

SnapDrive™ 3.0

Installation and Administration Guide

Draft 1.0 (07/31/03)

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 210-00563
August, 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 European Union and Japan, and a trademark of Network Appliance, Inc. in the United States. 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, 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, NearStore, SecureAdmin, Serving Data by Design, Smart SAN, SnapCache, SnapDrive, SnapVault, vFiler, and Web Filer are trademarks of Network Appliance, Inc. in the United States.

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)
- ◆ Basic network functions and operations
- ◆ Windows® 2000 and Windows 2003 server management
- ◆ Network Appliance filer management

About filer command execution

You can enter filer commands in 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

Interface conventions

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

Table of Contents

	Preface	v
Chapter 1	Overview of SnapDrive	1
	SnapDrive terminology	2
	How SnapDrive works	4
	How virtual disks work	7
	Understanding filer storage	9
	Planning disk allocation	10
	Understanding volume size	11
Chapter 2	Preparing to Install SnapDrive.	17
	What to read	18
	Selecting a SnapDrive configuration	19
	Preparing hosts	29
	Preparing filers	32
	Preparing the SnapDrive service account.	44
Chapter 3	Installing or Updating SnapDrive	51
	Upgrading to SnapDrive 3.0	52
	Upgrading to SnapDrive 3.0 and converting VLD-type virtual disks	53
	SnapDrive 3.0 upgrade and conversion process	54
	VLD to LUN conversion.	59
	Upgrading to SnapDrive 3.0 if you have no VLD-type virtual disks	63
	Uninstalling old components	64
	Installing SnapDrive for the first time	68
	Installing the driver	69
	Installing the new SnapDrive components	71
Chapter 4	Creating Virtual Disks	77
	About virtual disk management	78

	Creating a virtual disk	79
	Creating a virtual disk on a new Windows 2000 cluster	90
	Creating a virtual disk quorum on a new Windows cluster	91
	Creating a virtual disk as quorum on an existing Windows cluster	94
	Creating a virtual disk on an existing Windows 2000 cluster	95
Chapter 5	Managing Virtual Disks.	97
	Connecting virtual disks	98
	Disconnecting virtual disks	106
	Expanding virtual disks	109
	Virtual disk properties	112
	Administering SnapDrive remotely	114
	Enabling SnapDrive notification	116
Chapter 6	SnapDrive Snapshots	119
	How snapshots work	120
	Creating snapshots	122
	Connecting to snapshots	126
	Restoring virtual disks from snapshots	129
	Deleting snapshots	131
	Archiving snapshots	132
Chapter 7	Multipathing	133
	Multipathing overview	134
	MPIO setup	136
	MPIO path management	138
Chapter 8	Using SnapMirror with SnapDrive	143
	SnapMirror overview	144
	SnapMirror replication	146
	Enabling SnapMirror	147

	Connecting to destination volumes	148
	SnapMirror disaster recovery	150
Appendix A	SnapDrive Command-line Reference	151
	iSCSI connection commands	155
	Virtual disk commands	157
	Multipathing commands	161
	Snapshot commands	164
Appendix B	SnapDrive Requirements and Recommendations.	167
	Index	177

About this chapter This chapter explains the SnapDrive technology.

Topics in this chapter

This chapter covers the following topics:

- ◆ “SnapDrive terminology” on page 2
- ◆ “How SnapDrive works” on page 4
- ◆ “How virtual disks work” on page 7
- ◆ “Understanding filer storage” on page 9

SnapDrive terminology

This document uses the following terms in *SnapDrive-specific* context:

- ◆ *Failover* refers to situations where a system component fails, and another component takes over its functions while the system continues to operate.
- ◆ *Filer* refers to any NetApp® storage appliance that supports the FCP (Fibre Channel Protocol), iSCSI, and/or GbE (Gigabit Ethernet) protocols.
- ◆ *File system* refers to NTFS, the native Windows 2000 and Windows 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* refers to a computer system that accesses storage on a filer. For this document, the host must be running the following software:
 - ❖ Windows 2000 Server (or Advanced Server for Windows-cluster configurations) or Windows 2003 Server (Standard Edition or Enterprise Edition)
 - ❖ SnapDrive 3.0
- ◆ NIC specifies one of three types of network interface card, each one of which SnapDrive requires under specific conditions:
 - ❖ *HBA (Host Bus Adapter)* refers to an adapter card supplied in the various NetApp attach kits for Windows and used to connect a host to a NetApp storage area network (SAN).

For FCP LUN-type, the Windows host must have a hardware HBA installed. For information about the HBAs supported for FCP LUN-types, see the SAN (FCP) Host Attach Kit 1.1 for Windows at <http://now.netapp.com>.

For iSCSI LUN-type, the Windows host does not require a hardware iSCSI HBA. Instead Microsoft's iSCSI initiator software is installed on the host. The software enables the iSCSI protocol over the host's standard Ethernet NIC, preferably GbE. For information about the iSCSI initiator software, see the iSCSI Host Support Kit at <http://now.netapp.com>.
 - ❖ *100Base-TX* is used interchangeably with *FastEthernet* to refer to any NIC compliant with the 100 Mbps FastEthernet protocol. These cards can connect hosts and filers to data-center switching fabrics, and they can carry internal "metadata" on the private "heartbeat" network used to monitor SAN health and performance. They can also be used for iSCSI-type LUNs, though GbE is strongly recommended.

- ◆ *Volume* refers to a functional unit of filer storage, based on one or more RAID groups, that is made available to a host.
- ◆ *Snapshot* refers to 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.
- ◆ *Block pointers* are used by a filer to locate the physical disk block on which data is stored.
- ◆ A *SAN (Storage Area Network)* is a storage complex composed of one or more filers and connected to a host within 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.
- ◆ When referring to the FCP and iSCSI environments, this document uses special terminology:
 - ❖ The HBA port on the host is referred to as an *initiator*.
 - ❖ The adapter on the filer storing the virtual disk is known as the *target*.
- ◆ *Virtual disk* refers to 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).
- ◆ *MSCS* (See *Windows clustering*).
- ◆ *MPIO (Multipath Input/Output for Storage Devices)* refers to the Microsoft® technology for implementing redundant paths between a host (initiator) and a target storage device. MPIO is available only for FCP-type virtual disks.
- ◆ *Windows clustering* (also referred to occasionally as *MSCS*) refers to a two- to a four-node host cluster, which is supported by certain SnapDrive configurations.

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 within a Windows 2000 and Windows 2003 environments.

SnapDrive manages virtual disks on a NetApp filer, making these virtual disks available as local disks on the Windows hosts. This allows the 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
 - ❖ 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 to create virtual filers (vfilers), SnapDrive can create, connect to, and manage 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:

- ◆ 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.

SnapDrive components

Some of the software components of SnapDrive are integrated in the SnapDrive software while others are available at the Network Appliance's NOW Web site at <http://now.netapp.com>. You must install all SnapDrive components before you can successfully use the software.

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. It

- ◆ Resides in the Windows 2000 and Windows 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

- ◆ Enter individual commands
- ◆ Run management scripts

Underlying SnapDrive service: This software interacts with software on the filer to facilitate virtual disk management for

- ◆ The host
- ◆ Applications running on the host.

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

iSCSI driver: This driver supports virtual disks within the iSCSI environment. It

- ◆ Supports an iSCSI connection between the host and the filer
- ◆ Is a SCSI/RAID controller on the host <<Reviewer:: is this correct??>>
- ◆ Does not include an HBA hardware component. Instead an iSCSI initiator software is installed on the host. The software enables the iSCSI protocol over the host's standard Ethernet NIC, preferably GbE.

To obtain the necessary software and firmware for the iSCSI driver, see the Network Appliance™ iSCSI Host Support Kit Windows at <http://now.netapp.com>.

Note

You must have the necessary software and firmware installed on your Windows host before you install SnapDrive.

FCP driver: This driver supports virtual disks within the FCP environment. It

- ◆ Supports an FCP connection between the host and the filer
- ◆ Is a SCSI/RAID controller on the host
- ◆ Includes an HBA hardware component

To obtain the necessary software and firmware for the FCP driver, see the Network Appliance™ FCP HBA Attach Kit for Windows at <http://now.netapp.com>.

Note

You must have the FCP HBA hardware and the necessary software and firmware installed on your Windows host before you install SnapDrive.

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 FCP)-type virtual disks
- ◆ Require the pair of HBAs supplied in the NetApp Dual HBA FCP Attach Kit for Windows

How virtual disks work

Virtual disk definition

A SnapDrive virtual disk is a software emulation of a locally attached Windows storage device, such as a disk drive or RAID array. This technology provides all the convenience of data storage within the Windows environment—and it further leverages NetApp filers for simplified management, data protection, and high availability.

How the filer interacts with a virtual disk

To the filer, a virtual disk 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 file is slightly larger than the raw disk size reported to the Windows host, and this capacity does not change unless you explicitly increase the size of the virtual disk.

Note

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

The filer is not aware of the many NTFS files a Windows user can store on the virtual disk; the filer interacts solely with the single file that represents the entire virtual disk.

In physical terms, the filer uses WAFL to distribute the blocks that compose virtual disk file across the physical disks on the filer.

How Windows interacts with a virtual disk

You can format and manage virtual disks on the filer just as you format and manage other Windows disks that store application data. Similarly, the 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 SnapDrive virtual disk is 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.

Virtual disk types

SnapDrive virtual disks come in two types:

FCP-type: The FCP-type virtual disks use the Fibre Channel Protocol (FCP) to communicate between a host and a filer.

iSCSI-type: The iSCSI-type virtual disks use the iSCSI protocol to communicate between a host and a filer.

Although the FCP-type and iSCSI-type virtual disks use different software drivers and different hardware attachments, the two types of virtual disks are functionally identical. That is, both virtual disks are used for data storage on the filer.

How virtual disks work

A virtual disk uses FCP or iSCSI connections to provide Windows hosts with access to data storage on a NetApp SAN.

In a NetApp SAN environment, ports on the host are known as *initiators*, and the adapter ports on filers are referred to as *targets*. These targets connect to target storage devices (virtual disks, also referred to as LUNs in this documentation), which provide the initiator with data storage (raw disk access).

The Windows host (SAN host) initiates data storage and retrieval operations by using FCP or iSCSI to access virtual disks on the filer, which acts as a target-mode device (or *storage server*).

Both FCP and iSCSI use SCSI commands to control the host-side HBA, which connects the host to the filer.

For additional details, see the Data ONTAP *Block Access Management Guide*.

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 10
- ◆ “Understanding volume size” on page 11

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 as balanced as possible.

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

Storage requirements

To ensure that all the virtual disks in your volume remain writable, the volume storing the virtual disks must be at least twice the size of all the virtual disks. The space is used to store the following:

- ◆ Data that changes between snapshots (Even if all the data on the virtual disks change following the most recent snapshot, and none has been committed to disk, everything can still be written to disk.)
- ◆ The active file system of the virtual disk
- ◆ Metadata

Space-related filer settings

SnapDrive works best with certain settings on your filer:

- ◆ Upon disk creation or connection, SnapDrive sets file-based space reservation to On for each virtual disk.

Caution

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

- ◆ Data ONTAP™ software 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. However, Network Appliance recommends that you manually reset the snap reserve option to 0% for all volumes holding SnapDrive virtual disks. For details, see “Resetting the snap reserve option” on page 43.

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. 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 120 for more information.

- ◆ The volume must also provide enough additional space to hold the number of snapshots you intend to keep online. The maximum number of snapshots is 255 per filer volume. The amount of space consumed by a snapshot depends on the amount of data that changed following the previous snapshot and, to a smaller extent, on the space necessary to store the pointers maintained by the snapshot.

Space reservation

Space reservation blocks snapshot creation whenever the filer volume storing the virtual disk no longer has enough free space to accommodate all write operations required by the virtual disk in the event a snapshot is taken. In this manner, the feature prevents situations where all writable blocks on the volume are locked by snapshots, and no blocks are available for writing new data.

When you create a filer volume, the Space Reserved check box is not selected on the FilerView pane accessed through LUNs > Manage. However, when you create a virtual disk with SnapDrive, file-based space reservation is enabled for each virtual disk.

Caution

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

File-based space reservation, as its name implies, grants space reservations on a file-by-file basis.

When a virtual disk is first created, 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 a snapshot of the filer volume holding the virtual disk is created, 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.

Note

To monitor Used, Available, Reserved, and Total space on a specific filer volume, enter **df -r** at the filer console.

Example: The following sequence illustrates the effect of various virtual disk operations upon free space on a volume 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: 10 MB (for overhead) Reserved: 40 GB Available: 60 GB Volume Total: 100 GB Snapshot creation guaranteed.	Because space reservation is mandatory for SnapDrive, the largest virtual disk you can create on an empty volume is slightly less than half the size of that volume. Space equal to the size of the virtual disk is always held in reserve so that even if the disk is full, and all the data on it changes, enough reserved space remains to write all that new data to the volume.
Write 40 GB of data to the virtual disk.	Used: 40 GB Reserved: 40 GB Available: 20 GB Volume Total: 100 GB Snapshot creation guaranteed.	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.
Delete all the data on the virtual disk.	Used: 40 GB Reserved: 40 GB Available: 20 GB Volume Total: 100 GB Snapshot creation guaranteed.	Windows reports the virtual disk as empty, but the space on the volume used by data remains at 40 GB, because all the data on the disk was locked by the snapshot.

Action	Results	Comment
Write 20 GB of data to the virtual disk.	Used: 60 GB Reserved: 40 GB Available: 0 GB Volume Total: 100 GB Snapshot creation blocked.	The amount of space used on the volume increases to 60 GB, because the 40 GB of deleted data belongs to the snapshot and therefore continues to count against the Used total. You cannot take a snapshot now, because no space is available. That is, all space is used by data or held in reserve so that any and all changes to the content of the virtual disk can be written to the volume.
Expand the volume by 100 GB.	Used: 60 GB Reserved: 40 GB Available: 100 GB Volume Total: 200 GB Snapshot creation guaranteed.	After you expand the volume, free space becomes available again, and therefore, snapshot creation is no longer blocked.
Write 20 GB of data to the virtual disk.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation guaranteed.	According to Windows, the virtual disk is full once again. The volume still has 80 GB of available space. None of the data currently on the disk belongs to a snapshot.
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 guaranteed.	Because none of the overwritten data belongs to a snapshot, it disappears when the new data replaces it.
Create a snapshot of the virtual disk.	Used: 80 GB Reserved: 40 GB Available: 80 GB Volume Total: 200 GB Snapshot creation guaranteed.	The snapshot locks all 40 GB of data currently on the disk. A total of 80 GB of data now belongs to the two snapshots of the virtual disk.
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 guaranteed.	Because the data being replaced belongs to a snapshot, it remains on the disk.

Action	Results	Comment
Delete both snapshots of the virtual disk.	Used: 40 GB Reserved: 40 GB Available: 120 GB Volume Total: 200 GB Snapshot creation guaranteed.	The 80 MB of data locked by the two snapshots disappears from the Used total when the snapshots are deleted.
Expand the virtual disk by 40 MB.	Used: 40 GB Reserved: 80 GB Available: 80 GB Volume Total: 200 GB Snapshot creation guaranteed.	The amount of space reserved increases to match the expanded size of the virtual disk. This guarantees that the entire contents of the disk can be written to the volume.
Delete the virtual disk.	Used: 0 GB Reserved: 0 GB Available: 200 GB Volume Total: 200 GB	Deletion of the virtual disk removes from the volume not just the virtual disk itself, but all data on it at the time of deletion and all snapshots of the virtual disk as well.

About this chapter

This chapter explains the tasks you must complete prior to 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 nonclustered and clustered configurations supported by SnapDrive.

Topics in this chapter

This chapter contains the following sections:

- ◆ “What to read” on page 18
- ◆ “Selecting a SnapDrive configuration” on page 19
- ◆ “Preparing hosts” on page 29
- ◆ “Preparing filers” on page 32
- ◆ “Preparing the SnapDrive service account” on page 44

What to read

Protocol-specific reading

SnapDrive installation requirements and procedures vary according to the virtual disks you choose to create. Use the following table to determine which NetApp documents you should read. (If you plan to install both protocols, read both sets of documents.)

