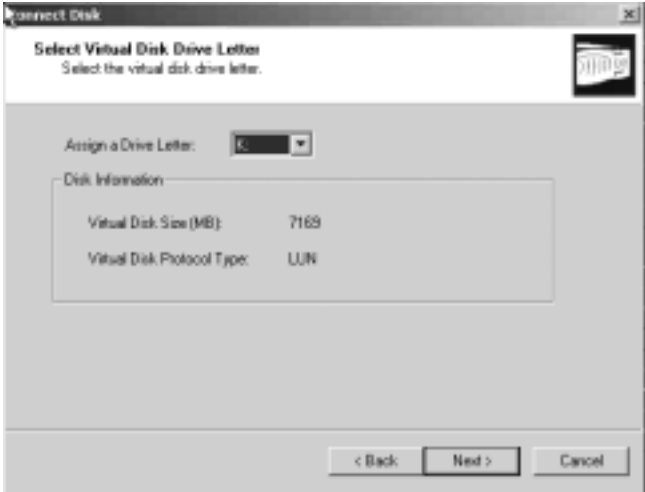
Caution

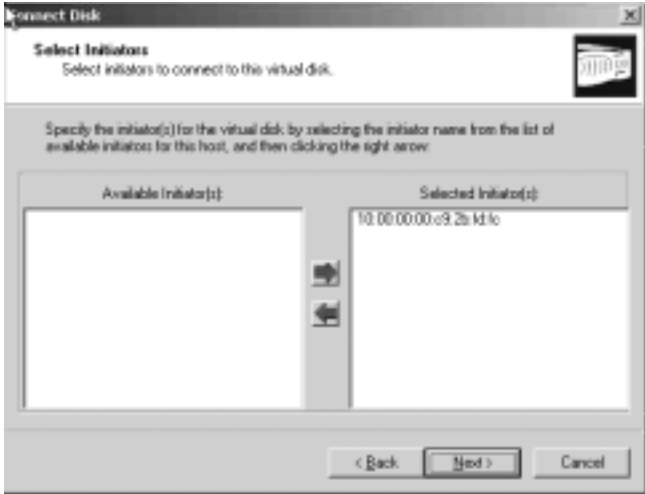
This version of SnapDrive is not aware of the Data ONTAP LUN cloning feature. Therefore, do not use the LUN cloning feature to clone a virtual disk backed by a snapshot that is connected using SnapDrive. SnapDrive considers such a disk to be temporary, and it deletes the disk upon disconnect.

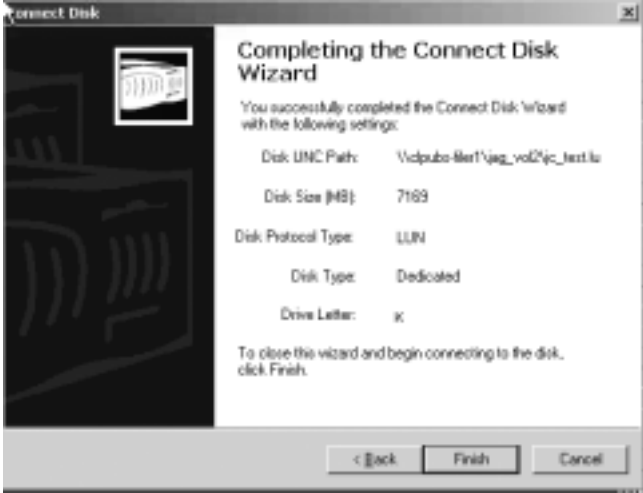
Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	Perform the following actions to launch the Connect Disk wizard: a. Expand the Storage option in the left panel of the MMC, if it is not expanded already. b. Double-click SnapDrive in the left panel of the MMC. c. Select Disks. d. Click Action (from the menu choices on top of the MMC). e. Select Connect Disk from the drop-down menu.
3	In the Connect Disk Wizard, click Next.

Step	Action
4	In the Provide Virtual Disk Location panel, perform the following actions.  - Click Browse to browse to the \~snapshot directory of the filer volume holding the snapshot 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 directory, make sure that cifs.show_snapshot is set to On and vol option nosnapdir is set to No on your filer.
5	In the Select a Virtual Disk Type panel, Dedicated is automatically selected because a snapshot can be connected only as a dedicated virtual disk. Click Next. Result: The Virtual Disk Snapshot Information panel is displayed.

Step	Action
6	In the Virtual Disk Snapshot Information panel, a path is automatically specified where a temporary read-write virtual disk is created when you connect to the disk backed up by the snapshot. Click Next.  Result: The Select Virtual Disk Drive Letter panel is displayed.

Step	Action
7	In the Select Virtual Disk Drive Letter panel, perform the following actions.  - Select from the list of available drive letters for the virtual disk you are creating. - Click Next. Result: The Select Initiators panel is displayed.

Step	Action
8	In the Select Initiators panel, perform the following actions.  - 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. - Click Next. Result: The Completing the Connect Disk Wizard panel is displayed.

Step	Action
9	In the Completing the Connect Disk Wizard panel, perform the following actions.  The screenshot shows a Windows XP-style dialog box titled 'Completing the Connect Disk Wizard'. On the left is a dark graphic with a server icon. The main text area says 'You successfully completed the Connect Disk Wizard with the following settings:'. Below this, several settings are listed: 'Disk UNC Path: \\olpubs-llert1\jag_vol2\jc_text.lu', 'Disk Size (MB): 7169', 'Disk Protocol Type: LUN', 'Disk Type: Dedicated', and 'Drive Letter: x:'. At the bottom, it says 'To close this wizard and begin connecting to the disk, click Finish.' and there are three buttons: '< Back', 'Finish', and 'Cancel'. - 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 newly connected virtual disk now appearing under SnapDrive > Disks in the left panel.

Restoring virtual disks from snapshots

About restoring from snapshots

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

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

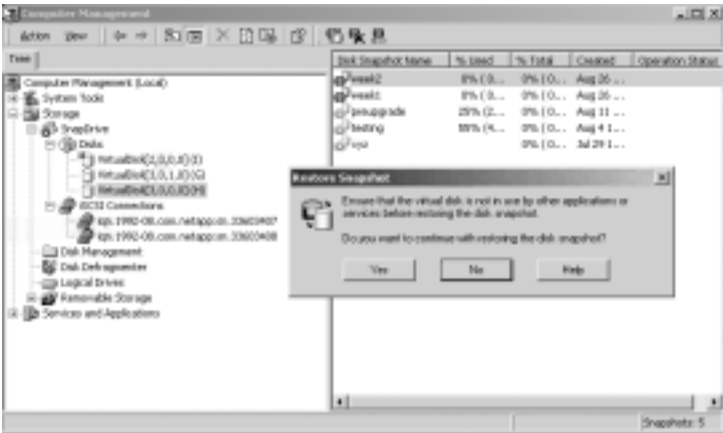
If you expand the virtual disk and then restore it from a snapshot taken prior to that expansion, the restored virtual disk reverts to its size at the moment the snapshot was taken.

Restoring a virtual disk from a snapshot

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

Step	Action
1	Shut down all resources directly or indirectly dependent on the virtual disk. Make sure that the virtual disk is not being used by the Windows file system or any other process, and that no user has the virtual disk open in Windows Explorer. Shut down any application that is using the virtual disk. Caution————— Make sure that the Windows Performance Monitor (perfmon) is not monitoring the virtual disk.
2	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.

Step	Action
3	Perform the following actions: 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. Double-click Disks. d. Select the virtual disk that you want to restore.
4	In the right pane of the MMC, perform the following actions: a. Right-click the specific snapshot you want to restore. b. Select Restore Disk From Snapshot from the drop-down menu. Note_____ You can only restore a snapshot that is consistent with the active file system. Inconsistent snapshots are grayed out and not available for restoration. _____

Step	Action
5	In the Restore Snapshot panel, click Yes to restore the snapshot you selected.  Caution_____ Do not attempt to manage any Windows cluster resources while the restore is in progress.