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

To create...	Read...
iSCSI-type virtual disks	◆ This document ◆ <i>Setup Guide for iSCSI Microsoft Windows Initiator Support Kit 1.0</i> ◆ <i>Data ONTAP Storage Management Guide</i>, which shipped with your filer
FCP-type 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</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:

- ◆ Virtual disk type—iSCSI or FCP
- ◆ Host operating system—Windows 2000 Server (or Advanced Server for Windows-cluster configurations) or Windows 2003 Server (Standard Edition or Enterprise Edition)
- ◆ Host operating system Service Pack level
 - ❖ For Windows 2000: SP3 or SP4
 - ❖ For Windows 2003: (no Service Pack required)
- ◆ Host operating system hot fix level (various combinations of mandatory and optional hot fixes, which are determined by host operating system, Service Pack level, and special SnapDrive options. See “Understanding feature availability” on page 20.)
- ◆ Special options (Windows clustering, filer cluster failover, MPIO)

After you select a configuration, you can determine

- ◆ How to set up your hosts (See “Preparing hosts” on page 29.)
- ◆ How to set up your filers (See “Preparing filers” on page 32.)
- ◆ How to set up your SnapDrive service account (See “Preparing the SnapDrive service account” on page 44.)
- ◆ How to cable your configuration (See “iSCSI configurations” on page 20, “FCP configurations” on page 24, and “MPIO configurations” on page 26.)

Selection guidelines

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. This eliminates the need for SnapDrive traffic 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 type.

Note

Data ONTAP 6.4.2 supports all SnapDrive 3.0 configurations.

Host operating system		Feature availability by virtual disk type	
		iSCSI	FCP
Windows 2000 Server with...	SP3 + hot fix 816990	Standard features	Standard features
	SP3 and hot fixes 816990 & 815198	Standard features	Standard features, MPIO
	SP4	Standard features	Standard features, MPIO
Windows 2000 Advanced Server with...	SP3 + hot fixes 816990 & 851616/325040	Standard features, Windows cluster	Standard features, Windows cluster
	SP3 + hot fixes 816990, 851616/325040, & 815198	Standard features, Windows cluster	Standard features, Windows cluster, MPIO
	SP4	Standard features, Windows cluster	Standard features, Windows cluster, MPIO
Windows Server 2003, Standard Edition		Standard features	Standard features, MPIO
Windows Server 2003, Enterprise Edition		Standard features, Windows cluster	Standard features, Windows cluster, MPIO

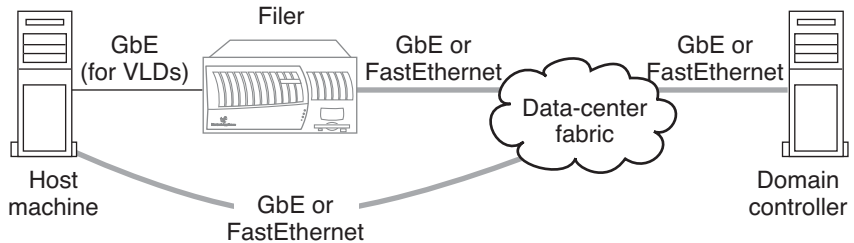
iSCSI configurations

The configurations in this section support iSCSI virtual disks.

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.



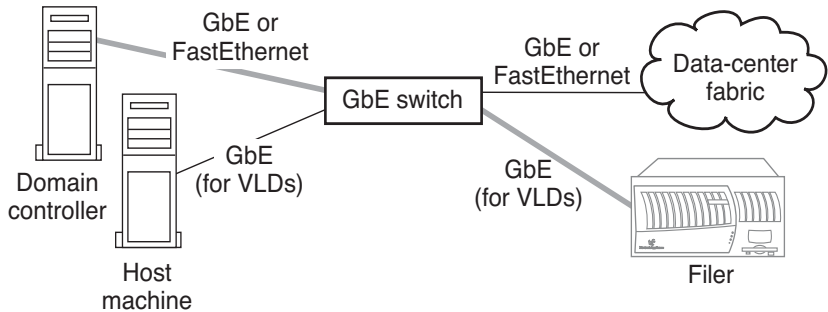
This configuration supports the following operating system edition, service pack, and hot fix combinations:

- ◆ Windows 2000 Server + SP3 + hot fix 816990
- ◆ Windows 2000 Server + SP4
- ◆ Windows 2000 Advanced Server + SP3
- ◆ Windows 2000 Advanced Server + SP3 + hot fix 816990
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Standard Edition
- ◆ Windows 2003 Server Enterprise Edition

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

- ◆ 1 GbE card dedicated to host-filer data transfer
- ◆ 1 FastEthernet (or GbE) card 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.



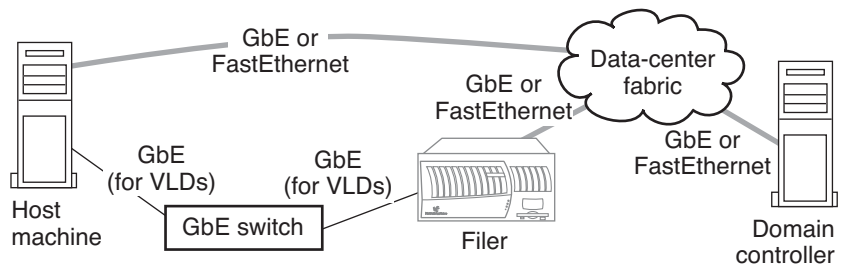
This configuration supports the following operating system edition, service pack, and hot fix combinations:

- ◆ Windows 2000 Server + SP3 + hot fix 816990
- ◆ Windows 2000 Server + SP4
- ◆ Windows 2000 Advanced Server + SP3 + hot fix 816990
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Standard Edition
- ◆ Windows 2003 Server Enterprise Edition

Because the switch connects to the data-center fabric, the host and filer in this configuration each use a single GbE card 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.



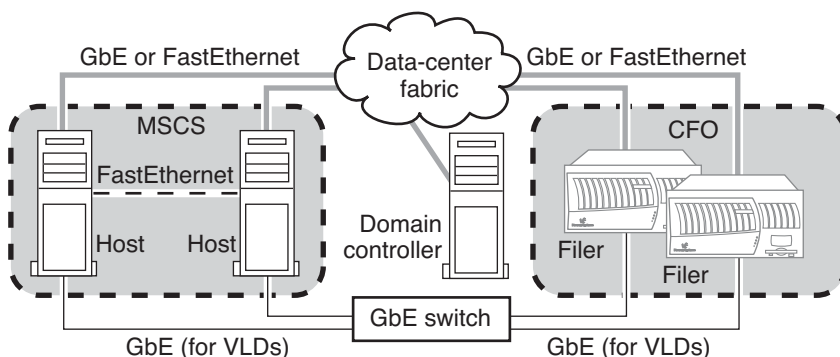
This configuration supports the following operating system edition, service pack, and hot fix combinations.

- ◆ Windows 2000 Server + SP3 + hot fix 816990
- ◆ Windows 2000 Server + SP4
- ◆ Windows 2000 Advanced Server + SP3 + hot fix 816990
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Standard Edition
- ◆ Windows 2003 Server Enterprise Edition

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

- ◆ 1 GbE card dedicated to host-filer data transfer
- ◆ 1 FastEthernet (or GbE) card 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).



Note

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

Conversely, you can connect a filer or filer cluster to multiple hosts. However, you must segregate the virtual disks for each host into separate, dedicated volumes, then make sure that only the host “owning” a dedicated volume connects to the virtual disks contained by that volume.

This configuration supports the following operating system edition, service pack, and hot fix combinations:

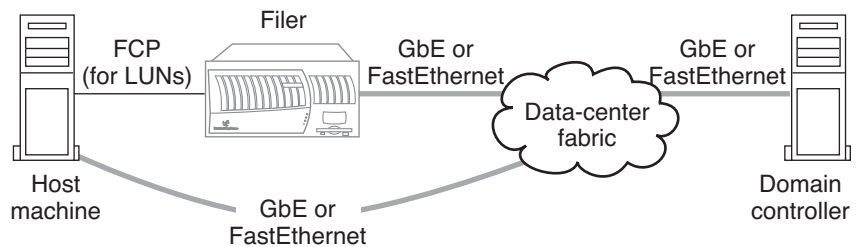
- ◆ Windows 2000 Advanced Server + SP3 + hot fixes 816990 and 851616/325040
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Enterprise Edition

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

- ◆ 1 GbE card dedicated to host-filer data transfer
- ◆ 1 FastEthernet (or GbE) card to connect to the data-center fabric
- ◆ 1 optional FastEthernet card 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.

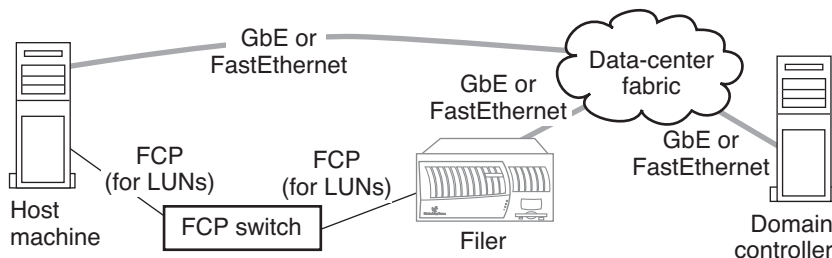
This configuration supports the following operating system edition, service pack, and hot fix combinations:

- ◆ Windows 2000 Server + SP3 + hot fix 816990
- ◆ Windows 2000 Server + SP4
- ◆ Windows 2000 Advanced Server + SP3
- ◆ Windows 2000 Advanced Server + SP3 + hot fix 816990
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Standard Edition
- ◆ Windows 2003 Server 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 LUN-type virtual disks.



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

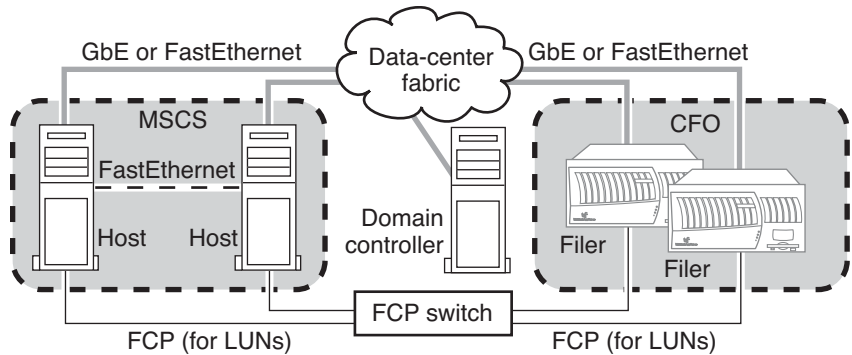
- ◆ 1 HBA to transfer LUN data between filer and host
- ◆ 1 FastEthernet or GbE NIC to connect to the data-center fabric

This configuration supports the following operating system edition, service pack, and hot fix combinations:

- ◆ Windows 2000 Server + SP3 + hot fix 816990
- ◆ Windows 2000 Server + SP4
- ◆ Windows 2000 Advanced Server + SP3
- ◆ Windows 2000 Advanced Server + SP3 + hot fix 816990
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Standard Edition
- ◆ Windows 2003 Server Enterprise Edition

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. See details in the note that accompanies “Windows cluster connected to a filer cluster through a dedicated GbE switch” on page 23.

This configuration supports the following operating system edition, service pack, and hot fix combinations:

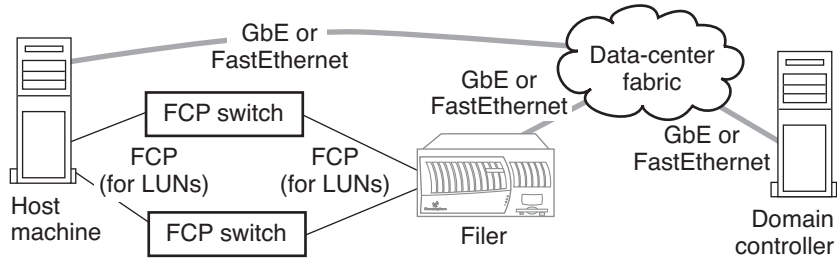
- ◆ Windows 2000 Advanced Server + SP3 + hot fixes 816990 and 851616/325040
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Enterprise Edition

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 FastEthernet card 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.



This configuration supports the following operating system edition, service pack, and hot fix combinations:

- ◆ Windows 2000 Server + SP3 + hot fixes 816990 and 815198
- ◆ Windows 2000 Server + SP4
- ◆ Windows 2000 Advanced Server + SP3 + hot fixes 816990 and 815198
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Standard Edition
- ◆ Windows 2003 Server Enterprise Edition

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

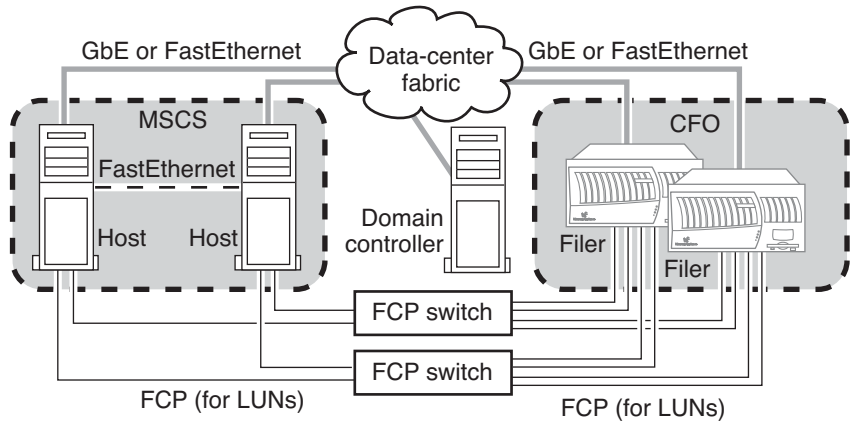
- ◆ 2 HBAs to transfer multipathed LUN data between filer and host
- ◆ FastEthernet (or GbE) card to connect to the data-center fabric

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.

This configuration must use one of the following configurations:

- ◆ Windows 2000 Advanced Server + SP3 + hot fixes 816990, 851616/325040, and 815198
- ◆ Windows 2000 Advanced Server + SP4
- ◆ Windows 2003 Server Enterprise Edition



Each host in this configuration uses the following connection hardware:

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

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

Preparing hosts

Tasks for preparing hosts

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

- ◆ Verify that each host meets minimum processor and memory requirements.
- ◆ Install on each host the proper connection hardware for your SnapDrive configuration.
- ◆ Install on each host the proper operating system edition, service pack, and hot fixes for your SnapDrive configuration.

Minimum requirements

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

Note
Be sure to read the important qualifications that follow this table.

Component	Minimum Requirement
CPU	500 MHz Pentium® III
Memory	256 MB RAM
HBAs	Emulex® LP9002L-F2 host bus adapters (for FCP)
NICs	Intel® PRO/1000 Gigabit server adapters (for iSCSI)
Operating system	Windows 2000 Server (with SP3 or SP4) Windows 2000 Advanced Server (with SP3 or SP4) Windows 2003 Standard Edition Windows 2003 Enterprise Edition
Microsoft hot fixes	816990 (must be installed with SP3) 815198 (must be installed with SP3 if MPIO is deployed) 851616/325040 (must be installed with SP3 if MSCS is deployed).

HBAs and NICs: To determine the exact number and type of HBAs and NICs required by each host in your SnapDrive configuration, consult “iSCSI configurations” on page 20, “FCP configurations” on page 24, and “MPIO configurations” on page 26.

Interface drivers: Before installing SnapDrive, make sure to obtain the latest firmware and drivers for the HBAs and NICs you are using. This ensures high network bandwidth and ease of configuration.

- ◆ The latest Intel® GbE driver and software is available on the Intel Web site at the following URL: <http://downloadfinder.intel.com>. From this gateway, use the drop-down menus to navigate to the Web page labeled Intel PRO/1000 Gigabit Server Adapter.
- ◆ 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 Software Initiator, which 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: If you plan to use MPIO, you must install SP3 or SP4 before installing SnapDrive.

Note

The SnapDrive installation wizard will not let you install the MPIO drivers unless your host has already been upgraded to SP3 or SP4.

Hot fixes:

- ◆ If your host is running SP3, you must install hot fix 816990 on your host before you install SnapDrive. This hot fix must be requested directly from Microsoft Product Support Services: <http://support.microsoft.com>.
This hot fix eliminates an erroneous error message when you shut down your Windows 2000 host. For details, read Knowledge Base article 816990 at the Microsoft Web site: <http://support.microsoft.com>.
- ◆ If your host is running MPIO on either Windows 2000 Server or Advanced Server with SP3, you must install hot fixes 816990 and 815198 before you install SnapDrive.
Hot fix 815198 eliminates certain incorrect displays of WMI information when MPIO is installed. This hot fix must be requested directly from Microsoft Product Support Services: <http://support.microsoft.com>.