Deleting snapshots

Reasons to delete snapshots

Delete older snapshots for the following reasons:

- ◆ To keep the number of stored snapshots less than the hard limit of 255 for Data ONTAP.
Be sure to delete old snapshots before the hard limit is reached; otherwise, subsequent snapshots could fail.
- ◆ To free up space on the filer volume
Even before the snapshot limit has is reached, a snapshot fails if not enough reserved space for it remains on the disk.

Deleting a snapshot

To delete a snapshot, complete the following steps.

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

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	Perform the following actions: 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. Double-click Disks. d. Select the virtual disk whose snapshot you want to delete.

Step	Action
3	In the right pane of the MMC, select the snapshot you want to delete. Note_____ You can only delete a snapshot that is consistent with the active file system. Inconsistent snapshots are grayed out and not available for deletion. _____
4	Click Action (from the menu choices on top of the MMC).
5	Select Delete from the drop-down menu.
6	In the Delete Snapshot panel, click Yes to delete the snapshot you selected.

Overview of archiving and restoring snapshots

About archives of SnapDrive backups

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

What to back up

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

Ways to archive SnapDrive backups

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

Note

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

Process of 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.

About this chapter

This chapter explains how SnapDrive implements multipathing to connect hosts to virtual disks (LUNs).

Topics in this chapter

This chapter discusses the following topics:

- ◆ “[Multipathing overview](#)” on page 202
- ◆ “[MPIO setup](#)” on page 204
- ◆ “[MPIO path management](#)” on page 206

Supplemental information on MPIO

Appendix A lists MPIO-related commands (and associated parameters) that run under sdcli.exe, the SnapDrive command-line utility. See “[Multipathing commands](#)” on page 233.

Multipathing overview

What multipathing does

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

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

How SnapDrive implements multipathing

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

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 3 or Service Pack 4 Note _____ Windows 2000 Server with SP3 requires hotfixes 816990, 822831, 815198, and 815616/325040. Windows 2000 Server with SP4 requires hotfix 822831. Windows 2000 Advanced Server with SP3 or SP4 in an MSCS configuration requires hotfixes 816990, 822831, 815198, and 815616/325040. _____ OR Windows Server 2003 ◆ Enterprise Edition is required for Windows cluster configuration Note _____ Windows Server 2003 Enterprise edition in an MSCS configuration requires hotfix 824354. _____
Disk-access protocol	FCP
Host clustering (optional)	Windows cluster. Host clustering also requires installation of the NetApp Dual HBA FCP Attach Kit for Windows on each Windows cluster node.
Operating system on filer	Data ONTAP 6.4.2 or higher
Filer clustering (optional)	NetApp filer clusters

MPIO setup

Installation assumptions

The following section assumes that you successfully installed SnapDrive 3.0 on a supported hardware-and-software configuration, and most important, you selected the check box labeled “Install (or Update) MPIO drivers” on the SnapDrive Driver Installation panel of the SnapDrive InstallShield Wizard.

Note

As previously mentioned, to use the MPIO option, you must install a pair of HBAs supplied in the NetApp Dual HBA FCP Attach Kit for Windows in each host in your configuration.

How MPIO features become available

When you create a virtual disk (LUN) on a Windows host on which MPIO is 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 [Step 16](#) of “[Creating a virtual disk](#)” on page 131. For Windows clusters, you specify an initiator for each Windows node in the cluster, as described in [Step 11](#) of “[Creating a virtual disk](#)” on page 131.

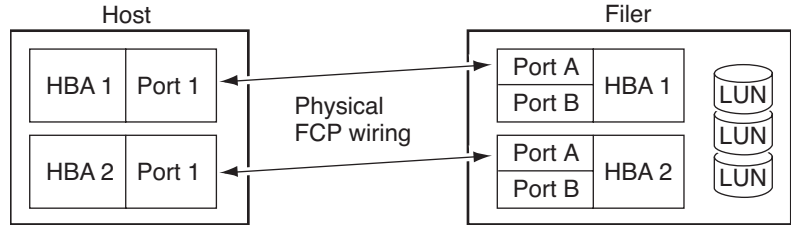
After you have successfully created the LUN, the multipath management features become available.

Supported MPIO topologies

MPIO configurations consist of three basic sets of physical components:

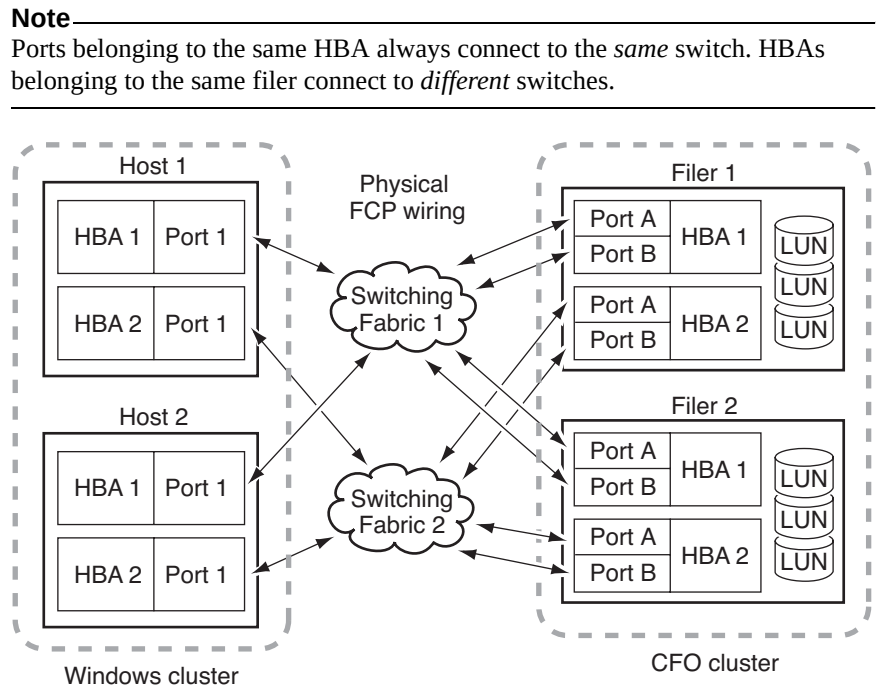
- ◆ Host (a single node or a Windows cluster pair)
- ◆ Switch (two per configuration provides maximum protection for fabric-attached filer clusters. Switches are not used in direct attached configurations.)
- ◆ Filer (a single head or a filer cluster pair)

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



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

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



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.

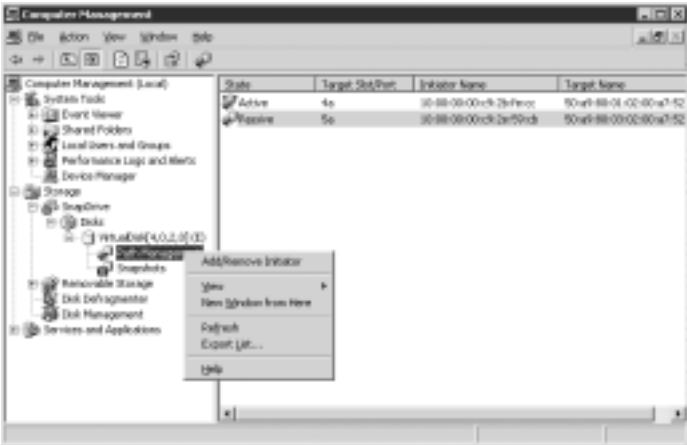
Note_____

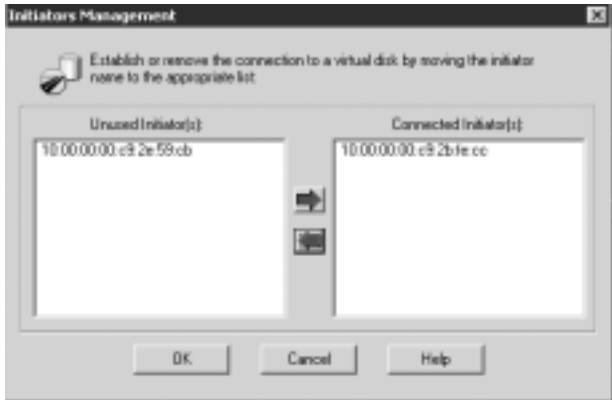
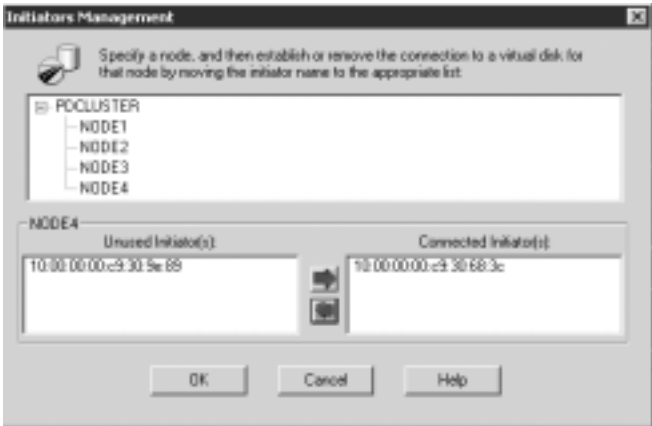
All GUI details correspond to the Computer Management Console. All command-line details correspond to the “cmd.exe session window.”

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.	
Command line	Single command	Launch a cmd.exe window; enter a “sdcli.exe path” 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 233.	
Command line	Automation script	Launch a cmd.exe window; enter the path and name of the script to be run. Note_____ When scheduling the batch file through the Windows Task Scheduler, specify a “Log on as” user account that has appropriate host, filer, and domain access permissions. For example, a properly configured SnapDrive service account has all necessary accesses enabled. _____	

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

Note You can use this same basic procedure to unmap MPIO paths as well. See also “[Multipathing commands](#)” on page 233 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 MPIO paths you want to manage.
2	After the Path Management icon appears on a branch beneath the virtual disk icon, right-click it. On the drop-down menu, select Add/Remove Initiator. 

Step	Action
3	If you are mapping MPIO paths for a Windows cluster configuration, 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.  The screenshot shows the 'Initiators Management' window. It has a title bar with a close button. Below the title bar is a message: 'Establish or remove the connection to a virtual disk by moving the initiator name to the appropriate list.' There are two list boxes: 'Unused Initiator(s)' on the left and 'Connected Initiator(s)' on the right. The 'Unused Initiator(s)' box contains the text '10:00:00:00:c9:2e:59:cb'. The 'Connected Initiator(s)' box contains the text '10:00:00:00:c9:2b:1e:cc'. Between the two boxes are two arrows: a right-pointing arrow and a left-pointing arrow. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.
4	To add MPIO paths on a Windows cluster, select an initiator for node 1 from the Unused Initiator(s) box in the Initiator 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.  The screenshot shows the 'Initiators Management' window for a cluster configuration. It has a title bar with a close button. Below the title bar is a message: 'Specify a node, and then establish or remove the connection to a virtual disk for that node by moving the initiator name to the appropriate list.' There is a tree view on the left showing a hierarchy: 'POCLUSTER' (expanded) with sub-items 'NODE1', 'NODE2', 'NODE3', and 'NODE4'. Below the tree view is a section for 'NODE4'. Inside this section, there are two list boxes: 'Unused Initiator(s)' on the left and 'Connected Initiator(s)' on the right. The 'Unused Initiator(s)' box contains the text '10:00:00:00:c9:30:5e:89'. The 'Connected Initiator(s)' box contains the text '10:00:00:00:c9:30:18:3c'. Between the two boxes are two arrows: a right-pointing arrow and a left-pointing arrow. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

Understanding MPIO path states

You can add, enable, activate, disable, or remove (delete) MPIO paths. The disable option disables all paths associated with WWPNs (World-wide Port Names) 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 four 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.)
- ◆ Target Port/Slot, which is the “friendly” scheme for identifying a port on an HBA on the filer bus; for example, “7a.”
- ◆ Initiator WWPN, which is the network identifier for a port on an HBA in the host; for example, “10:00:00:00:c9:2b:fd:50.”
- ◆ Target WWPN, which is the network identifier for a port on an HBA in the filer.

Changing MPIO path states

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

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

GUI command, sdcli command, or other event	On	Result
sdcli path add	A LUN	A new path is created.
map FCP port	A LUN	A passive 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 becomes disabled.
sdcli path enable	A disabled path	The path becomes passive.
sdcli path remove	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 = 20 seconds)	A path in the Pending Remove state	The path is deleted.

About this chapter

This chapter discusses how to use a SnapMirror destination volume to replicate SnapDrive virtual disks.

This chapter does not explain how to setup, configure, or manage SnapMirror on your filer. Instead, it focuses 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 Guide*.

Topics in this chapter

This chapter discusses the following topics:

- ◆ “[SnapMirror overview](#)” on page 212
- ◆ “[SnapMirror replication](#)” on page 214
- ◆ “[Initiating replication](#)” on page 216
- ◆ “[Connecting to destination volumes](#)” on page 218
- ◆ “[SnapMirror disaster recovery](#)” on page 221

SnapMirror overview

Understanding SnapMirror

SnapMirror creates asynchronous replicas of volumes that host virtual disks.

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.

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

Understanding asynchronous 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 at which 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 writes to the source disk are not available in the event of a catastrophic failure.

Requirements for using SnapMirror with SnapDrive

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

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

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

- ◆ 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 destination volume must have CIFS shares identical to those on the source volume.
You can create CIFS shares manually for the volumes on the destination filer. The data paths for these shares must match exactly as those on the source volumes. See your Data ONTAP *Data Protection Guide* for details.
- ◆ The Windows domain account used by the SnapDrive service must be a member of the local BUILTIN\administrators group on both the source and destination filers.
- ◆ The Windows domain account used to administer SnapDrive must have full access to the Windows domain to which both the source and destination filers belong.
- ◆ The source and destination filers must be configured to grant rsh access to the Windows domain account used by the SnapDrive service. For information about configuring your filer to grant rsh access, see [“Preparing the SnapDrive service account”](#) on page 48.
- ◆ The source and destination filers must be configured to grant root access to the Windows domain account used by the SnapDrive service. That is, the `waf_l_map_nt_admin_to_root` option must be set to On. For information about enabling filer options, see your Data ONTAP documentation.
- ◆ If you want to use a Windows host to access the replicated LUNs on the destination volume, the destination filer must have at least one LUN access protocol licensed (iSCSI or FCP).
- ◆ A TCP/IP connection must exist between the source filer and the destination filer.
- ◆ The SnapDrive service can perform one task at a time. Therefore, if you are scheduling multiple tasks on a host, make sure that you schedule these tasks to *not* start at exactly the same time. If multiple tasks are scheduled at the same time, only the first one will succeed, while others will fail.

SnapMirror replication

Replication upon snapshot creation

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

Replication using rolling snapshots

A special type of snapshots called the “rolling” snapshots can also be created using the SnapMirror GUI. These snapshots are used exclusively to facilitate frequent SnapMirror volume replication. As the regular snapshots, the rolling snapshots are replicated to the SnapMirror destination volume as soon as they are created.