- ◆ If you are running MSCS (a Microsoft cluster) on Windows 2000 Advanced Server with SP3, you must install hot fixes 816990 and 851616/325040 before you install SnapDrive.
Hot fixes 851616/325040 correct problems having to do with incorrect drive letter or disk type assignment.

Preparing filers

Conditions for filer preparation

Prior to 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 filer 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*.

Minimum filer requirements

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

Note

Be sure to read the important qualifications that follow this table.

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

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 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)
Volume	create_ucose	On	◆ Disk creation ◆ Disk connection

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

SnapDrive-specific limitations

Users should remain aware of the following SnapDrive 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 jumbo frames.
- ◆ SnapDrive does not support the use of NIC Teaming on Windows hosts.
- ◆ SnapDrive does not support the use of LUN cloning.
- ◆ A Windows host running SnapDrive can connect directly to the physical, “hosting” filer (vfiler0) created by the 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.

- ◆ The Spanning Tree protocol should be disabled to keep virtual disk reconnection times to a minimum after the host reboots.

Note

Dedicated virtual-disk volumes are particularly important for filers running Data ONTAP 6.4.2, which uses file-based space reservation. Because all virtual disks in the dedicated volumes have space reservations, they are always written to disk. By contrast, non-virtual disk files that lack space reservations might not get written properly to disk.

- ◆ Volumes used to store files on virtual disks should not be shared with non-host machines or applications not running on a host.
- ◆ 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.

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 detailed information about the following procedures, see the *Data ONTAP Block Access Management Guide*.

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 as long as each virtual disk resides in one of the following locations:
 - ❖ The root of a volume (but not the root of the root volume)
 - ❖ The root of a qtree

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.
- ◆ 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. (Consult 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.
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 39.) 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 43.)

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: 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 telnet 122.48.50.52</pre>
2	At the filer prompt, create the volume by entering the following command: vol create <i>volname number</i> <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 39.) 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 43.)

Creating a qtree: To create a qtree on the filer to host multiple VLD-type virtual disks, 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: telnet accounting-filer2 telnet 122.48.50.52

Step	Action
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: qtree create /vol/corphq/accounting <i>vol</i> indicates the root volume. <i>corphq</i> indicates the volume name. <i>accounting</i> indicates the qtree name.

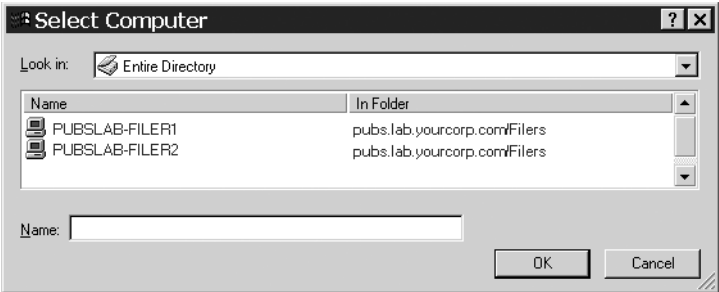
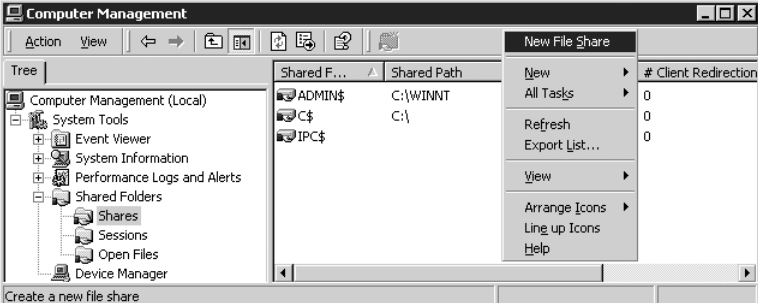
Creating a CIFS share: To establish a CIFS share for a volume that will contain virtual disks, complete the following procedure.

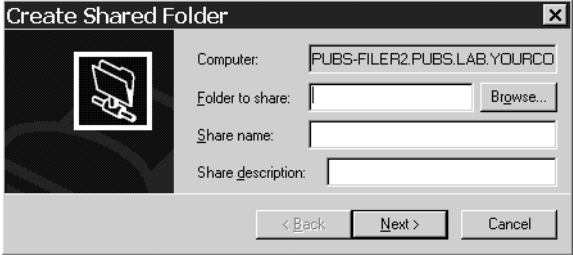
Note

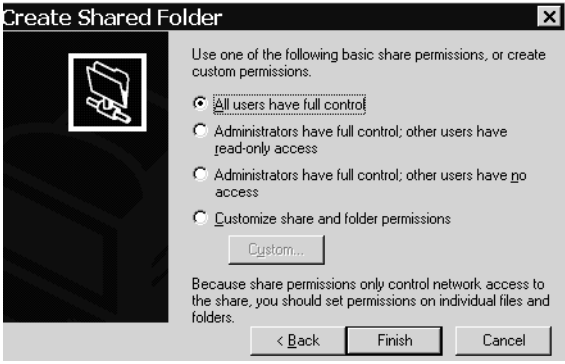
Before you create a CIFS share for your volume, you must have CIFS enabled and configured (through the `cifs setup` command) on the filer. For SnapDrive to operate properly, the filer's CIFS (NetBIOS) name must exactly match the filer listed (UNIX host name).

For more information about running CIFS setup, see your *Data ONTAP File Access Management Guide*.

Step	Action
1	At the Start Menu on the Windows host, select Programs > Admin Tools > Computer Management.
2	In the Computer Management window, select Action > Connect to another computer.

Step	Action
3	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. 
4	Double-click System Tools.
5	Double-click Shared Folders.
6	Click Shares.
7	Right-click the right pane of the window, then select New > File Share. 

Step	Action
8	In the Folder to Share field of the Create Shared Folder window, type the following: <i>c:\vol\volname\directoryname</i> <i>volname</i> is the name of the volume. <i>directoryname</i> is the name of the folder you want to share. 
9	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.
10	In the Share Description field, type a description of the share, then click Next.

Step	Action
11	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 http://accounting-filer2/na_admin/ 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 WinSrvr5-Mfg.

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 accomplish this, 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

Understanding the service account

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

Accessing the service account

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

Note

This document assumes that SnapDrive administrators possess general familiarity with Windows system administration and NetApp filer administration as well. To help you enable the various types of access required for the SnapDrive service account, this section provides intentionally cursory guidance for each task mentioned. For detailed procedures, consult your Windows and Data ONTAP documentation.

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

Note

When you specify the SnapDrive service account, be sure to assign an account with a password that does not change. If you do change the password, remember to do so through the panel that appears after you navigate to Start Menu > Settings > Control Panel > Administrative Tools > Services > SnapDrive > Log On.

- ◆ Both the filer and the host must be able to access the service account. This occurs under the following conditions:
 - ❖ The service account has administrator privileges on both the filer and host.
 - ❖ The service account is a domain account.
 - ❖ The host and filer belong to the same domain as the service account, or they 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. You enable such access by editing two files on the filer. These procedures are explained in the section “Enabling rsh access” on page 45.
- ◆ 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 39.

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 located 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
<code>/etc/hosts</code>	Provides a local mapping of host names to IP addresses.

File	Function
/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.
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 47.