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

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

How SnapDrive manages rolling snapshots

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

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

How rolling snapshots are named

The following format is used to name the rolling snapshots:

`@snapmir@{GUID}`

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

Examples: The following are examples of rolling snapshots:

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

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

Initiating replication

Requirements

Make sure you have read and satisfied the requirements listed in “[Requirements for using SnapMirror with SnapDrive](#)” on page 212 before you use the procedures in this section.

Initiating replication after snapshot creation

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

If...	Then...
You want to manually create a snapshot	See “ Creating a snapshot ” on page 181.
You want to set up a schedule for snapshot creation	See “ Scheduling snapshots ” on page 183.

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 panel of the MMC, if it is not expanded already. b. Double-click SnapDrive. c. Double-click Disks. d. Select the virtual disk, which you want to replicate, in the right panel of the MMC. e. Click Action (from the menu choices on top of the MMC). f. Select Update Mirror from the drop-down menu. Note _____ The Update Mirror option is grayed out if no mirror is configured. Result: The Update Mirror operation is initiated and a rolling snapshot of the virtual disk is created. After the snapshot has been created on the mirrored source volume, SnapDrive automatically updates the mirrored destination volume.

Connecting to destination volumes

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 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 restore of the virtual disk must happen from the most recent snapshot containing a valid image of that virtual disk.

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

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

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

Connecting to a mirrored destination volume

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

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

Step	Action	
2	Perform the following actions to rescan disks: - Expand the Storage option in the left panel of the MMC, if it is not expanded already. - Double-click Disk Management. - Click Action (from the menu choices on top of the MMC). - Select Rescan Disks from the drop-down menu.	
3	Connect to the mirrored virtual disk on the SnapMirror destination filer. See “Connecting virtual disks” on page 156 for more information.	
4	If you agree to breaking the mirror on the destination volume and perform a single file SnapRestore, click Yes in the Connect Disk dialog box. Note _____ You will need to perform this step only if the destination volume is not in “broken” state.	
5	If...	Then...
	The virtual disk will belong to a single system	Select Dedicated Drive, click Next, then skip to Step 7 .
	The virtual disk will be a Windows cluster resource	Select Shared Drive, then click Next.
6	Verify that you want the disk to be shared by the nodes listed, then click Next.	
7	In the Virtual Disk Properties Window, examine the properties of the virtual disk and assign a drive letter, then click Next.	
8	In the Select HBA window, select the port and node names of your HBA.	

Step	Action	
9	If...	Then...
	The virtual disk will belong to a single system	Go to Step 10 .
	The virtual disk 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”) panel. Details appear in the right panel.	

SnapMirror disaster recovery

About this section

This section describes how to bring a system back online using virtual disks that were replicated to SnapMirror destination volumes.

Note

These destination volumes can be on the same filer as the source volume, or on a different filer.

Recovering a virtual disk from a mirrored volume

You can use SnapMirror to replicate onto a volume virtual disks from one or more filers. When you use SnapMirror to replicate volumes from one filer to another, the destination filer can be in a different geographical location.

Configuring a source volume

For information about creating filer volumes, see [“Creating a filer volume”](#) on page 40. See the *Data ONTAP Data Protection Guide* for more information about data replication using SnapMirror.

Note

The CIFS shares on the destination filer should match those on the source filer. Typically these shares might be named C\$, D\$, and E\$.

Example: “share 1” for “qtree 1” on the source volume and “share 1” on “qtree 1” on the destination volume are both named “F\$.”

About this appendix This appendix details the SnapDrive operations you can execute through the `sdcli` command-line utility, which enables you to enter SnapDrive commands individually or through automation scripts.

Topics in this appendix This appendix details the `sdcli` command categories:

- ◆ iSCSI connection commands
- ◆ Virtual disk commands
- ◆ Multipathing commands
- ◆ Snapshot commands

Understanding `sdcli` commands The `sdcli` commands consist of three input parameters (for example, `sdcli snap create`), which must be specified in the correct order, as per usage, 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.

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\SnapDrive\
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: sdcli disk disconnect -d R Alternatively, enter the name and path of the automation script you want to run. Example: C:\SnapDrive Scripts\disconnect_R_from_host4.bat

Common command switches

Some or all of the sdcli commands share the command-line switches listed in the following table.

Switch	Comment
-d	The drive letter assigned to the virtual disk. If sdcli can't find the drive letter specified through the -d switch, it displays a list of all virtual disks connected to the host. Example: -d j indicates that the virtual disk is mapped to the J: drive on the host.
-D	A list of drive letters separated by spaces. Example: -D j k l indicates that the command applies to the J:, K:, and L: drives.
-dtype	The drive type (shared or dedicated).

Switch	Comment
<i>-e</i>	The name of an existing MSCS resource group, which is required only if the virtual disk is shared among MSCS nodes.
<i>-i</i>	The initiator name. ◆ For FCP, the initiator name is the WWPN (World Wide Port Node) 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 Block Access Management Guide.
<i>-I</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 <i>lputilnt.exe</i> utility supplied with your NetApp FCP HBA Attach Kit. After you launch <i>lputilnt.exe</i>, 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 <i>NodeMachineName</i> in the cluster applies to two of the available initiator WWPNs; the other <i>NodeMachineName</i> applies to the remaining pair of initiator WWPNs.
<i>-ID</i>	An MPIO path ID. For details, see “ Understanding MPIO path IDs ” on page 233.
<i>-m</i>	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 <i>-m</i> switch when running an <i>sdcli</i> command on the local host.
<i>-n</i>	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.
<i>-np</i>	The IP address and port of the network portal on the iSCSI connection target.
<i>-p</i>	The UNC path to the location of the virtual disk on the filer. This string takes the following form: <i>\\filename\sharename\virtualdiskfilename{.lun .vld}</i>

Switch	Comment
-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 tables of supported operations that follow.

iSCSI connection commands

Supported operations

The sdcli utility supports the following iSCSI connection operations: connect, disconnect, and list.

Operation
<code>iscsi_target connect</code> connects an iSCSI target using the specified network portal. Note_____ Depending on the initiator driver implementation, all other portals that the target is available through could also be used for the connection. _____ Syntax: <pre>sdcli iscsi_target connect -i InitiatorName -t TargetName -np IPAddress IPPort [-c CHAPName CHAPPassword]</pre> Example: <pre>sdcli iscsi_target connect -i iqn.1991-05.com.microsoft:node2 -t iqn.1992.08.com.netapp:sn33604307 -np 168.34.50.52 3260</pre> The preceding example creates an iSCSI connection between the specified iSCSI initiator and the specified iSCSI target.
<code>iscsi_target disconnect</code> disconnects the specified iSCSI initiator from the specified iSCSI target on all portals. Syntax: <pre>sdcli iscsi_target disconnect -i InitiatorName -t TargetName</pre> Example: <pre>sdcli iscsi_target disconnect -i iqn.1991-05.com.microsoft:node2 -t iqn.1992.08.com.netapp:sn.33604307</pre> The preceding example disconnects the specified iSCSI initiator from the specified iSCSI target.

Operation

`iscsi_target list` displays a list of all iSCSI targets. For each target, the command displays all portals the target is available through or connected to.

Syntax:

```
sdcli iscsi_target list {-f FilerName | -i InitiatorPortName}
```

-f displays all targets on the specified filer.

-i displays all targets the specified initiator is connected to.

Example:

```
sdcli iscsi_target list -f filer2
```

The preceding example lists all the iSCSI targets on the filer2 filer, as well as all portals those targets are available through or connected to.

```
sdcli iscsi_target list -i iqn.1991-05.com.microsoft:node2
```

The preceding example lists all the iSCSI targets that the specified initiator is connected to, as well as all portals those targets are available through or connected to.