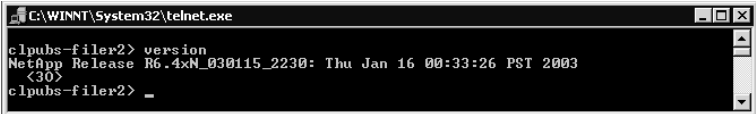
Example: In the following edited /etc/hosts.equiv file, the host named WinSrvr1 is mapped to the filer and the SnapDrive service account for the host:

```
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 <i>filername</i> version <i>filername</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 46.
	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 46.
	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.

Installing or Updating SnapDrive

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, or the VLD Manager, is currently installed, follow directions under “Upgrading to SnapDrive 3.0” on page 52.
- ◆ If no version of SnapDrive or VLD Manager is installed, follow instructions under “Installing SnapDrive for the first time” on page 68.

Upgrading to SnapDrive 3.0

When to use this section

Use this section if a previous version of the SnapDrive or VLD Manager application is installed on your system.

Which procedure to follow

How you upgrade to SnapDrive 3.0 depends on what components of SnapDrive or VLD Manager you are currently using.

- ◆ If your Windows host has VLD-type virtual disks connected, follow the procedures under “Upgrading to SnapDrive 3.0 and converting VLD-type virtual disks” on page 53.
- ◆ If your Windows host has only LUN-type virtual disks connected, follow the procedures under “Upgrading to SnapDrive 3.0 if you have no VLD-type virtual disks” on page 63.

Upgrading 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 some extra steps if you are currently using VLD-type virtual disks. Network Appliance recommends that you read over the upgrade process that follows, to familiarize yourself with the requirements and upgrade steps.

Note

For more information on the VLD to LUN conversion, see “VLD to LUN conversion” on page 59.

Upgrading to SnapDrive 3.0 and converting VLD-type virtual disks

SnapDrive 3.0 upgrade and conversion process

Upgrade process

To upgrade to SnapDrive 3.0 when your Windows hosts has VLD-type virtual disks connected, perform 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 to create a drive map. This information can be accessed using the SnapDrive MMC interface. Recording this information will help you ensure that no drive letters are changed by the conversion, so that all scripts and applications will function correctly after the conversion.
2	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 there are no SnapManager backups scheduled to occur while you are upgrading. If there are backups 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 application(s) access VLD-type virtual disks, determine the correct application-specific instructions to use to stop your application(s). 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 “Stopping Microsoft Exchange for VLD conversion” on page 57.
	Microsoft SQL Server	Follow the instructions “Stopping Microsoft SQL Server for VLD conversion” on page 57.
	Domino	Follow the instructions “Stopping Domino for VLD conversion” on page 58.
	All other applications	Follow the instructions “Stopping all other applications for VLD conversion” on page 58.
6	Download and install the Microsoft iSCSI Software Initiator version 1.0. See the iSCSI Microsoft® Windows® Initiator Support Kit 1.0 Description Page on the NOW site for instructions.	

Step	Action
7	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 will create a single, consistent snapshot of all the virtual disks that share this filer volume and are connected to this Windows host. _____
Upgrade SnapDrive and convert your VLDs	
8	Upgrade SnapDrive to SnapDrive 3.0. a. Uninstall old versions or components if necessary. See “Uninstalling old components” on page 64. b. Install SnapDrive 3.0. See “Installing the components” on page 71.
9	Create a small test LUN of about 100 MB and connect to it before attempting the conversion. Caution_____ If this step is unsuccessful, and you continue with the upgrade, you will not be able to access any of your converted LUNs. _____
10	Convert your VLD-type virtual disks to LUNs. See “VLD to LUN conversion” on page 59.
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 can be restored by SnapDrive 3.0.
13	If you stopped any applications, restart those applications.

Step	Action
14	If you use Microsoft Exchange, Lotus Domino, or Microsoft® SQL Server, verify that all the application databases are mounted correctly after the application is restarted.
15	If you use SnapManager, create a valid SnapManager backup.

Stopping Microsoft Exchange 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.

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. For more information on stopping the Microsoft Exchange Information Store service, see NEED DOC REFERENCE.

Stopping Microsoft SQL Server for VLD conversion

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

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.

Step	Action
4	Select the MSSQLSERVER service and select Action > Stop to stop the service. For more information on stopping Microsoft SQL Server, see NEED DOC REFERENCE.

Stopping Domino for VLD conversion

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

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 on 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.

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

Upgrading to SnapDrive 3.0 and converting VLD-type virtual disks

VLD to LUN conversion

VLD conversion requirement

VLD-type virtual disks are not supported in SnapDrive 3.0. To be able 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.

Caution

Before running this wizard, you must make sure that you have no applications accessing the VLD-type virtual disk to be converted.

LUN connection types

SnapDrive 3.0 supports two ways to connect to LUNs: Fibre Channel Protocol (FCP) and Gigabit Ethernet (GbE) with iSCSI.

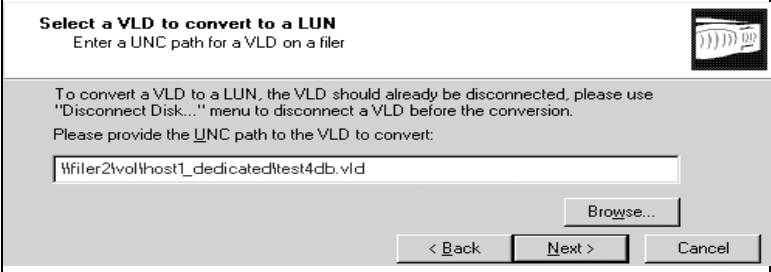
Note

You can use only one type of connection from any one host.

Converting a virtual disk

After you have prepared your environment for the VLD to LUN conversion and made sure that no application is accessing the VLD-type virtual disk to be converted, you are ready to convert your VLD-type virtual disk. To convert a VLD-type virtual disk to a LUN, complete the following steps.

Step	Action
1	Make sure that no applications are accessing the VLD-type virtual disk to be converted.
2	Select Start > Programs > Administrative Tools > Computer Management to open the Computer Management window.
3	In the Computer Management window, select Storage > SnapDrive > Disks. Select the VLD-type virtual disk you want to convert.
4	Right-click and select Convert VLD to LUN.
5	After the Convert VLD to LUN Disk Wizard appears, click Next.

Step	Action
6	In the “Select a VLD...” panel, the UNC path to the VLD-type virtual disk you selected is already filled in. The name of the .vld file becomes the name of the new LUN. Example: \\filer2\vol\host1_dedicated\test4db.vld becomes the new LUN named test4db.lun 
7	To automatically reconnect the LUN after it is converted, leave the Connect LUN... check box checked (recommended). Click Next.
8	If a .lun file exists with the same name as the .vld file you are converting, a panel is displayed prompting you to specify a different name for the converted disk.
9	If the VLD-type virtual disk you are converting contains snapshots, a message box is displayed informing you that they will be invalidated. Click Yes to continue the conversion. Note After the conversion, previously created snapshots will no longer be usable by SnapDrive 3.0. However, if the conversion fails, the old snapshots could be used to restore the VLD-type virtual disk.

Step	Action						
10	In the “Select a Virtual Disk type” panel, select the Virtual Disk Type. [screen shot here]						
	<table><tr><th>If...</th><th>Then...</th></tr><tr><td>The VLD-type virtual disk being converted belongs to a single-host system</td><td>Select Dedicated, click Next, and then skip to Step 12.</td></tr><tr><td>The VLD-type virtual disk being converted is an MSCS cluster resource</td><td>Select Shared, and click Next.</td></tr></table>	If...	Then...	The VLD-type virtual disk being converted belongs to a single-host system	Select Dedicated, click Next, and then skip to Step 12.	The VLD-type virtual disk being converted is an MSCS cluster resource	Select Shared, and click Next.
	If...	Then...					
	The VLD-type virtual disk being converted belongs to a single-host system	Select Dedicated, click Next, and then skip to Step 12.					
The VLD-type virtual disk being converted is an MSCS cluster resource	Select Shared, and click Next.						
11	In the “Information about...” panel, verify that you want the disk to be shared by the nodes listed and click Next. [screen shot here]						
12	In the Select Virtual Disk Properties panel, make sure 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 click Next. [screen shot here]						
13	If your system is configured for iSCSI, select the desired initiator and click the Right Arrow. Click Next.						
14	 Completing the Convert VLD/LUN Wizard You have successfully completed the Convert VLD to LUN Wizard with the following settings : VLD UNC Path : \\pubs-filer2\vol1\host1_dedicated\test4db.vl LUN name : test4db.lun  The conversion operation is not reversible. To close this wizard and begin converting the disk, click Finish. < Back Finish Cancel						

Converting a quorum disk

To convert a VLD-type virtual disk that serves as the quorum disk for a Windows cluster configuration, complete the following steps.

Note

The following procedure assumes extensive knowledge of Windows clusters.

Step	Action
1	Stop all application services running on the cluster.
2	Create or identify a LUN that can be used temporarily as the quorum disk. This LUN should be at least as large as the quorum disk.
3	Change the quorum disk to the temporary LUN created in step 1. For more information, see Microsoft Knowledge Base Article 280353, "How to Change the Quorum Disk Designation."
4	Convert the VLD-type virtual disk to a LUN. See "VLD to LUN conversion" on page 59.
5	Redesignate the converted disk (now a LUN) as the quorum disk.

Upgrading 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 to SnapDrive 3.0 without VLD-type virtual disks, you need to do the following.

Stage	Process
1	Uninstall old SnapDrive versions or components if necessary. See “Uninstalling old components” on page 64.
2	Install the required version of the iSCSI Software Initiator or FCP driver. See “Installing the driver” on page 69.
3	Network Appliance strongly recommends that you create a system backup and an Emergency Repair Disk before upgrading to SnapDrive 3.0.
4	Install SnapDrive 3.0. See “Installing the components” on page 71.

Uninstalling old components

Uninstalling the VLD driver

SnapDrive 3.0 will not work properly if any version of the VLD driver 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 are not currently using 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.
2	On the Windows host, navigate to the Microsoft Device Manager: right-click on My Computer, 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..., then click OK in the dialog box to confirm that you want to uninstall the VLD driver.

When to uninstall older versions of SnapDrive or VLD Manager

Check the following table to determine whether you need to uninstall an older version of SnapDrive or the VLD Manager application as a prerequisite for installing SnapDrive 3.0.

If...	Then...
Any version of VLD Manager is installed on the host	See “Uninstalling SnapDrive 1.0 or the VLD Manager application” on page 65.
SnapDrive 1.0 is installed on the host	See “Uninstalling SnapDrive 1.0 or the VLD Manager application” on page 65.

If...	Then...
SnapDrive 2.0 or later is installed on the host	You can install SnapDrive 3.0 without uninstalling the 2.x version.

In any case, the SnapDrive installation wizard automatically checks for legacy SnapDrive installations, and it does not let you install version 3.0 until you uninstall any pre-2.0 version of the SnapDrive application.

Uninstalling SnapDrive 1.0 or the VLD Manager application

To upgrade SnapDrive 1.0 or VLD Manager to SnapDrive 3.0 you must first uninstall the SnapDrive 1.0 or VLD Manager application.

Use the standard Windows uninstall procedure: Start Menu > Settings > Control Panel > Add/Remove Programs. Click the entry for SnapDrive 1.0 or VLD Manager and respond to the prompts presented by the uninstall wizard. After you complete removal of the SnapDrive 1.0 or VLD Manager application from your Windows host, run the SnapDrive InstallShield wizard to install SnapDrive 3.0.

Uninstalling SnapDrive 2.1

If, for some reason, you need to uninstall SnapDrive 2.1, use Start Menu > Settings > Control Panel > Add/Remove Programs. Alternatively, you can navigate to the folder containing the SnapDrive 2.1 installation package and launch the InstallShield wizard, which guides you through the uninstall procedure.

The wizard presents you with the option of uninstalling the MPIO drivers along with SnapDrive 2.1. Do not attempt to uninstall the MPIO drivers through the Device Manager; proper uninstallation of the MPIO drivers can only be achieved through the SnapDrive InstallShield wizard.

If you want to remove the VLD and FCP drivers as well, you must do so through the Device Manager in the Computer Management window.

Uninstalling SnapDrive 2.0.1

If, for some reason, you want to uninstall SnapDrive 2.0.1, complete the following steps:

Step	Action	
1	If...	Then
	You want to uninstall any installation of SnapDrive 2.0.1 and simultaneously upgrade to SnapDrive 3.0	Complete the procedure in the section “Installing the new SnapDrive components” on page 71.
	You want to uninstall a “fresh” (first-time) installation of SnapDrive 2.0.1, and you don’t want to install SnapDrive 3.0 at the same time	Skip to Step 6.
	You want to uninstall an installation of SnapDrive 2.0.1 resulting from an upgrade from SnapDrive 2.0, and you don’t want to install SnapDrive 3.0 at the same time	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	Set the command prompt to the drive containing the installation package from which you originally installed SnapDrive 2.0.1. Note _____ If the volume containing the SnapDrive installation package is not already mapped to a drive letter on your host, you must first create that mapping by selecting My Computer > Map Network Drive, selecting an available drive letter from the drop-down menu in the Drive field, typing (or browsing to) the UNC location where the installation package is located, selecting the “Reconnect at logon” check box, and clicking Finish. _____ Example: G:	
4	Enter the following command at the prompt: cd <i>path</i> <i>path</i> is the fully qualified directory to the setup package from which you originally installed SnapDrive 2.0.1. Example: \NetApp\WindowsClientApps\SnapDrive\2.0.1\download\install	

Step	Action
5	Enter the following command: <pre><i>wizardname</i> /v "REINSTALLMODE=vomus REINSTALL=ALL"</pre> <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.
6	Navigate to Start Menu > Settings > Control Panel > Add/Remove Programs, and then double-click the SnapDrive icon.
7	Click Remove to launch the SnapDrive Uninstall process.
8	Follow the prompts to uninstall SnapDrive 2.0.1.

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 components You need to install the following SnapDrive components on your hosts:

- ◆ One of the virtual disk drivers:
 - ❖ The FCP driver to create FCP-type virtual disks
 - ❖ The iSCSI driver to create iSCSI-type virtual disks
- ◆ SnapDrive, which includes the following:
 - ❖ The snap-in for the Windows MMC
 - ❖ The underlying virtual disk service
 - ❖ The command-line interface
 - ❖ The optional MPIO drivers (for FCP connections only)

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

Stage	Process
1	Install the required version of the iSCSI or FCP driver. See “Installing the driver” on page 69.
2	Install SnapDrive 3.0. See “Installing the components” on page 71.

Installing the driver

Installing the FCP or iSCSI driver

Before you install SnapDrive, you need to install the correct version of the FCP or iSCSI driver, depending on which protocol you will use to connect your Windows host to the NetApp filer.

Note

If you are currently running SnapDrive 2.1 over an FCP connection, and you intend to run SnapDrive 3.0 over the same connection, you do not need to re-install the driver. Proceed to “Installing the new SnapDrive components” on page 71.

Installing the FCP Host Bus Adapter and driver: For instructions on installing these FCP components, see the *Host Bus Adapter Installation and Setup Guide 1.1 for Fibre Channel Protocol on Windows*.

Installing the iSCSI driver: To install the Microsoft iSCSI 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 for instructions.
2	Click on 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 click Next. Result: The Installing Microsoft iSCSI Initiator screen shows a progress bar.

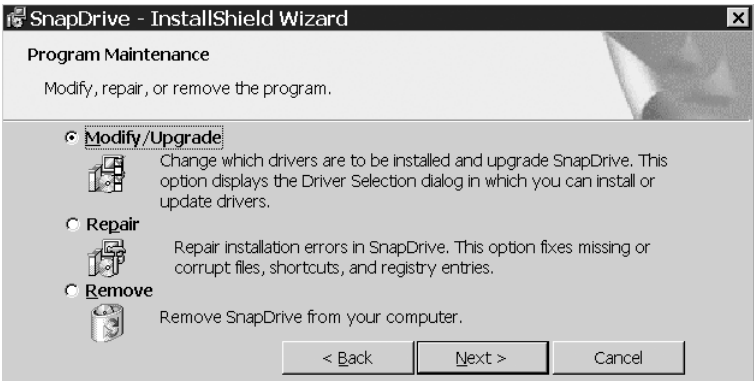
Step	Action
7	Accept the option to Install Complete iSCSI Initiator by clicking OK in the pop-up window.
8	Select I agree on the license agreement.
9	On the Microsoft iSCSI Initiator Information screen, click Next.
10	On the Installation Complete screen, click Close.

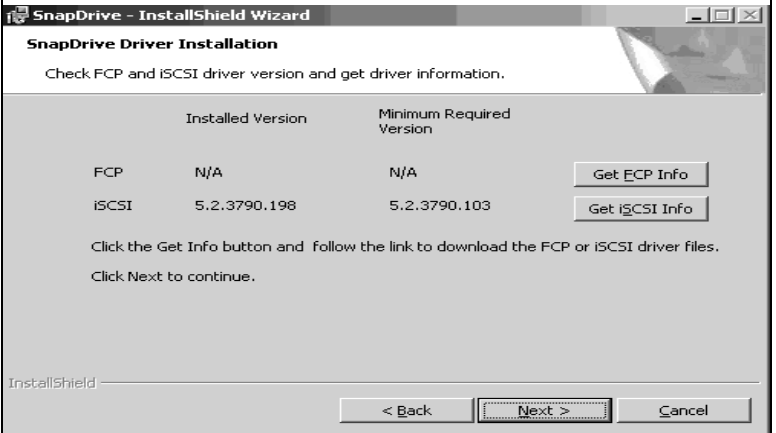
Installing the new SnapDrive components

Installing the components

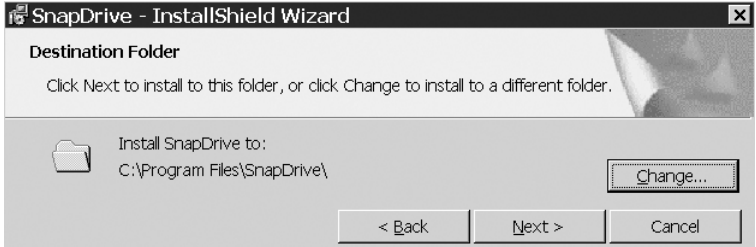
After you install the virtual disk driver you will use, install the new SnapDrive components by completing the following procedure.

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

Step	Action
1	Browse to the location of the SnapDrive installation package and double-click setup.exe or SnapDrive3.0.exe, then proceed to the next step.
2	Click Next at the “Welcome...” panel for the InstallShield Wizard for SnapDrive.
3	Accept the license agreement and click Next.
4	If the Program Maintenance panel appears, click Modify/Upgrade, then click Next. 

Step	Action	
5	If...	Then...
	The version installed is the same or later than the Minimum Required Version for the type of virtual disk you will be using (FCP or iSCSI)	Click Next and proceed to the next step.
	The version installed is earlier than the Minimum Required Version	Update the driver (see “Installing the driver” on page 69). Then restart the SnapDrive InstallShield Wizard.
		

Step	Action	
6	In the SnapDrive Driver Installation panel, select the “update MPIO drivers” or “install MPIO drivers” box if you want to install or upgrade the MPIO feature, then click Next. 	
7	If...	Then...
	If you are upgrading from SnapDrive 2.0 or later	Skip to Step 11.
	If this is a new SnapDrive installation	Supply the setup information covered in the next four steps.
8	In the Customer Information panel, type your user name and organization name, then click Next. 	

Step	Action
9	The Destination Folder panel prompts you for a directory in which to install SnapDrive on the host. By default this is C:\Program Files\SnapDrive. To accept the default, click Next, then proceed to step Step 10.  To specify a different location, click the Change button. In the Change Current Folder panel, type the path to the target directory in the “Folder name” text box. Alternatively, navigate to the folder you prefer, then select it. When the correct target location appears in the “Folder name” text box, click OK.  On the Destination Folder panel, click Next, and proceed to the next step.

Step	Action
10	On the SnapDrive Service Credentials panel, 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.
11	In the “Ready to...” panel, which is not pictured here, click Install. Result: The Installing SnapDrive panel appears, informing you that installation might take several minutes to complete.
12	After the InstallShield Wizard Complete panel appears, click Finish.
13	If you are installing or upgrading the MPIO drivers, the SnapDrive Installer Information pop-up panel appears. Click Yes to reboot the machine.
14	Once the reboot process completes, SnapDrive is successfully installed on your host.

About this chapter

This chapter explains how to use SnapDrive to create FCP-type and iSCSI-type virtual disks.

Topics in this chapter

This chapter covers the following topics:

- ◆ “About virtual disk management” on page 78
- ◆ “Creating a virtual disk” on page 79
- ◆ “Creating a virtual disk on a new Windows 2000 cluster” on page 90
- ◆ “Creating a virtual disk on an existing Windows 2000 cluster” on page 95

About virtual disk management

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. All virtual disk management must be performed 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

Creating a virtual disk

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

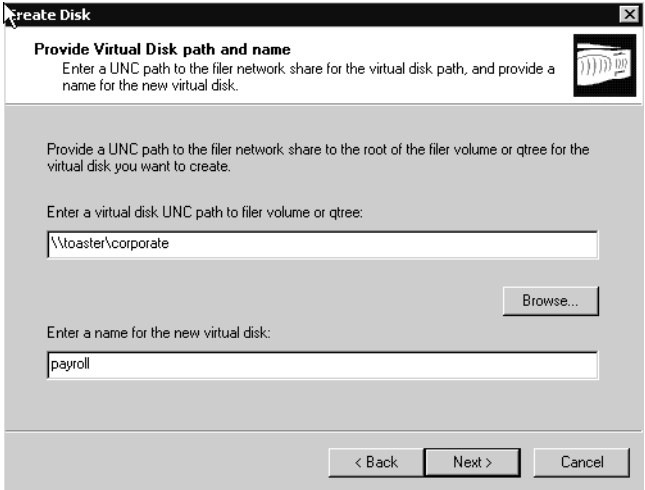
Caution

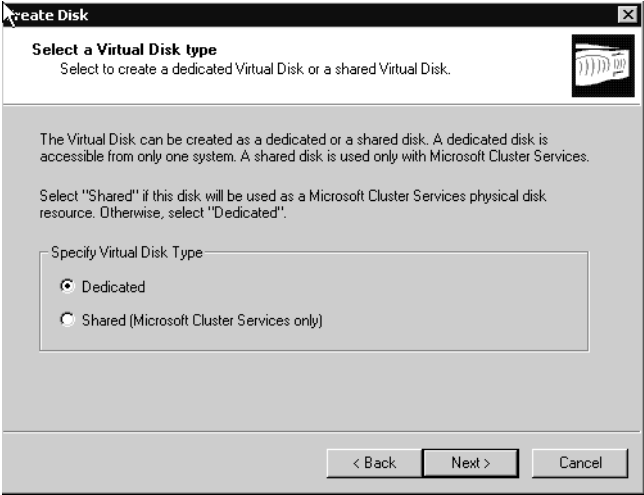
-- If you are adding the virtual disk to a cluster, make sure to perform the following procedure on whichever node owns that cluster.

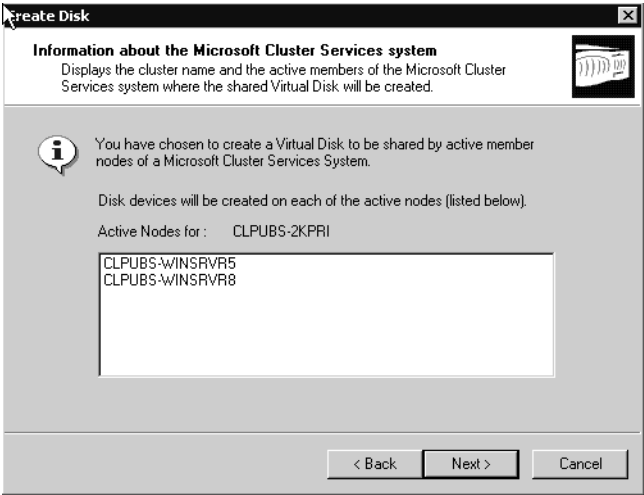
-- To avoid the possibility of unwritable files, do not attempt to create a virtual disk on a filer volume that holds anything other than virtual disk files. Conversely, do not put anything other than virtual disk files on a filer volume that contains virtual disks.

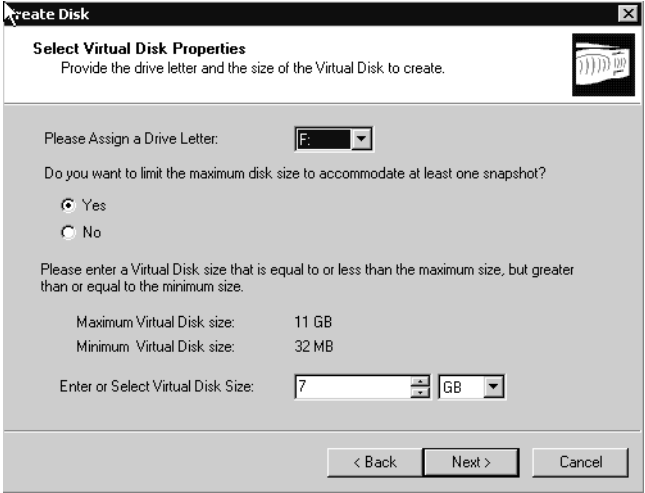
To create a virtual disk, complete the following steps.

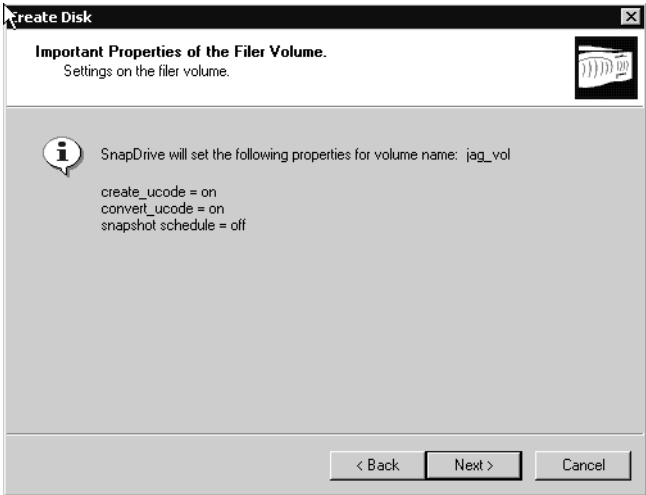
Step	Action
1	Create the dedicated volumes that will hold your virtual disks on the filer and create CIFS shares for those volumes. See “Creating a filer volume” on page 36 and “Creating a CIFS share” on page 39, and also consult the <i>Data ONTAP File Access Management Guide</i> .
2	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
3	Perform the following actions to launch the Create Disk wizard: 1. Expand the Storage option in the left panel of the MMC if it is not expanded already. 2. Double-click SnapDrive. 3. Select Disks. 4. Click Action (from the menu choices on top of the MMC). 5. Select Create Disk from the drop-down menu.

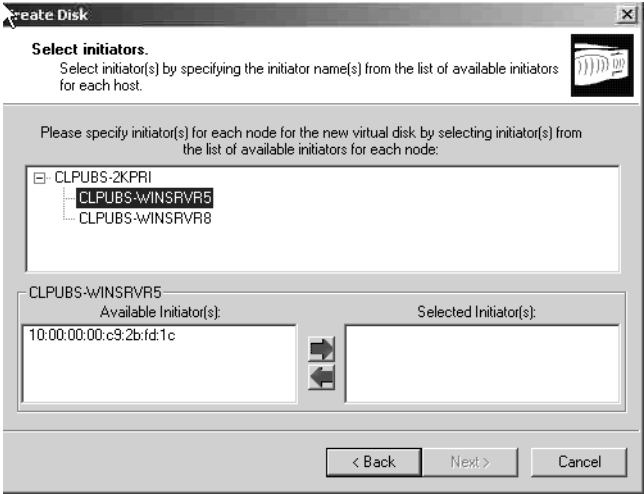
Step	Action
4	In the Create Disk wizard, click Next.
5	In the “Provide Virtual Disk...” panel (as shown in the example below), perform the following tasks: ◆ In the “Enter a virtual disk UNC path...” field, type the filer location for the virtual disk. Alternatively, click Browse and navigate to that location. ◆ In the “Enter a name...” field, type in an easy-to-remember name for the virtual disk. For example, “payroll” or “michigan” The name you enter in this field is automatically lowercased.  ◆ Click Next. Result: The Select a Virtual Disk Type panel is displayed.

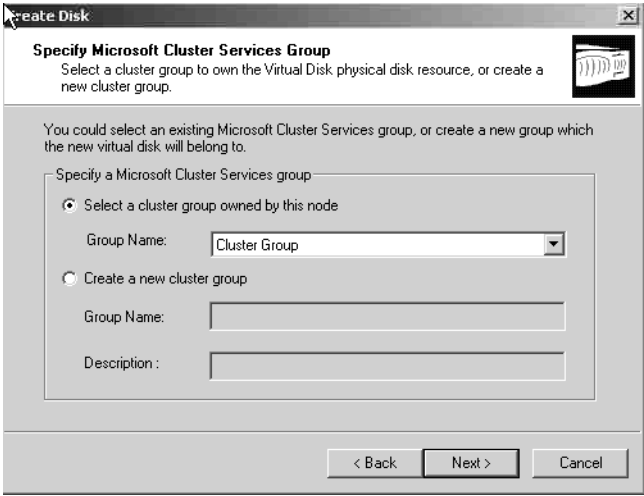
Step	Action						
6	In the “Select a Virtual Disk type” panel (as shown in the example below), perform one of the following tasks:  <table><tr><th>If...</th><th>Then...</th></tr><tr><td>The virtual disk will belong to a single-host system</td><td>Select Dedicated, click Next, then skip to Step 8.</td></tr><tr><td>The virtual disk will be a Windows cluster resource</td><td>Select Shared, click Next, then proceed to the next step.</td></tr></table>	If...	Then...	The virtual disk will belong to a single-host system	Select Dedicated, click Next, then skip to Step 8.	The virtual disk will be a Windows cluster resource	Select Shared, click Next, then proceed to the next step.
If...	Then...						
The virtual disk will belong to a single-host system	Select Dedicated, click Next, then skip to Step 8.						
The virtual disk will be a Windows cluster resource	Select Shared, click Next, then proceed to the next step.						

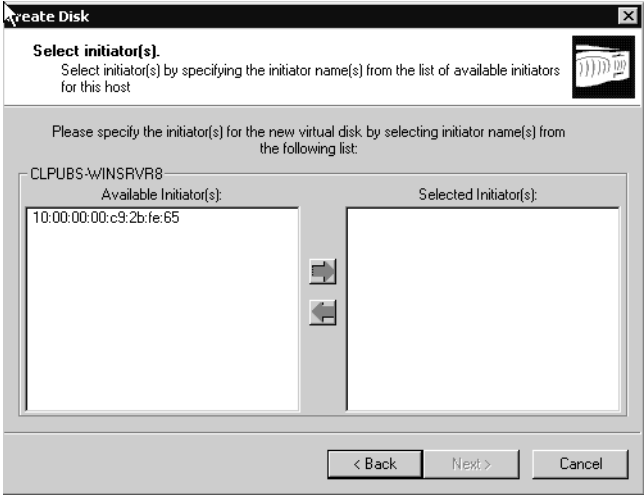
Step	Action
7	In the “Information about...” panel, verify that you want the disk to be shared by the nodes listed and click Next. 

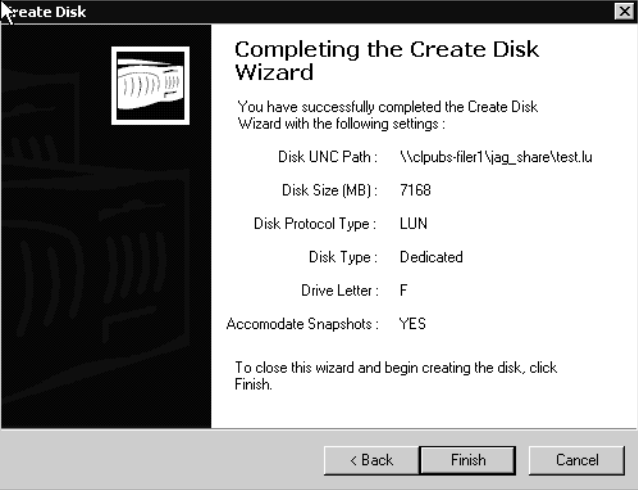
Step	Action
8	In the “Select Virtual Disk Properties” panel (as shown in the example below), perform the following tasks: ◆ Select from the list of available drive letters for the virtual disk you are creating. ◆ Select either Yes or No radio button for “Do you want to limit the maximum disk size to accommodate at least one snapshot?” ◆ 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...” panel is displayed (as described in the next step). Otherwise, the “Select Initiators...” panel is displayed. 

Step	Action	
9	The “Important Properties...” panel (as shown in the example below) 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 Initiator(s) panel is displayed. 	
10	If...	Then...
	The virtual disk will belong to a single-host system	Go to Step 14.
	The virtual disk will be a Windows cluster resource	Go to the next step.

Step	Action
11	In the “Select Initiator(s)” panel (as shown in the example below), perform the following tasks: 1. Double click the cluster group name to display the hosts that belong to the cluster. 2. Click the name of a host to select it. The list of Available Initiators for that host is displayed in the bottom left window. 3. Select the initiator for the virtual disk you are creating. 4. Click the right-pointing 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-pointing arrow. 5. Repeat Steps 2 through 4 for all the hosts. 6. Click Next. Result: The “Specify Microsoft Cluster Services Group” panel is displayed. 

Step	Action
12	In the “Specify Microsoft Cluster Services Group” panel (as shown in the example below), perform the following tasks: ◆ 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. 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. 
13	Go to Step 15.

Step	Action
14	In the “Select Initiator(s)” panel (as shown in the example below), perform the following tasks: ◆ Select the FCP or the iSCSI initiator for the virtual disk you are creating from the Available Initiators list on the left side. Note For FCP MPIO installations, you can select two ports simultaneously. ◆ Click the right-pointing 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-pointing arrow. ◆ Click Next. Result: The “Completing the Create Disk Wizard” panel is displayed.  Note See the <i>Data ONTAP Block Access Management Guide for FCP</i> and <i>Data ONTAP Block Access Management Guide for iSCSI</i> for information about how to determine the port for your HBA.

Step	Action
15	In the “Completing the Create Disk Wizard panel (as shown in the example below), perform the following tasks: ◆ 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 new virtual disk now appearing under SnapDrive in the left panel. 

Note

When you use Device Manager to uninstall a physical or logical disk device and then rescan (scan for hardware changes), you might receive an erroneous prompt to restart your computer. This problem typically occurs when a Windows Explorer window is open so that you can view disk contents as Windows uninstalls the new device and rescans. To prevent Windows Explorer from improperly holding handles to disk drives and displaying the erroneous reboot prompt on hosts running Windows SP2, install and enable Microsoft hot fix 306185. For details, see “Hot fixes” on page 30.

Note

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 *not* 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 *without* using SnapDrive.
 - Data objects other than virtual disks are stored on this filer volume.
-

Creating a virtual disk on a new Windows 2000 cluster

About creating virtual disks on a new Windows cluster

The process of creating a shared virtual disk (that is, a non-quorum disk) on a new or an existing Windows cluster is the same as creating a virtual disk on a single system, as explained in “Creating a virtual disk” on page 79. However, when creating a 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.)

If the virtual disk you are creating will be a quorum disk (in a new or an existing Windows cluster), you must follow the procedures described in this section.

About using locally-attached disks as quorum

If you will be using a locally-attached SCSI disk to serve as a quorum disk, you do not need to follow instructions in this section. Simply create the Windows cluster and designate the locally-attached SCSI disk as quorum according to the Microsoft documentation, then create *shared* virtual disks according to the procedure described in “Creating a virtual disk” on page 79.

For more information

For procedural information about creating a virtual disk as a quorum disk, see the following topics:

- ◆ “Creating a virtual disk quorum on a new Windows cluster” on page 91.
- ◆ “Creating a virtual disk as quorum on an existing Windows cluster” on page 94.

Creating a virtual disk quorum 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 or more host machines with Windows 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 LUN	Each host node must have the following installed: ◆ A GbE card (as recommended in the iSCSI Microsoft Initiator Software Support Kit 1.0) ◆ The Microsoft Software Initiator driver ◆ (Optionally) A FastEthernet card 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 LUN	Each host node must have the following installed: ◆ A NetApp qualified HBA ◆ The driver and firmware for the HBA For information about the qualified HBAs, go to http://now.netapp.com.

Note

To ensure that both 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 node. This allows plenty of time for one node to “get ahead” of the other node, preventing the computer from competing for the shared disk, which could cause a failure. See Microsoft article 259267 for more information.

Creating a virtual disk as a quorum disk

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

Task	Procedure
1	Make sure that the appropriate FCP HBA drivers or the Microsoft iSCSI software initiator drivers and SnapDrive are installed on both systems. See “Prerequisites” on page 91 for information about the drivers. See “Installing or Updating SnapDrive” on page 51 for information about installing SnapDrive.
2	Create a shared virtual disk on node 2 to serve as the quorum disk; see “Creating a virtual disk” on page 79. Make a note of the drive letter you assign to the virtual disk.
3	Disconnect the virtual disk from node 2.
4	Using the drive letter you noted in Step 2, connect the virtual disk to node 1.
5	Install and configure the Windows cluster on node 1, using the virtual disk you created as the quorum disk in Step 2. See your Microsoft documentation for detailed information about configuring Windows clusters.
6	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.

Task	Procedure
7	From node 2, connect the virtual disk you created in Step 2. See “Connecting virtual disks” on page 98 for instructions.
8	Install and configure Windows cluster on node 2, and join node 2 to the cluster you created in Step 5.
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	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 _____ Use the Cluster Administrator to perform and verify this operation. _____

Creating a virtual disk as quorum on an existing Windows cluster

When to use this this procedure

Follow these instructions to create a virtual disk as a quorum disk if your host is already running in a Windows cluster configuration.

<<Information will be available in the next draft.>>

Creating a virtual disk on an existing Windows 2000 cluster

When to use this procedure

Follow these instructions if your host is already running in a Windows cluster configuration and does not have any vir

Installing and configuring the virtual disk

To install and configure a 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 node 1. See “Prerequisites” on page 91 for information about the drivers. See “Installing the new SnapDrive components” on page 71.
2	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.
3	Install the appropriate FCP HBA drivers or the Microsoft iSCSI software initiator drivers and SnapDrive on node 2. See “Prerequisites” on page 91 for information about the drivers. See “Installing the new SnapDrive components” on page 71..
4	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.
5	From node 1, create as many shared virtual disks as are necessary to hold your data. For information about how to create virtual disks, see “Creating a virtual disk” on page 79.

Step	Action
6	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 98
- ◆ “Disconnecting virtual disks” on page 106
- ◆ “Expanding virtual disks” on page 109
- ◆ “Virtual disk properties” on page 112
- ◆ “Administering SnapDrive remotely” on page 114
- ◆ “Enabling SnapDrive notification” on page 116

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.

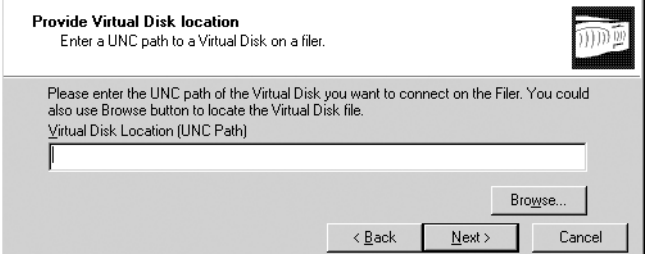
Caution

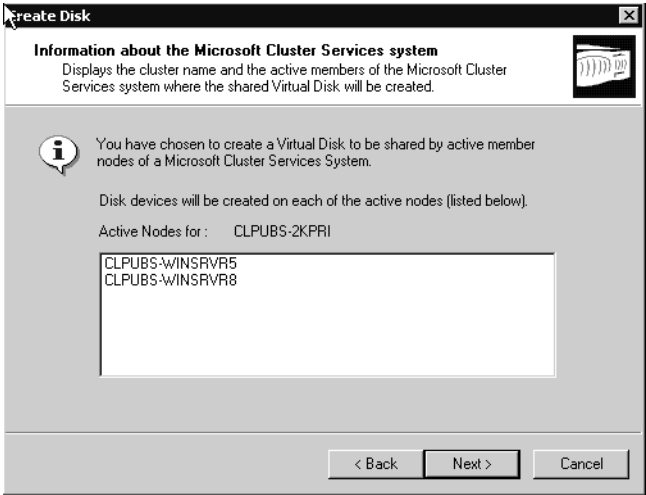
Do not try to connect to a virtual disk if it is already connected to another machine; SnapDrive does not support such simultaneous use.

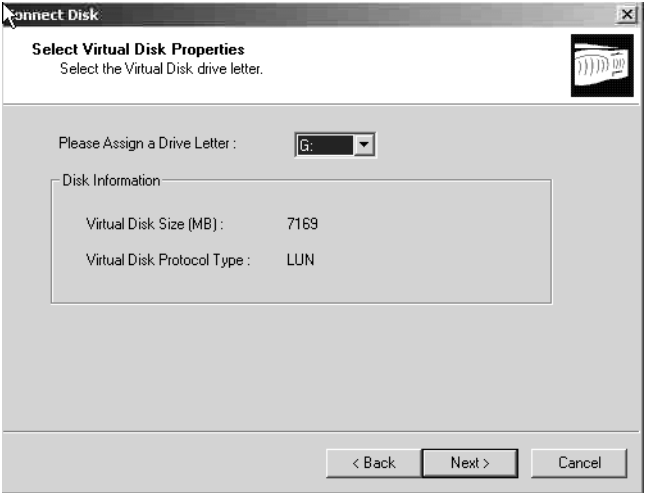
Connecting a virtual disk

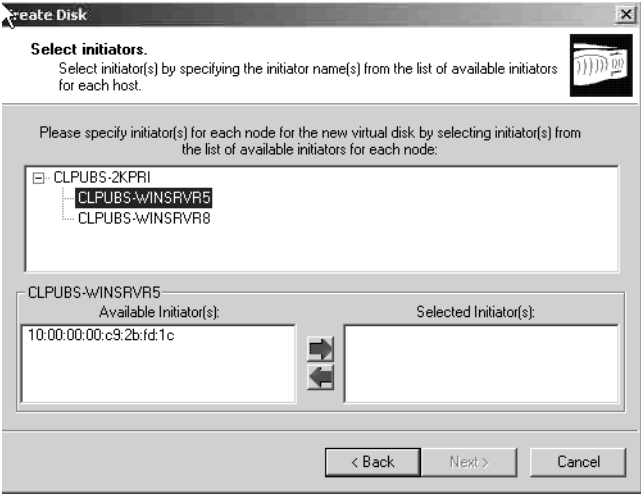