Virtual disk commands

Supported operations

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 DriveLetter -z DriveSize -I NodeMachineName InitiatorWWPN [[NodeMachineName InitiatorWWPN] ...] -dtype {shared dedicated} {[-e ResourceGroupName] [-n ResourceGroupName ResourceGroupDesc]}</pre> Examples: <pre>sdcli disk create -dtype dedicated -z 1024 -p \\filer2\sd_vds_only\mktng.lun -d R -I host3 10:00:00:00:C9:2B:FD:12</pre> The preceding example creates a dedicated, 1-GB virtual disk named mktng.lun in the filer2 volume named sd_vds_only. Next, it connects this virtual disk to the host as drive R:. <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 host4 (the local machine running the sdcli command) and maps it to drive R:, using a pair of initiators. This command also creates MPIO paths through host5, which is partnered with host4 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 DriveLetter -I NodeMachineName  
InitiatorWWPN [[NodeMachineName InitiatorWWPN] ...] -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]
```

`-l` 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 monitored with the Windows Performance Monitor (perfmon).

Syntax:

```
sdcli disk delete [-m MachineName] {-p UNCpath | -d DriveLetter}
```

Example:

```
sdcli disk delete -p \\133.25.61.62\sd_vds_only\mktng.lun
```

The preceding example deletes the virtual disk mktng.lun from the sd_vds_only volume on the filer identified by the IP address 133.25.61.62.

disk disconnect disconnects a virtual disk from the host. The virtual disk must be connected (mapped to a Windows drive letter) for the command to succeed.

Note

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

Syntax:

```
sdcli disk disconnect [-m MachineName] {-p UNCpath | -d DriveLetter} [-f]
```

Caution

The -f switch causes the virtual disk to be forcibly unmounted, even if an application or the Windows operating system is using it. Therefore, use this feature with extreme care.

Examples:

```
sdcli disk disconnect -d z
```

The preceding example disconnects the virtual disk mapped to the drive letter “Z:” on the SnapDrive host running the sdcli command.

```
sdcli disk disconnect -p \\filer2\sd_vds_only\mktng.lun -f
```

The preceding example forces disconnection of the virtual disk mktng.lun, which is in the sd_vds_only volume on filer2. Because the -f switch is being used, all open files in the virtual disk might be lost or corrupted.

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 DriveLetter} -z DriveSizeIncrement
```

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.)

`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, and virtualdiskfilename)
- ◆ Disk serial number
- ◆ Whether the disk is dedicated or shared
- ◆ Disk size (in megabytes)
- ◆ Mount point (the drive letter to which the virtual disk is mapped on the host)

Multipathing commands

Supported operations

The `sdc li` 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 `sdc li`, *pathID* specifies the virtual path created by mapping a virtual disk on the filer to an initiator port on the host. This number, which is generated by the Windows enumerator and also known as a DSM Path, is created from four consecutive hex numbers.

Example: 0x4000d07

- ◆ The SCSI port number representing the initiator on the host is 04, but because it begins the string, and because it is between 01 and 09, inclusive, the leading 0 is omitted, and the value is simply represented as 4. (When the value is between 0xA and 0xF, inclusive, the leading 0 is not omitted.)
- ◆ The host bus number is 00.
- ◆ The “target” address ID for the target port is 0d.
- ◆ The LUN number, 07, which 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
 - ◆ Target Slot/Port
 - ◆ Initiator WWPN
 - ◆ Target WWPN.
-

Supported MPIO commands

The table in this section lists the MPIO-related operations supported by `sdcli`: activate, add, disable, enable, list, remove, and version.

Operation
<code>path activate</code> directs I/O through the specified path and causes the currently active path to become passive. (This command can only be performed on a passive path.) Syntax: <pre>sdcli path activate [-m <i>MachineName</i>] -ID <i>PathID</i></pre> Example: <pre>sdcli path activate -ID</pre> The preceding example activates path 0x4000d07 and makes passive whatever path was active when the command was run.
<code>path add</code> creates a new virtual path from the initiator on the host to the virtual disk on the filer. Syntax: <pre>sdcli path add [-m <i>MachineName</i>] {-p <i>UNCpath</i> -d <i>DriveLetter</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 <code>mktng.lun</code> on the <code>sd_vds_only</code> volume on <code>filer2</code>, assigning the new path to the initiator port associated with WWPN 10:00:00:00:c9:2b:fd:13.
<code>path disable</code> disables the specified path. (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: <pre>sdcli path enable [-m <i>MachineName</i>] -ID <i>PathID</i></pre> Example: <pre>sdcli path enable -ID 0x4000d07</pre> The preceding example changes the status of path 0x4000d07 from disabled to enabled.
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. Syntax: <pre>sdcli path list [-m <i>MachineName</i>] {-p <i>UNCpath</i> -d <i>DriveLetter</i>}</pre> Example: <pre>sdcli path list -d z</pre> The preceding example lists all the MPIO paths specified for the virtual disk mapped to Z: on the local host.
path remove deletes the specified mapping (virtual path) between the LUN on the filer and the initiator on the host. Syntax: <pre>sdcli path remove [-m <i>MachineName</i>] {-p <i>UNCpath</i> -d <i>DriveLetter</i>} -i <i>InitiatorPortName</i></pre> Example: <pre>sdcli path remove -p \\filer2\sd_vds_only\mktng.lun -i 10:00:00:00:c9:2b:fd:13</pre> 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.
path version indicates whether NTAPDSM is installed on the specified system. Syntax: <pre>sdcli path version [-m <i>MachineName</i>]</pre> Example: <pre>sdcli path version</pre> The preceding example returns information about whether NTAPDSM is installed on the local host.

Snapshot commands

Supported operations

The following table lists the snapshot-related operations supported by `sdcli`: create, delete, list, mount, rename, restore, unmount, and update mirror.

Operation
<code>sdcli snap create</code> creates a new snapshot of the specified virtual disks on the SnapDrive system. Syntax: <pre>sdcli snap create [-m MachineName] -s SnapshotName -D DriveLetterList [. . .] [-x]</pre> <code>-x</code> causes snapshots to be created only for the drives specified by the <code>-D</code> switch. Otherwise, snapshots are created for all the disks on the filer volumes used by the listed drives. Example: <pre>sdcli snap create -s Jun_13_03 -D j k l</pre> The preceding example creates a snapshot named <code>Jun_13_03</code> for each volume containing one or more of the virtual disks mapped to the specified drives (that is, J:, K:, and L:). The snapshots created are consistent for all virtual disks contained by those volumes.
<code>sdcli snap delete</code> deletes an existing snapshot. Note You must make sure that the virtual disk whose snapshot you are deleting is not monitored with the Windows Performance Monitor (<code>perfmon</code>). Syntax: <pre>sdcli snap delete [-m MachineName] -s SnapshotName -D DriveLetterList [. . .]</pre> Example: <pre>sdcli snap delete -s Jun_13_03 -D k</pre> The preceding example deletes the snapshot named <code>Jun_13_03</code> that is associated with the virtual disk mapped to K: on the local host.