To connect your host to a virtual disk, complete the following steps.

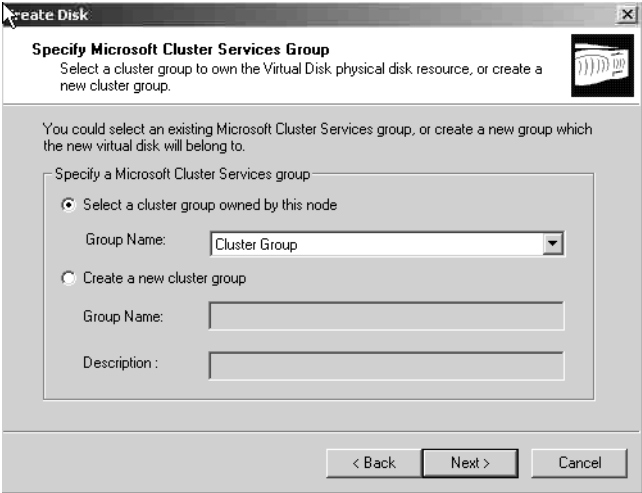
Step	Action
1	Close all Explorer windows on your host.
2	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
3	Perform the following actions to launch the Connect Disk wizard: 1. Double click SnapDrive in the left panel of the MMC. 2. Select Disks. 3. Click Action (from the menu choices on top of the MMC). 4. Select Connect Disk from the drop-down menu.
4	In the Connect Disk Wizard, click Next.

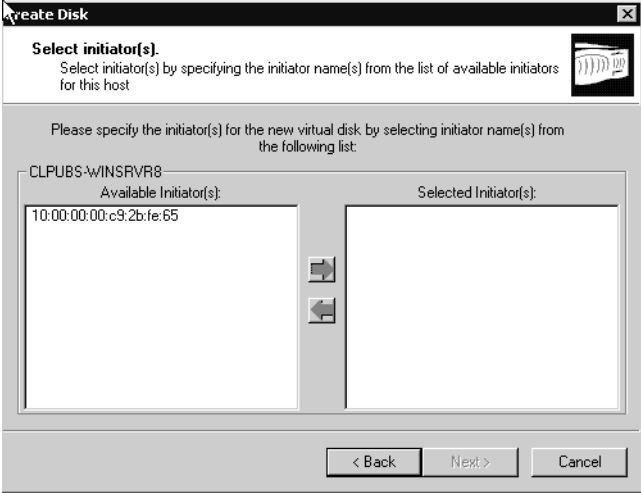
Step	Action	
5	Click Browse in the Provide Virtual Disk Drive Location window, then navigate to the filer volume on which the virtual disk resides. 	
6	Select a virtual disk file (with a .lun extension), then click Next. Note _____ Access to the filer volume is restricted according to IP address. Do not use Dynamic Host Configuration Protocol (DHCP), which is not supported, because DHCP allows the IP addresses to change, and that, in turn, can result in a denial of access to the filer volume. _____	
7	If...	Then...
	The virtual disk will belong to a single system	Select Dedicated, click Next, then continue to Step 10.
	The virtual disk will become a Windows cluster resource	Select Shared, click Next, then continue to the next Step.

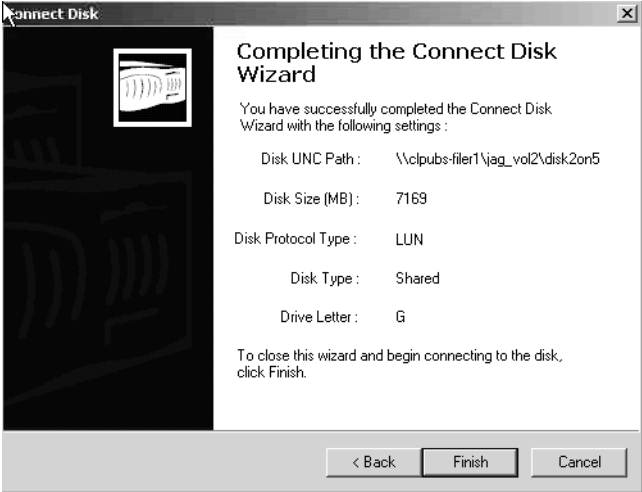
Step	Action
8	In the “Information about...” panel, verify that you want the disk to be shared by the nodes listed and click Next. 

Step	Action	
9	In the “Select Virtual Disk Properties” panel (as shown in the example below), perform the following tasks: ◆ Select from the list of available drive letters for the virtual disk you are creating. ◆ Select a disk size, which must fall within the minimum and maximum values displayed in the panel. ◆ Click Next.	
		
10	If...	Then...
	The virtual disk will belong to a single-host system	Go to Step 15.
	The virtual disk will be a Windows cluster resource	Go to the next step.

Step	Action
11	In the “Select Initiator(s)” panel (as shown in the example below), perform the following tasks: 1. Double click the cluster group name to display the hosts that belong to the cluster. 2. Click the name of a host to select it. The list of Available Initiators for that host is displayed in the bottom left window. 3. Select the initiator for the virtual disk you are creating. 4. Click the right-pointing 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-pointing arrow. 5. Repeat Steps 2 through 4 for all the hosts. 6. Click Next. Result: The “Specify Microsoft Cluster Services Group” panel is displayed. 

Step	Action
12	In the “Specify Microsoft Cluster Services Group” panel (as shown in the example below), perform the following tasks: ◆ 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. ◆ Click Next. Result: The “Completing the Create Disk Wizard” panel is displayed. 
13	Go to Step 16.

Step	Action
14	In the “Select Initiator(s)” panel (as shown in the example below), perform the following tasks: ◆ Select the FCP or the iSCSI initiator for the virtual disk you are creating from the Available Initiators list on the left side. Note For FCP MPIO installations, you can select two ports simultaneously. ◆ Click the right-pointing 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-pointing arrow. ◆ Click Next. Result: The “Completing the Create 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
15	In the “Completing the Connect Disk Wizard panel (as shown in the example below), perform the following tasks: ◆ 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

Overview

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 as a file on the filer volume.

Note

Before you disconnect a virtual disk that serves as a Windows cluster quorum disk, you must remove the cluster resource dependencies from the virtual disk resource.

Disconnecting a virtual disk

To disconnect virtual disk from a host, 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. Result: The currently connected disks are displayed in the right panel of the MMC.
3	Select the disk that you want to disconnect in the right panel.
4	Click Action (from the menu choices on top of the MMC) and select Disconnect Disk.
5	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

If any application, such as Windows Explorer or the Windows operating system is using any file contained within the virtual disk, you cannot disconnect that virtual disk. Under extraordinary circumstances (in the case of a runaway application, for example), you can use Force Disconnect Disk to override this protection.

Caution

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.
3	Double-click SnapDrive in the left panel of the MMC, then select Disks. Result: The currently connected disks are displayed in the right panel of the MMC.
4	Select the disk that you want to “force disconnect” in the right panel.
5	Click Action (from the menu choices on top of the MMC) and 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 Computer Management window.

Step	Action
7	To reconnect a virtual disk after a forced disconnect, see “Connecting virtual disks” on page 98.

Deleting a virtual disk

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.

Caution

Do not delete a virtual disk being used by a host because SnapDrive cannot undelete the 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, then select Disks. Result: The currently connected disks are displayed in the right panel of the MMC.
3	Select the disk that you want to delete in the right panel.
4	Click Action (from the menu choices on top of the MMC) and 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 9 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.)
- ◆ A virtual disk that is a quorum disk in a Windows cluster configuration cannot be expanded. Network Appliance does not support this functionality. Therefore, make sure that the quorum disk is 500 MB when you create it, and do not use it for anything other than Windows cluster configuration information. A quorum disk created and managed in this manner should never need expansion.
- ◆ 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 Computer Management (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 Computer Management window (MMC) is launched.
2	Double-click SnapDrive in the left panel of the MMC, then select Disks. Result: The currently connected disks are displayed in the right panel of the MMC.
3	Select the disk that you want to expand in the right panel.
4	Click Action (from the menu choices on top of the MMC) and select Expand Disk. Result: The Expand Disk panel is displayed. 

Step	Action
5	In the Expand Disk panel (as shown in the previous step), perform the following steps: ◆ Leave the field “Do you want to limit...” set to the default setting Yes. Note _____ 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: Note _____ -- Set the units for this value (MB, GB, or TB) in the box to the right of the “Expand by...” box. -- Make sure to pick a value for the “Expand by...” 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.

Virtual disk properties

Properties you can examine

You can examine the following property for virtual disks:

Monitor Time Interval: Specifies how frequently SnapDrive monitors the snap reserve space on the filer volume for all virtual disks on the system. The default is every 30 minutes.

About examining and modifying virtual disk properties

You can examine the virtual disk properties by using either the SnapDrive GUI in the Computer Management window or the sdcli.exe command-line interface.

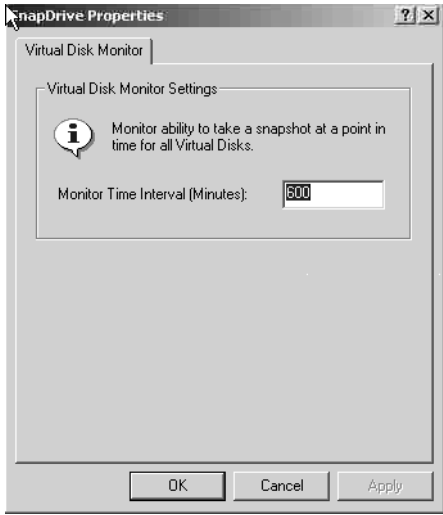
If you plan to make changes to the properties of virtual disks, you must first disconnect that disk.

The virtual disk properties are global—any changes you make to these properties affect all virtual disks on a Windows host.

Examining and modifying global virtual disk properties

To examine or modify the Virtual Disk Monitor settings, complete the following steps.

Step	Action
1	Select Start > Programs > Administrative Tools > Computer Management. Result: The Computer Management window (MMC) is launched.
2	Click SnapDrive in the left panel.
3	Click Action (from the menu choices on top of the MMC) and select Properties. Result: The SnapDrive Properties panel with the Virtual Disk Monitor tab selected is displayed.

Step	Action
4	In the Virtual Disk Monitor tab (as shown in the example below), enter a value in the Monitor Time Interval field, in minutes. The following values are valid: Default and minimum value—30 minutes Maximum value—10080 minutes (7 days) Disable the snapshot monitoring—0 minutes  The screenshot shows a window titled 'SnapDrive Properties' with a tab labeled 'Virtual Disk Monitor'. Inside, there's a section titled 'Virtual Disk Monitor Settings' containing an information icon and the text 'Monitor ability to take a snapshot at a point in time for all Virtual Disks.' Below this is a label 'Monitor Time Interval (Minutes):' followed by a text input field containing the number '500'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.
5	Click OK.

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, then click Action (from the menu choices on top of the MMC) and select Connect to Another Computer. Result: The Select Computer window is displayed.

Step	Action
3	In the Select Computer window, browse to or select the host production machine you want to administer remotely. Result: The Computer Management (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.

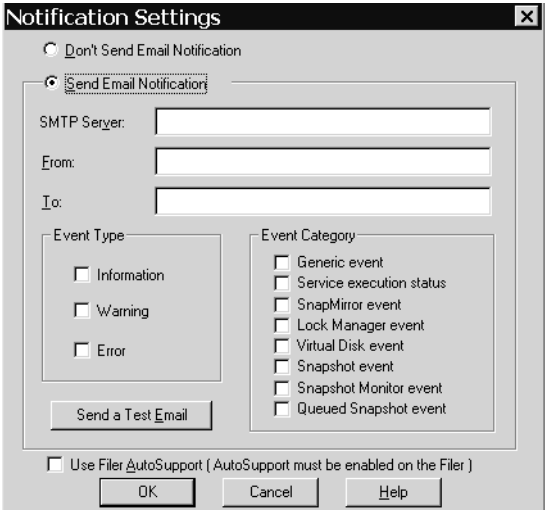
Note

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, then click Action (from the menu choices on top of the MMC) and select Notification Settings. Result: The Notification Settings window is displayed.

Step	Action
3	In the Notification Settings panel (as shown in the example below), perform the following actions: 1. Select Send Email Notification. 2. Enter the outgoing SMTP mail host, the From, and the To addresses. 3. Select one or more Event Types about which you want to be notified. 4. Select the Event Category items about which you want to be notified when the specified event types take place. 5. Select Use Filer Autosupport if you want to enable a subset of the Windows System Events for Autosupport on the filer. 6. Click OK.
	 Note 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.

This chapter does not describe how to archive your virtual disk snapshots to tape or other offline media. For that information, consult the documentation for the archiving application you use.

Topics in this chapter

This chapter discusses the following topics:

- ◆ “How snapshots work” on page 120
- ◆ “Creating snapshots” on page 122
- ◆ “Connecting to snapshots” on page 126
- ◆ “Restoring virtual disks from snapshots” on page 129
- ◆ “Deleting snapshots” on page 131

How snapshots work

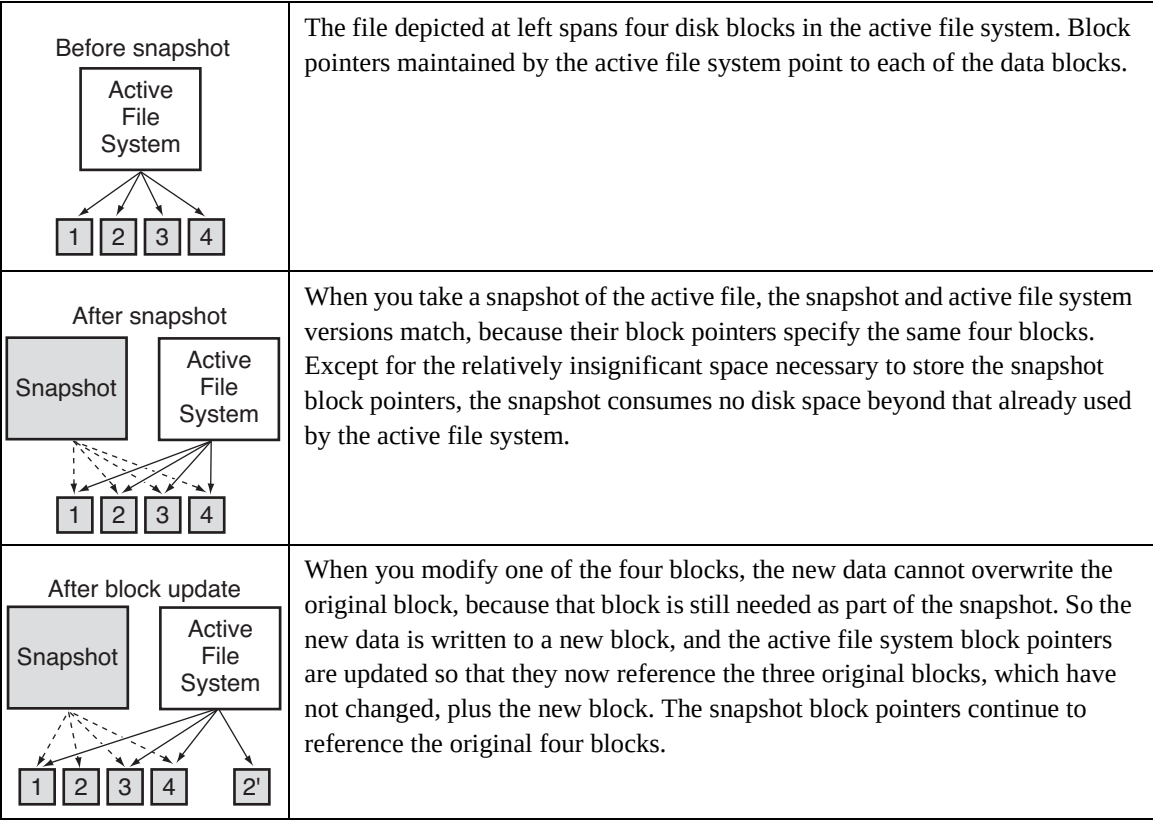
What a snapshot is

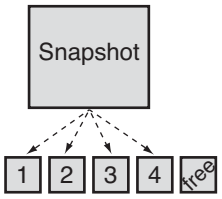
A snapshot is a point-in-time, read-only image of the filer volume. Snapshots can restore your databases rapidly if you encounter data corruption or other problems.

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.



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

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

You must be aware of the following Snapshot requisites:

- ◆ You must set the `vol options nosnapdir` command to `no` to disable the `nosnapdir` option.

Caution

If the `vol options nosnapdir` command is enabled (set to `yes`), it causes the snapshots in the SnapDrive MMC to be grayed out, thus causing the SnapManager backups to fail.

- ◆ 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.
- ◆ Snapshot operations on a single virtual disk actually take a snapshot of all the virtual disks on the volume. The exception to this is when the “-x” flag in the SnapDrive command line interface snapshot command is used: in that case, only the virtual disk drive specified by letter following the “-D” flag is flushed and a snapshot for it is created.

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

Step	Action
1	Right-click My Computer and select Manage from the pull-down menu.
2	In the left pane of the Computer Management window, double-click SnapDrive.
3	Right-click the virtual disk you want to take a snapshot of, then select New Snapshot on the drop-down menu.
4	Type an easy-to-interpret name for the snapshot in the text box on the Create Snapshot panel.  Example: expenses_db_15Jan03_4pm Result: Your snapshot is created under the following directory: /~snapshot/<i>snapshotname</i> <i>snapshotname</i> is the name of the snapshot Information about the snapshot also appears in a list with all the other previous snapshots for that virtual disk in the right panel of the Computer Management window.

Scheduling snapshots You need to create separate SnapDrive snapshot schedules for each volume that contains virtual disks.

To schedule SnapDrive snapshots, which must be handled by the Windows Task Scheduler, complete the following steps.

Step	Action
1	Select Start Menu > Settings > Control Panel > Scheduled Tasks.
2	Double-click Add Scheduled Tasks.

Step	Action
3	When the Scheduled Task Wizard appears, click Next.
4	After the next panel appears, click Browse, and navigate to the SnapDrive installation folder.
5	Double-click sdcli.exe.
6	After the following panel appears, type a name for the snapshot schedule in the text entry field, select from the list of frequencies, then click Next. 
7	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
8	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 leverage the Windows task scheduler to execute any of the sdcli.exe options, or even run a batch file containing numerous command operations.

Connecting to snapshots

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.

Space considerations

- Connecting to the data in a snapshot consumes additional space on the filer volume. The filer volume must have sufficient space for the following:
- ◆ The virtual disk in the active file system (including anticipated growth)
 - ◆ Snapshots of the virtual disk, including
 - ❖ The snapshot whose data you are connecting to
 - ❖ Future snapshots
 - ◆ The .rws file (You must leave at least as much free space as the combined size of all the changes made to the virtual disk).

Caution _____
Do not take snapshots of a virtual disk backed by snapshot, as this might cause you to run out of disk space on the filer volume.

When data is written, it goes to the virtual disk (.rws file) in the active file system. As long as such a virtual disk backed by a virtual disk in a snapshot exists, the snapshot it references remains locked, and it cannot be deleted.

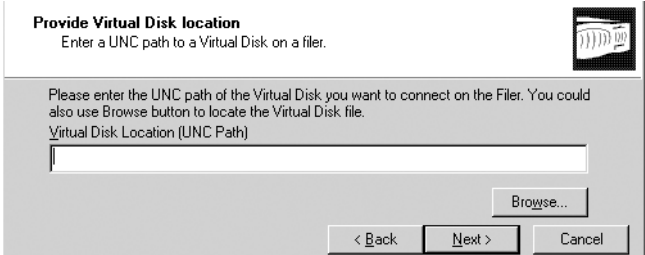
Connecting to a snapshot

To connect to a snapshot using SnapDrive, complete the following steps:

To enable browsing for the snapshots on your filer, set `cifs.show_snapshot` to On.

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	Right-click My Computer and select Manage from the pull-down menu.
2	Select SnapDrive, click Action, then select Connect Disk. Result: The Connect Disk Wizard appears.
3	Click Browse in the Virtual Disk Drive Location window, then browse to the <code>/~snapshot</code> directory of the filer volume holding the snapshot of the virtual disk.

Step	Action	
4	Type the path to the snapshot to connect. (Include the name of the virtual disk and the .lun extension as part of the path.) Alternatively, click Browse, navigate to the snapshot you want, then click OK. In any case, click Next when the path to the proper .lun file shows in the text box. 	
5	In the Virtual Disk Properties Window, examine the properties of the virtual disk, assign an unused drive letter, then click Next.	
6	Select an HBA port in the Select HBA window. <<Reviewer;; This applies to both FCP and iSCSI, Correct?>>	
7	If...	Then...
	The virtual disk created from the snapshot belongs to a single system	Go to Step 8.
	The virtual disk created from the snapshot is a Windows cluster resource	Select the cluster group that will own the cluster resource (or provide the information necessary for SnapDrive to create a new group), click Next, then go to Step 8.
8	Click Finish to connect to the snapshot of the virtual disk. Result: The Computer Management window displays the newly connected snapshot under SnapDrive in the left (“Tree”) panel. Details appear in the right 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.

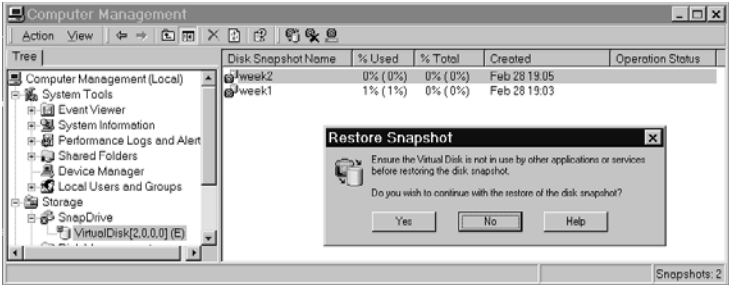