Operation
snap list lists all the snapshots that exist for the specified virtual disk. <pre>sdcli snap list [-m <i>MachineName</i>] -d <i>DriveLetter</i></pre> Example: <pre>sdcli snap list -d j</pre> The preceding example displays all the snapshots that exist for the volume containing the virtual disk mapped to “J:” on the local host.
snap mount mounts a snapshot of a virtual disk. Snapshots are always mounted in read/write mode. Syntax: <pre>sdcli snap mount [-m <i>MachineName</i>] [-r <i>LiveMachineName</i>] -k <i>LiveDriveLetter</i> -s <i>SnapshotName</i> -d <i>DriveLetter</i></pre> -r 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. -k refers to the drive letter assigned to the virtual disk in the active file system. Example: <pre>sdcli snap mount -r host3 -k j -s Jun_13_03 -d t</pre> The preceding example maps the snapshot named Jun_13_03 to drive T: on the local host. This snapshot represents a point-in-time image of the virtual disk mapped to J: on host3.
snap rename enables you to change the name of an existing snapshot. Syntax: <pre>sdcli snap rename [-m <i>MachineName</i>] -d <i>DriveLetter</i> -o <i>OldSnapshotName</i> -n <i>NewSnapshotName</i></pre> Example: <pre>sdcli snap rename -d j -o Jun_13_03 -n last_known_good</pre> The preceding example changes the name of the June_13_03 snapshot 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.

Note

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

Syntax:

```
sdcli snap restore [-m MachineName] -d DriveLetter -s SnapshotName
```

Example:

```
sdcli snap restore -d l -s Jun_13_03
```

The preceding example restores the virtual disk mapped to L: on the local host to its state when the snapshot named Jun_13_03 was taken.

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

Note

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

Syntax:

```
sdcli snap unmount [-m MachineName] -d DriveLetter [-f]
```

Caution

The `-f` argument forcibly unmounts the virtual disk, even if it is in use by an application or Windows. Such a forced operation could cause data loss, so use it with extreme caution.

Examples:

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

The preceding example disconnects the snapshot mapped to K: on the local host.

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

The preceding example forces disconnection of the snapshot mapped to the K: drive on the local host.

Operation

`snap update_mirror` updates the virtual disk to a SnapMirror destination volume residing on the same or a different filer.

Syntax:

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

Example:

```
sdcli snap update_mirror -d l
```

The preceding example updates the SnapMirror destination for the virtual disk mapped to the L: drive on the local host. You don't need to specify the location of the SnapMirror destination because that information was entered when mirroring was set up for the virtual disk.

About this appendix This appendix summarizes the various SnapDrive requirements and recommendations mentioned elsewhere in this document.

Assumed competence

To install and administer SnapDrive, you should be familiar with the following:

- ◆ The NFS and CIFS protocols, as applicable to file sharing and file transfers
- ◆ FCP, if you plan to create FCP-type virtual disks on a SnapDrive SAN
- ◆ SCSI, if you plan to create iSCSI-type virtual disks on a SnapDrive SAN
- ◆ Basic network functions and operations
- ◆ Windows 2000 server management, if your hosts have Windows 2000 installed
- ◆ Windows Server 2003 management, if your hosts have Windows Server 2003 installed
- ◆ Network Appliance filer management

Host requirements

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

Component	Requirement
CPU	500 MHz Pentium® III
Memory	256 MB RAM
HBAs	Emulex® LP9002L-F2 host bus adapters (for FCP)
Operating system	Windows 2000 Server (with SP3 or SP4) Windows 2000 Advanced Server (with SP3 or SP4) Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition in an MSCS configuration with hotfix 824354

Component	Requirement
Microsoft Windows 2000 Post Service Pack 3 hotfixes	816990, 822831, and 815616/325040 (must be installed with SP3) 815198 (must be installed with SP3 if MPIO is deployed) 822831 (must be installed with SP4)

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

Interface drivers: Obtain the latest firmware and drivers for the HBAs and NICs you are using. This ensures high network bandwidth and ease of configuration.

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

Service Packs: You must install SP3 or SP4 before installing SnapDrive on a Windows 2000 system.

Hotfixes: You must install the following hotfixes on your hosts before you install SnapDrive. You must request these hotfixes directly from Microsoft Product Support Services at <http://support.microsoft.com>.

- ◆ If your Windows 2000 host is running SP3, you must install hotfixes 816990, 822831, and 815616/325040.
- ◆ If your Windows 2000 host is running SP4, you must install hotfix 822831.
- ◆ If your host is running MPIO on either Windows 2000 Server or Windows Advanced Server with SP3, you must install hotfixes 816990, 815616/325040, and 815198.
- ◆ If your host is running Windows Server 2003 Enterprise Edition in an MSCS configuration, you must install hotfix 824354.

Name resolution: Make sure that name resolution (for example, DNS, WINS) is enabled on the Windows host such that SnapDrive can resolve a filer hostname to a reachable IP address, and an IP address to a hostname.

Filer requirements

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

Component	Minimum requirement
Operating system	Data ONTAP 6.4.2
Licenses	◆ iSCSI, if you plan to use iSCSI-accessed virtual disks ◆ FCP, if you plan to use FCP-accessed virtual disks ◆ SnapRestore, which is required only for restoring virtual disks from snapshots ◆ SnapMirror, 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 virtual disks. If you also want *full-featured, direct CIFS access* to a particular filer, you must install a separate CIFS license on that filer.

SnapDrive service account requirements

The SnapDrive service account, which is used to administer all SnapDrive functions, must be set up with the following access permissions. (For details, see “[Preparing the SnapDrive service account](#)” on page 48.)

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

Note

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

- ◆ The service account must have administrator privileges on both the filer and host.
- ◆ The service account must be a domain account.

- ◆ The host and filer must belong to the same domain as the service account, or belong to domains that have direct or indirect trust relationships with the domain to which the service account belongs.
- ◆ The service account must have “administrator” access to the filer.
- ◆ The service account must have rsh (Remote Shell access) to the filer.
- ◆ The host must have access to the filer volumes on which virtual disks are stored.

Volume and filer options

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

Note

Network Appliance *strongly recommends* that you do not change these values.

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

Note

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

Cluster recommendations

Network Appliance recommends that you observe the following practices when creating Windows clusters to host SnapDrive:

- ◆ Place the host and filer in the same broadcast domain.
- ◆ Segregate host-filer data traffic from data-center traffic whenever possible.
- ◆ Segregate internal cluster traffic from both host-filer traffic and data-center traffic, whenever possible.

SnapDrive-specific limitations

SnapDrive has the following limitations:

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

SnapDrive-specific cautions and recommendations

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

- ◆ Use SnapDrive to create and manage all the virtual disks on your filer.
- ◆ *Never* set the space reservation setting on the filer to Off.
- ◆ Do set the snap reserve setting on the filer to 0%.
- ◆ Place all virtual disks connected to the same host on a dedicated volume accessible by just that host.
- ◆ Unless you can be sure that name resolution publishes only the filer interface you intend, configure each network interface by *IP address*, rather than by name. Alternatively, prevent network interfaces from publishing to WINS by entering the following command at the filer prompt:

ifconfig *interfacename* -wins

interfacename is the name of the filer interface, such as e0, e4, or e4a.

- ◆ If you use snapshots, you cannot use the entire space on a filer volume to store your virtual disk. The filer volume hosting the virtual disk must be at least twice the combined size of all the virtual disks on the volume.
- ◆ Do not create any LUNs in /vol/vol0.
This volume is used by Data ONTAP to administer the filer and should not be used to contain any LUNs.

SnapDrive user interfaces

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

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

Note

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

- ❖ The GUI interface of the SnapDrive plug-in
 - ❖ Sdcli.exe commands in the Windows command-line environment.
-
- ◆ *Remote Administration* refers to a connection initiated by selecting Action > “Connect to another computer...” in the Computer Management Console of a Windows computer on the same network as the SnapDrive host. This type of session enables you to manage the host as if you were using a console directly attached to the host.
 - ◆ *Terminal Service* refers to the optional Windows component that allows remote desktop administration.
Be aware of the following drawbacks to using Terminal Service sessions:
 - ❖ 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.
 - ❖ The list of available drive letters may not be up-to-date when you map a newly-created virtual disk in the SnapDrive Create Disk wizard, making

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

If you encounter these problems, log off the Terminal Service session and then log on again (or preferably use the system console or a remote administration session instead). The newly created or disconnected disks should 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 interface
Creating a CIFS share	◆ FilerView ◆ Filer console ◆ Telnet session to the filer ◆ Remote Management session to the filer
Creating and managing volumes and qtrees	◆ FilerView ◆ Filer console ◆ Telnet session to the filer
SnapDrive-related SnapMirror operations	◆ FilerView ◆ Filer console ◆ Telnet session to the filer
Creating and managing virtual disks	◆ Host console ◆ Remote Management session to the host

Index

Symbols

/etc/hosts file 49

/etc/hosts.equiv file 49

A

abnormal disconnect (of virtual disk) 165

access protocols 12

access types and requirements for virtual disks (LUNs) 23

accessing virtual disks 12

administration, remote 174

applications, stopping for VLD conversion 71

archives, restoring from 199

archiving, snapshots 199

asynchronous replication 212

authentication, pass-through 8

Autosupport (filer), enabling 175

B

BUILTIN/administrators group 48

C

cautions and recommendations for SnapDrive 38

changing path states, MPIO 209

changing SnapDrive service account password 48

CIFS

- limited functionality supplied with FCP and iSCSI license 37

- setup 43

cifs setup command 43

CIFS shares

- cifs setup command 43

- creating 43

cluster

- See also* Windows cluster

- "private" network 27

- Cluster Service (MSCS), definition of 2

- converting VLDs in cluster groups 92

- FCP configurations 30

- iSCSI configurations 27

- MPIO configurations 32

- support in SnapDrive 5

commands, sdcli. *See* sdcli commands

configurations

- choosing 23

- FCP 29

- guidelines 23

- iSCSI 25

- multipathing (MPIO) 32, 204

configuring, filer volumes 40

connect

- to (mirrored) destination volumes 218

- to a virtual disk 156

- to virtual disks (LUNs) in a snapshot 187

connection, iSCSI

- details 126

- disconnecting 125

- establishing 121

- ways to establish 120

converting

- VLD quorum disk 93

- VLDs for MSCS 89

- VLDs in a cluster group 92

- VLDs to LUNs 73

create

- iSCSI connection 121

- shared virtual disks (on a Windows cluster)
141

- snapshots using SnapDrive 180, 181

- virtual disks 131

creating a CIFS share 43

creating a filer volume 40

creating a qtree 42

crossover FCP cable 29

D

Data ONTAP, required version 36

data restore from snapshots 194

dedicated filer volume required for virtual disks (LUNs) 40

- delete
 - a virtual disk 167
 - snapshots 197
- details of iSCSI connections 126
- df -r (filer command) 16
- disaster recovery with SnapMirror 221
- disconnect
 - a virtual disk 164
 - forced (of virtual disk) 165
 - from an iSCSI target 125
- disks
 - hot spare 14
 - virtual 130
- documentation
 - Data ONTAP 43
 - filer 36
 - obtaining 22
 - virtual disk protocols 22
- drive letters, list incorrect when viewed via Terminal Service 246
- drivers, obtaining 35
- dump command 199

E

- email notification, setting up 175
- examine, virtual disk properties 172
- expand
 - a quorum disk 171
 - virtual disks 168, 169

F

- failover
 - definition 2
 - NetApp cluster 6
- FCP
 - adapters 33
 - configurations 29
 - crossover cable 29
 - documentation 22
 - Host Bus Adapter (HBA) 22
 - initiator 7
 - installing 101
 - license required on filer 36
 - MPIO configurations 32

- obtaining firmware and driver 35
- requirements for virtual disks 24
- single-host, single-filer configurations 29
- switch 30, 32
- switched configuration 30
- uninstalling driver 115
- windows cluster configurations 30
- feature availability by virtual disk access type 24
- features, updating mirrors 216
- Fibre Channel Protocol *See* FCP
- fields
 - iSCSI Initiator Name 126
 - iSCSI Target Name 126
 - Number of LUNs 126
 - Target Portal IP Address 126
 - Target Portal Port 126
- file
 - /etc/hosts 49
 - /etc/hosts.equiv 49
- file system 2
- filer
 - /etc/hosts and /etc/hosts.equiv files 49
 - administrator access required for SnapDrive 48
 - BUILTIN/administrators group 48
 - checking licenses 37
 - creating a volume 40
 - dedicated volume required for LUNs 40
 - definition 2
 - df -r command 16
 - documentation 36
 - guidelines for creating volumes 39
 - interaction with virtual disks 11
 - licenses required 36
 - options set by SnapDrive 37
 - preparing 36
 - requirements 36
 - resetting the snap reserve 47
 - rsh (remote shell) access required 48
 - settings for SnapDrive 15
 - upgrading 112
 - user interfaces 246
 - volume preparation 39
 - Windows domain account 48
- filer cluster
 - FCP configurations 30

- iSCSI configurations 27
- MPIO configurations 32
- filer console, definition 246
- FilerView
 - checking filer licenses 37
 - creating a volume 40
 - definition 246
 - modifying /etc/hosts and /etc/hosts.equiv files 49
 - opening a session 40, 42, 46
 - setting snap reserve 47
- firmware, obtaining 35
- forcing disconnect (of a virtual disk) 165

G

- GbE (Gigabit Ethernet)
 - iSCSI configurations 25
 - switched configuration 26
- guidelines
 - for choosing SnapDrive configuration 23
 - for creating filer volumes 39

H

- host 2
- Host Bus Adapter (HBA)
 - definition of 3
 - documentation, for FCP 22
- host console
 - definition 246
 - error messages not seen in Terminal Service session 246
- hot spare disks 14
- hotfixes, Post Service Pack 3 requirements 24

I

- initiator
 - definition of 3
 - obtaining iSCSI 35
- installing
 - FCP 101
 - first time 100
 - iSCSI 101
 - SnapDrive components 104

- iSCSI
 - cluster configurations 27
 - configurations 25
 - initiator 7
 - installing 101
 - license required on filer 36
 - obtaining software 35
 - single-host, single-filer configurations 25
 - uninstalling 116

- iSCSI connections
 - creating 121
 - details 126
 - disconnecting from a target 125
 - establishing 121
 - ways to establish 120
- iSCSI Initiator Name field 126
- iSCSI protocol
 - documentation 22
- iSCSI Target Name field 126
- iSCSI-accessed virtual disks
 - requirements 24

L

- latency, minimizing with GbE crossover cable 25
- licenses
 - checking with FilerView 37
 - required on filer 36
- limitations
 - LUN cloning 38
 - MultiStore 38
 - qtree quotas. 38
 - SnapDrive 38
- Logical Unit Numbers. *See* LUNs
- LUNs
 - See also* virtual disks
 - access types and requirements 23
 - cloning not supported 38
 - conversion to 73
 - dedicated filer volume required 40
 - definition of
 - not visible when created via Terminal Service 246
 - snap reserve setting on filer 47
 - with MultiStore, limited to vfiler0 38

LUN-type virtual disks, definition 3

M

modify, virtual disk properties 172

Monitor Time Interval property 172

mpdev.sys 202

MPIO

- accessing using MMC 206

- active path 202

- changing path states 209

- configurations 32

- drivers 7

- enabling 204

- overview 202

- passive path 202

- path IDs 233

- path states 209

- required hotfix 35, 242

- requirements 24

- requirements, hardware and software 202

- supported topologies 204

- uninstalling 113

mpio.sys 202

MS Exchange, stopping for VLD conversion 70

MS SQL Server, stopping for VLD conversion 70

MSCS

- See also* Windows cluster

- converting VLDs 89

- definition 2

- FCP configurations 30

- iSCSI configurations 27

- MPIO configurations 32

msspsfltr.sys 202

multipathing. *See* MPIO

MultiStore, SnapDrive limitation 38

N

NDMP-based backup application 199

NetApp Windows Attach Kit for FCP

- documentation 22

Network Interface Card (NIC), definition of 3

network, "private" for internal cluster traffic 27

notification settings, for SnapDrive 175

ntapdsm.sys 202

NTFS 2

Number of LUNs field 126

O

obtaining firmware and drivers 35

operating system

- filer requirement 36

- required on Windows host 34

options, snap reserve 47

P

pass-through authentication 8

password, changing for SnapDrive service account 48

path states, MPIO 209

properties, modifying virtual disk 172

protocols, connection 12

Q

qtrees

- creating 42

- SnapDrive limitation 38

quorum

- converting to LUN 93

- creating a virtual disk as a 142

- expanding 171

R

read/write mode, connecting to snapshots in 187

recommendations

- and cautions for using SnapDrive 38

- for configuring filer volumes 40

- snap reserve 47

recovering, a virtual disk 221

recovery, from mirrored volume 221

remote administration

- definition of 246

- of SnapDrive 174

remote shell. *See* rsh

replication

- asynchronous 212

- initiating 216

- SnapMirror 214
 - upon snapshot creation 214
 - using rolling snapshots 214
- requirements
 - administrator access to filer 48
 - Data ONTAP 36
 - filer 36
 - filer licenses 36
 - for SnapMirror 212
 - for snapshots 181
 - matrix for SnapDrive, protocols, Windows OS 23
 - operating system 34
 - rsh (remote shell) access to filer 48
 - SnapDrive service access to Windows 48
 - SnapDrive service account 48
 - Windows domain 48
 - Windows host 34
- restore
 - from snapshots 194
 - virtual disks from archives 199
- rolling snapshots
 - and replication 214
 - described 214
 - management of 214
 - naming 215
- rsh (remote shell)
 - access to filer 48
 - enabling 49
 - requirements 48
- rules
 - for connecting to virtual disks 156
 - for creating virtual disks 131
 - for managing virtual disks 130
 - for snapshots 187

S

- SAN (Storage Area Network), definition of 4
- sdcli commands
 - about understanding 223
 - executing 224
 - for iSCSI connection 227
 - for snapshots 236
 - multipathing commands 233

- switches (options) available for 224
- disk connect 230
- disk convert 230
- disk create 229
- disk delete 231
- disk disconnect 231
- disk expand 232
- disk list 232
- iscsi_target connect 227
- iscsi_target disconnect 227
- iscsi_target list 228
- map fcp port 210
- path activate 210, 234
- path add 210, 234
- path disable 210, 234
- path enable 210, 235
- path list 235
- path remove 210, 235
- path version 235
- snap create 236
- snap delete 236
- snap list 237
- snap mount 237
- snap rename 237
- snap restore 238
- snap unmount 238
- snap update_mirror 239
- service account
 - for SnapDrive 48
 - requirements 48
 - Windows domain 48
- service packs
 - requirements 24
 - SP3, SP4 24
- single-homed configuration, using GbE switch 26
- single-host, single-filer configurations
 - FCP 29
 - iSCSI 25
- snap reserve, recommended setting 16, 47
- SnapDrive
 - administrator access to filer required 48
 - capabilities 5
 - cautions and recommendations 38
 - command-line interface 6
 - command-line interface reference 223

- competencies assumed 241
- components 6
- configuring filer volumes 40
- feature availability by virtual disk access type and OS 24
- feature support, requirements 23
- filer options set automatically 37
- installing components 104
- limitations 38
- preparing to install 21
- selecting configurations 23
- service account 48
- snap reserve on filer 47
- uninstalling 113
- user interfaces 246
- SnapMirror
 - asynchronous replication 212
 - connecting to (mirrored) destination volumes 218
 - described 212
 - disaster recovery 221
 - initiating replication 216
 - license required on filer 36
 - overview 212
 - replication 214
 - requirements for using with SnapDrive 212
 - rolling snapshots 214
 - Update Mirror feature 216
 - using with SnapDrive 211
 - virtual disk recovery 221
- SnapRestore, licence required on filer 36
- snapshots
 - archival 199
 - connecting to virtual disks (LUNs) 188
 - definition 4
 - deleting 197
 - described 178
 - effect on disk space 17
 - how to create 181
 - reason for creating 180
 - replication upon creation of 214
 - requisites for 181
 - restoring from 194
 - restrictions on creating 180
 - rolling 214, 215
 - space required 15
 - source volume, configuring 221
 - SP3, additional hotfixes required 24
 - SP4, feature support 24
 - space reservation
 - example 16
 - filer setting 15
 - overview 16
 - states, path (MPIO) 209
 - support matrix for SnapDrive features, protocols, and host OS 24
- T**
 - target 4
 - Target Portal IP Address field 126
 - Target Portal Port field 126
 - Telnet
 - description of 246
 - opening a session 43
 - using to access a filer 42
 - Terminal Service 246
 - definition 246
 - drawbacks 246
 - workaround for problems 247
- U**
 - uninstalling
 - FCP driver 115
 - iSCSI initiator 116
 - SnapDrive and MPIO 113
 - SnapDrive components 113
 - VLD driver 113
 - Update Mirror feature 216
 - upgrading
 - cluster with VLDs 60
 - cluster without VLDs 96
 - filer 112
 - procedures 56
 - single system with VLDs 65
 - single system without VLDs 99
 - to Windows 2003 58
 - user interfaces
 - for SnapDrive and the filer 246
 - recommended for various operations 247

V

vFilers (virtual filers)

- SnapDrive limitations 38
- using with SnapDrive 5

view

- details of an iSCSI connection 126
- properties of virtual disks 172

virtual disks

- access types and requirements 23
 - capabilities 11
 - connecting to 156
 - converting connected 73
 - converting for MSCS 89
 - converting unconnected 81
 - creating as a quorum 142
 - creating shared 141, 153
 - data access overview 12
 - dedicated filer volume required 40
 - deleting 167
 - disconnecting 164
 - documentation about protocols 22
 - expanding 169
 - expanding quorum disks 171
 - filer interaction 11
 - filer options set on creation and connection 37
 - how to create 131
 - limitations 11
 - LUN-type, definition 3
 - managing, rules about 130
 - Monitor Time Interval property 172
 - not visible when created via Terminal Service 246
 - properties 172
 - recovering, from SnapMirrored volume 221
 - rules for creating 131
 - snap reserve setting on filer 47
 - VLD-type, definition 4
 - Windows interaction 11
- virtual filers (vFilers), using with SnapDrive 5
- VLD driver, uninstalling 113
- VLDs
- converting connected 73
 - converting for MSCS 89
 - converting in cluster group 92

- converting quorum disk 93
- converting to LUNs 73
- converting unconnected 81

volume

- configuring source 221
- connecting to (mirrored) destination 218
- contents 15
- creating 40
- definition 4
- guidelines for creating 39
- options set by SnapDrive 37
- preparation 39
- recommendations for configuring 40
- recovery, from mirrored 221
- resetting snap reserve 47
- restricted to single host 40
- sizing 15

W

WAFL 2

Windows 2000

- Advanced Server requirements and feature support 24
- Server requirements and feature support 24

Windows 2000 Server cluster. *See* Windows cluster

Windows cluster

- creating a shared virtual disk 141
- creating a virtual disk as a quorum 142
- definition of 4
- FCP configurations 30
- iSCSI configurations 27
- MPIO configurations 32

Windows domain, requirements 48

Windows host

- administrator access required 48
- preparing 34
- requirements 34

Windows operating system, requirements 24

Windows Server 2003 cluster. *See* Windows cluster

Windows Server 2003, supported versions and feature support 24

workgroup mode authentication 8