A virtual disk restore recalls a selected snapshot. During a restore, the entire virtual disk drive is restored from the snapshot. For a restore to succeed, no open connections can exist between the host machine (or any other application) and the files in the virtual disk.

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 is not monitoring the virtual disk. —————
2	Right-click My Computer and select Manage from the pull-down menu.
3	Double-click SnapDrive, then select the virtual disk you want to restore.

Step	Action
4	In the right pane, right-click the specific snapshot you want to restore, then select Restore 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.
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 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.

Step	Action
1	Right-click My Computer and select Manage from the pull-down menu.
2	Double-click SnapDrive, then select any virtual disk on the volume that contains the snapshot you want to delete.
3	In the right pane, right-click the specific snapshot you want to delete, then select Delete from the drop-down menu.
4	In the Delete Snapshot panel, click Yes to delete the snapshot you selected.

Archiving snapshots

About archives of SnapDrive backups

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

A SnapDrive backup consists of snapshots of the virtual disk drives that store the data files.

What to do: Using any popular Windows backup software package, back up a current snapshot of the virtual disk file itself.

It is important to back up a virtual disk in a SnapDrive snapshot. This is because a filer can store virtual disks from multiple hosts, but the only consistent virtual disks are those connected to the host that created the SnapDrive snapshot. Within the 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.

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. This 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.

Restoring virtual disks from archival media: 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 SnapManager® for Microsoft Exchange software. For more information about recovering virtual disks using SnapManager, see the current *SnapManager for Microsoft Exchange System Administrator's Guide*.

About this chapter This chapter explains how SnapDrive implements multipathing to connect hosts (initiators) to LUNs (target devices).

Topics This chapter covers the following issues:

- ◆ “Multipathing overview” on page 134
- ◆ “MPIO setup” on page 136
- ◆ “MPIO path management” on page 138

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 161.

Multipathing overview

What multipathing does

Multipathing facilitates redundant paths between a Windows host and a virtual disk.

This feature eliminates 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 simply as “MPIO,” is managed through the SnapDrive plugin under the Microsoft Management Console 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 Windows 2003 Server ❖ Enterprise Edition is required for Windows cluster configuration
Disk-access protocol	FCP

Component	Supported configurations
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.

Enabling MPIO

When MPIO is installed and you create a LUN, the virtual disk creation wizard automatically prompts you to specify an HBA port for each Windows cluster node in your configuration. See Step 15 of the section “Creating a virtual disk” on page 80.

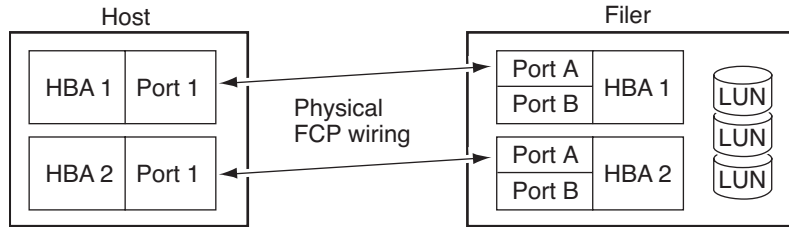
After you create the LUN, and it is connected to an HBA port on the host (or an HBA port on each node of your Windows cluster), the multipath management features become available.

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.

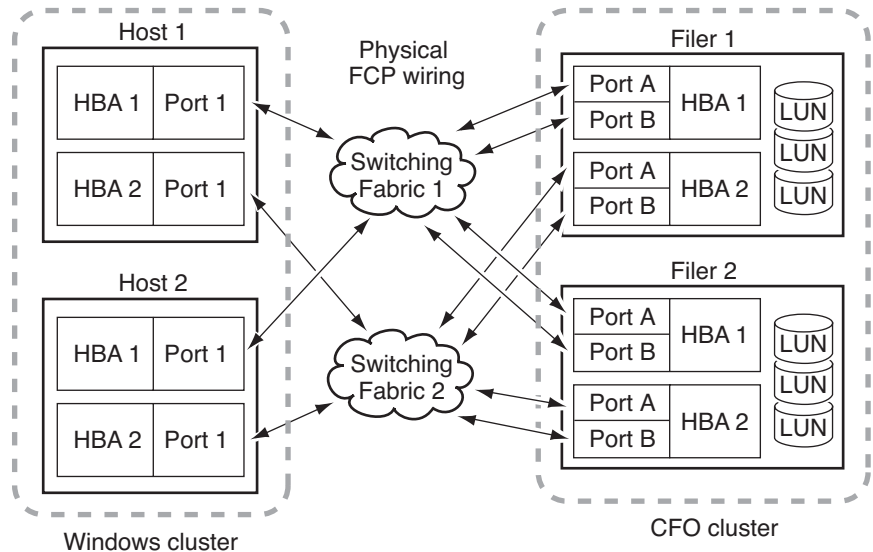


Windows cluster connected to a filer cluster through switches: The setup offering maximum protection against a single point of failure consists of a Windows cluster, a pair of FCP switches, and a filer cluster.

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.

Note

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



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.”

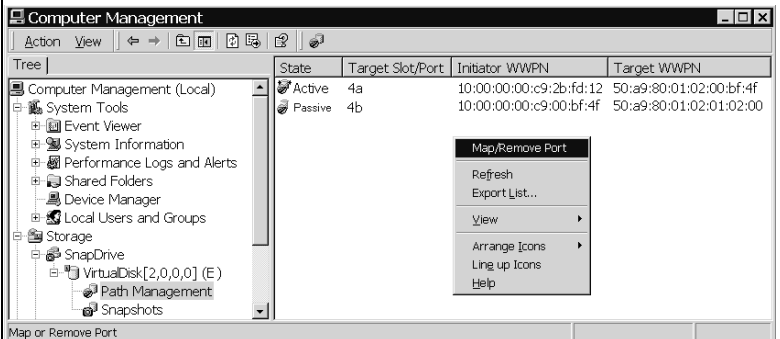
Interface	Method	How to access	
GUI	Main menu bar	Select Action > Path Management	
GUI	Tool bar	Click the Path Management icon, which is pictured at right	
GUI	Path Management icon in the left pane	Right-click the icon, then select Map/Remove Port	
Command line	Single command	Launch a cmd.exe window; 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 161.	
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. —————	

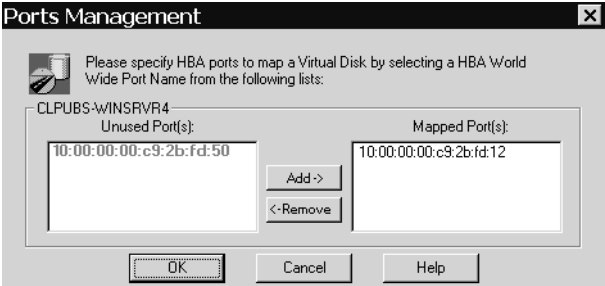
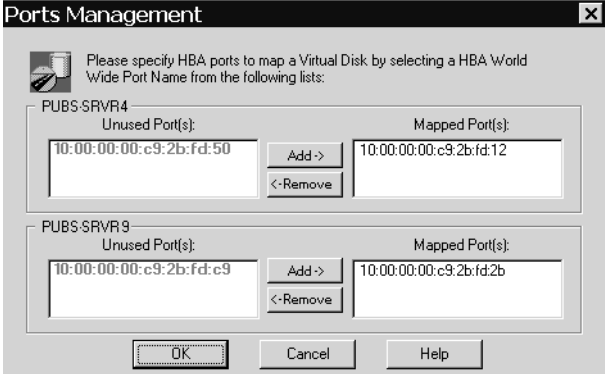
Example: The following procedure shows how to use one of the GUI methods to create an MPIO path. Specifically, the procedure involves mapping a target (a LUN) on the filer to an initiator (HBA port) on the host.

Note

You can use this same basic procedure to unmap MPIO paths as well. See also “Multipathing commands” on page 161 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 Map/Remove Port.



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 a port from the Unused Ports box in the Ports Management Screen, then click the right arrow to move it to the Mapped Ports box. Click OK to complete the procedure. 
4	To map MPIO paths on a Windows cluster, select a port for Node 1 from the Unused Port(s) box in the top half of the Ports Management Screen, then click the right arrow to move it to the Mapped Port(s) box. Repeat this procedure for the second node, this time moving the port from left to right in the bottom half of the screen. 

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 host bus. **Example:** “7a.”
- ◆ **Initiator WWPN**, which is the network identifier for a port on an HBA in the host. **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
<code>sdcli path add</code>	A LUN	Creation of a new path
<code>map FCP port</code>	A LUN	Creation of a passive path
<code>sdcli path activate</code>	A passive path	The passive path becomes active (and the active path becomes passive)

GUI command, sdcli command, or other event	On	Result
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 144
- ◆ “SnapMirror replication” on page 146
- ◆ “Enabling SnapMirror” on page 147
- ◆ “Connecting to destination volumes” on page 148
- ◆ “SnapMirror disaster recovery” on page 150

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*.
- ◆ You must manually establish 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 “- - -”. Make sure that the destination volume is offline when you do this. 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 configured exactly like the source volume:
 - ❖ It must be at least as large as the source volume.
 - ❖ It must have CIFS shares identical to those on the source volume.
- ◆ The Windows domain account used by the SnapDrive service must be a member of the local BUILTIN\administrators group on both the source and destination filers.
- ◆ The Windows domain account used to administer SnapDrive must have full access to the Windows domain to which both the source and destination filers belong.
- ◆ 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 44.
- ◆ 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 wish 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.
- ◆ You can create CIFS shares manually for the volumes on the destination filer. The data paths for these shares must match exactly those found on the source volumes. See your Data ONTAP *Data Protection Guide* for details.

SnapMirror replication

Replication upon snapshot creation

Each time you take a snapshot of a virtual disk, SnapDrive checks to determine that the virtual disk resides on a SnapMirror source volume. After the snapshot is complete, SnapDrive sends a SnapMirror update request to all the destination volumes associated with the source volume for that virtual disk.

Replication using rolling snapshots

When the SnapDrive Update Mirror option is On, SnapDrive creates and manages a “rolling” snapshot, which is used exclusively to facilitate frequent SnapMirror volume replication.

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

SnapDrive creates a new rolling snapshot every time the SnapDrive user interface initiates a mirror update operation for a specific virtual disk drive residing on a source volume.

SnapDrive begins the process by checking for previous rolling snapshots of the virtual disk set containing the specified virtual disk drive.

Examples: The following examples cover what might happen next:

- ◆ If SnapDrive doesn’t find any rolling snapshots containing the virtual disk image, it creates a rolling snapshot on the 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 snapshot and creates a fresh one to replace it. Then SnapDrive initiates a SnapMirror update.

Enabling SnapMirror

SnapMirror implementation rules

To use SnapMirror in conjunction with SnapDrive, perform the following tasks:

- ◆ Manually configure the source and destination volumes—but not the replication schedule—for SnapMirror replication.
- ◆ On both the source and destination filers, enable the iSCSI and FCP licenses, as appropriate for the virtual disk protocols you are using.

Enabling the Update Mirror option

To enable SnapDrive’s Update Mirror option, complete the following steps.

Step	Action	
1	Create a virtual disk on the source filer or source volume. See “Creating a virtual disk” on page 75 for instructions about how to create virtual disks.	
2	Right-click the virtual disk you just created.	
3	If...	Then...
	You want to use the Update Mirror option to replicate a virtual disk using rolling snapshots Note _____ This option is grayed out if no mirror is configured. _____	Select Update Mirror to create a mirrored virtual disk on the destination volume. Note _____ SnapDrive automatically updates the mirrored destination volume whenever snapshots are taken of virtual disks on the mirrored source volume. _____
	You do not want to use the Update Mirror option	Create a snapshot of your virtual disk using SnapDrive. Virtual disk replication takes place automatically.

Connecting to destination volumes

Before you connect Before connecting to a virtual disk in a SnapMirror destination volume, you must disable the SnapDrive Update Mirror. Next, you must restore the virtual disk from the most recent snapshot containing a valid image of that virtual disk. SnapDrive automatically performs all tasks required to connect virtual disk images in a SnapMirror destination volume.

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

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

Step	Action
1	Right-click My Computer and select Manage from the context menu.
2	Disconnect the failed source disk. See “Disconnecting virtual disks” on page 106 for more information.
3	Connect to the mirrored virtual disk on the SnapMirror destination filer. See “Connecting virtual disks” on page 98 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.

Step	Action	
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.	
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 36. 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.exe` command-line utility, which enables you to enter SnapDrive commands individually or through automation scripts.

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

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

Understanding `sdcli.exe` commands The `sdcli.exe` 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 -m host4 -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
-m host4 -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.exe` commands To run `sdcli.exe` commands, complete the following steps:

Step	Action
1	Using a host that has SnapDrive installed, select Start Menu > Run. . .
2	Type <code>cmd</code> in the dialog box entry field, then click OK.
3	After the Windows command prompt window opens, navigate to the directory on your host where SnapDrive is installed. Example: <pre>C: cd \Program Files\SnapDrive\</pre>
4	Enter the individual command you want to run. Make sure to include all input parameters in the proper order and to specify both required and desired command-line switches in any order. Example: <pre>sdcli disk disconnect -m host4 -d R</pre> Alternatively, enter the name and path of the automation script you want to run. Example: <pre>C:\SnapDrive Scripts\disconnect_R_from_host4.bat</pre>

Common command switches

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

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

Switch	Comment
-e	The name of an existing Windows cluster resource group, which is required only if the virtual disk is shared among Windows cluster nodes.
-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 one of the following two forms: ❖ <i>iqn.<iSCSI qualified name></i> ❖ <i>eui.<IEEE EUI-64 identifier></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 <code>lputilnt.exe</code> utility supplied with your NetApp FCP HBA Attach Kit. After you launch <code>lputilnt.exe</code>, navigate to Main Menu > Adapter > Configuration Data and select “16 - World-Wide Name” in the Region field. The available WWPNs appear in the list box directly beneath the Region field. When MPIO is running, you can specify up to four node-initiator pairs. The first <code>NodeMachineName</code> in the cluster applies to two of the available initiator WWPNs; the other <code>NodeMachineName</code> applies to the remaining pair of initiator WWPNs.
-ID	An MPIO path ID (For details, see “Understanding MPIO path IDs” on page 161).
-m	The host on which the virtual disk is mounted. You can use an IP address or a machine name to identify the host. (The <code>-m</code> switch is optional. If you don’t specify this switch, the <code>sdcli.exe</code> command is run against a virtual disk attached to the machine used to run the command.)
-n	The name and description of a Windows cluster resource group to be created as part of the associated command. This switch is required only if you need to create a Windows cluster resource group to facilitate the sharing of a virtual disk among Windows cluster nodes.
-p	The UNC path to the location of the virtual disk file on the filer. This string takes the following form: <code>\\filename\sharename\virtualdiskfilename{.lun .vld}</code>

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. (See “Understanding volume size” on page 11).

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 <code>sdcli.exe</code> 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 may also be used for the connection.	
Syntax: <code>sdcli iscsi_target connect -i InitiatorName -t TargetName -np IPAddress IPPort [-c CHAPName CHAPPassword]</code>	
Example: <code>sdcli iscsi_target connect -i iqn.1991-05.com.microsoft:node2 -t iqn.1992.08.com.netapp:sn33604307 -np 168.34.50.52 3260</code> 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: <code>sdcli iscsi_target disconnect -i InitiatorName -t TargetName</code>	
Example: <code>sdcli iscsi_target disconnect -i iqn.1991-05.com.microsoft:node2 -t iqn.1992.08.com.netapp:sn.33604307</code> 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 of 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 of the iSCSI targets that the specified initiator is connect to, as well as all portals those targets are available through or connected to.

Virtual disk commands

Supported operations The `sdcli.exe` utility supports the following virtual disk-related operations: create, connect, delete, disconnect, expand, list, and convert.

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 -m 133.25.61.44</pre> The preceding example creates a dedicated, 1 GB virtual disk file named “mktng.lun” in the filer2 volume named “sd_vds_only.” Next, it connects this virtual disk as drive “R:” to the host, which has been specified by IP address, rather than machine name. <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 <code>sdcli</code> 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 a Windows cluster.

Operation

disk connect connects a virtual disk 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 LUN-type virtual disk located in the filer2 volume “sd_vds_only” and named “mktng.lun,” which belongs to the Windows cluster resource group “tech_mktng” on the “mktng” cluster. MPIO paths are connected for both nodes on the cluster.

disk delete deletes a virtual disk. The virtual disk must be connected (mapped to a Windows drive letter) for the command to succeed.

Syntax:

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

Example:

```
sdcli disk delete -p \\133.25.61.62\sd_vds_only\mktng.lun -m host3
```

The preceding example deletes the virtual disk file “mktng.lun,” which was connected to host3, from the “sd_vds_only” volume on the filer identified by the IP address “133.25.61.62.”

Operation

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

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 -m 133.25.61.44
```

The preceding example forces disconnection of the virtual disk file “mktng.lun,” which is in the “sd_vds_only” volume on filer2, from the host whose IP address is 133.25.61.44. Because the `-f` switch is being used, all open files in the virtual disk might be lost or corrupted.

`disk expand` expands the disk by a user-specified size, as long as that figure falls within the SnapDrive-specified minimum and maximum values.

Syntax:

```
sdcli disk expand [-m MachineName>] {-p UNCpath | -d DriveLetter} -z DriveSizeIncrement
```

Example:

```
sdcli disk expand -z 1024 -d p
```

The preceding example increases the virtual disk mapped to “P:” by 1 GB. (In practice, SnapDrive expands the disk by the amount specified by `-z`, plus a certain increment required for system overhead.)

Operation

`disk list` displays a list of all the virtual disks connected to the host.

Syntax:

```
sdcli disk list [-m MachineName]
```

Example:

```
sdcli disk list -m host1
```

The preceding example lists all the SnapDrive virtual disks mapped to drive letters on host1. 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)

`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 | -d DriveLetter} [-l LUNName]
```

`-l` is the file name, including the `.lun` file extension, of the new virtual disk.

Example:

```
sdcli disk convert -m 133.25.61.44 -d j -p \\filer2\sd_vds_only\mktng.vld -l  
recycledvld.lun
```

The preceding example converts the virtual disk file “mktng.vld” into a LUN-type virtual disk named “recycledvld.lun.” (“mktg.vld” is in the “sd_vds_only” volume on filer2 and mapped to the drive letter “J:” on the host with the IP address 133.25.61.44.)

Multipathing commands

I

Supported operations

The `sdcli.exe` command supports the following MPIO-related operations: create, delete, connect, disconnect, expand, list, and convert.

Understanding MPIO path IDs

For all multipathing-related operations executed through `sdcli.exe`, *pathID* specifies the virtual path created by mapping a LUN-type 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: 4000d07

- ◆ 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 0A and 0F, 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.exe`: activate, add, disable, enable, list, remove, and version.

Operation
path activate directs I/O through the specified path and causes the currently active path to become passive. (This command can only be performed on a passive path.) Syntax: <pre>sdcli path activate [-m <i>MachineName</i>] -ID <i>PathID</i></pre> Example: <pre>sdcli path activate -m host3 -ID</pre> The preceding example activates the path associated with pathID 4000d07 and makes passive whatever path was active when the command was run.
path add creates a new virtual path from the initiator on the host to the virtual disk on the 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 -m host3 -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 host3 to the virtual disk “mktng.lun” located on the “sd_vds_only” volume on filer2, assigning the new path to the initiator port associated with WWPN 10:00:00:00:c9:2b:fd:13.
path disable 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 4000d07</pre> The preceding example places the currently passive path (4000d07) on standby.
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 67112199</pre> The preceding example changes the status of path 67112199 from disabled to enabled.

Operation
<code>path list</code> enumerates all virtual paths and their status for the specified LUN-type 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 LUN-type virtual disk mapped to “Z:” on the host running the SnapDrive command.
<code>path remove</code> 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 file on the filer2 volume “sd_vds_only.”
<code>path version</code> indicates whether NTAPDSM is installed on the specified system. If the -m switch is not specified, the command is executed against the host issuing the <code>sdcli</code> command. Syntax: <pre>sdcli path version [-m <i>MachineName</i>]</pre> Example: <pre>sdcli path version -m host4</pre> The preceding command, which was issued from host3, returns information about whether NATDSM is installed on host4.

Snapshot commands

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

Operation
sdcli snap create 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> -x causes snapshots to be created only for the drives specified by the -D switch. Otherwise, snapshots are created for all the disks on the filer volume(s) used by the listed drives. Example: <pre>sdcli snap create -m host 3 -s Jun_13_03 -D j k l</pre> 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 snapshot(s) created will be consistent for all virtual disks contained by those volumes.
sdcli snap delete deletes an existing snapshot. 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 “Jun_13_03” that is associated with the virtual disk mapped to “K:” on the host running the sdcli command.
sdcli snap restore replaces the current virtual disk image in the active file system with the point-in-time image captured by the specified snapshot. Syntax: <pre>sdcli snap restore [-m MachineName] -d DriveLetter -s SnapshotName</pre> Example: <pre>sdcli snap restore -d l -s Jun_13_03 -m host3</pre> The preceding example restores the virtual disk mapped to “L:” on host3 to its state when the snapshot named “Jun_13_03” was taken.

Operation
sdcli 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.”
sdcli 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 machine running sdcli.
sdcli 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> [-rw]</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 name of the host running the SnapDrive command. -k refers to the drive letter assigned to the virtual disk in the active file system. Example: <pre>sdcli snap mount -m host4 -r host3 -k j -s Jun_13_03 -d t</pre> The preceding example maps the snapshot named “Jun_13_03” to “T:” on host4. This snapshot represents a point-in-time image of the virtual disk mapped to “J:” on host3.

Operation
snap unmount disconnects a snapshot of a virtual disk that is mounted as a virtual disk. Syntax: <pre>sdcli snap unmount [-m <i>MachineName</i>] -d <i>DriveLetter</i> [-f]</pre> 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: <pre>sdcli snap unmount -m host3 -d k</pre> The preceding example disconnects the snapshot mapped to “K:” on host3. <pre>sdcli snap unmount -m host3 -d k -f</pre> The preceding example forces disconnection of the snapshot mapped to “K:” on host3.
snap update_mirror updates the virtual disk to a SnapMirror destination volume residing on the same or a different filer. Syntax: <pre>sdcli snap update_mirror [-m <i>MachineName</i>] -d <i>DriveLetter</i></pre> Example: <pre>sdcli snap update_mirror -m host3 -d l</pre> The preceding example updates the SnapMirror destination for the virtual disk mapped to “L:” on host3. 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

For customer convenience, this appendix gathers in a single location the various SnapDrive requirements and recommendations mentioned elsewhere in this document.

- Assumed competence
- The installers and administrators of SnapDrive deployments should be familiar with the following topics:
- ◆ 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
 - ◆ iSCSI, 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 2003 server management, if your hosts have Windows 2003 installed
 - ◆ Network Appliance filer management

Host requirements

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

Note

Be sure to read the important qualifications that follow this table.

Component	Minimum requirement
CPU	500 MHz Pentium® III
Memory	256 MB RAM
HBAs	Emulex LP9002L-F2 host bus adapters
NICs	Intel® PRO/1000 Gigabit server adapters

Component	Minimum requirement
Operating system	Windows 2000 Server (with SP2 or SP3) or Windows 2000 Advanced Server (with SP2 or SP3) or Windows 2003 Server (Standard Edition) or Windows 2003 Server (Enterprise Edition)
Microsoft hot fixes	306185 (must be installed with SP2) 307939 (must be installed with SP2 if Windows cluster service is deployed) 816990 (must be installed with SP3) 815198 (must be installed with SP3 if MPIO is deployed) <<Reviewer:: any hot fixes to be added here?>>

HBAs and NICs: To determine the exact number and type of HBAs and NICs required by each host in the SnapDrive configuration you selected, consult “” on page 20 and “FCP configurations” on page 24.

Interface drivers: Before installing SnapDrive, make sure to obtain the latest firmware and drivers for the HBAs and NICs you are using. This ensures high network bandwidth and ease of configuration.

- ◆ The latest Intel® GbE driver and software is available on the Intel Web site at the following URL: <http://downloadfinder.intel.com>. From this gateway, use the drop-down menus to navigate to the Web page labeled Intel® PRO/1000 Gigabit Server Adapter.
- ◆ 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 latest iSCSI driver is available at the NOW software download site: <http://now.netapp.com/NOW/cgi-bin/software>. From this gateway, navigate to the iSCSI Host Support Kit for Windows download page.

Service Packs: <<Patrick to update this section.>> If you plan to use MPIO, you must install SP3. <<Reviewer:: what is checked for Windows 2003?>>

Note

The SnapDrive installation wizard checks for SP3, and it does not let you install the MPIO drivers unless your host is already upgraded to SP3. If you plan to install MPIO among your SnapDrive options, your only choice is to apply SP3.

When deploying MPIO without a Windows cluster, you can use Windows 2000 Server or Advanced Server. Both options require the additional installation of SP3 and hot fixes 816990 and 815198.

Hot fixes: If you elect to use SP2 for non-MPIO configurations, you must install certain hot fixes on your machine, as explained in the following section.

- ◆ [Is this hot fix needed for anything other than the VLD problem? If not, can delete whole bullet] If your host is running SP2, you must install hot fix 306185 on your host *before* you install SnapDrive. This hot fix is available on the SnapDrive CD-ROM. Alternatively, you can download it from the SnapDrive Web site:

<http://now.netapp.com/NOW/download/software/snapdrive/2.1/>.

This hot fix eliminates an erroneous reboot prompt that pops up whenever you mount or dismount a VLD drive.

When you install SnapDrive, the InstallShield wizard automatically enables hot fix 306185 by inserting the following registry entries.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Explorer
Value: DisableFixedDiskDriveAutorun
Value Type: REG_DWORD
Value Data: 1
```

Additional information about this hot fix is available in the Microsoft Knowledge Base article 306185 at www.Microsoft.com.

- ◆ If you plan to use Windows clustering with SP2, you must download and install hot fix 307939, which corrects a problem where the cluster service does not start unless a storage unit is already turned on. This hot fix is available on the SnapDrive CD-ROM. Alternatively, you can download it from the SnapDrive web site at

<http://now.netapp.com/NOW/download/software/snapdrive/2.1/>.

Note

Windows 2000 SP3 automatically installs hot fixes 306185 and 307939. When you install SnapDrive, the InstallShield wizard enables hot fix 306185. Therefore, hosts running SP3 do not require the manual installation or enabling of hot fixes 306185 and 307939.

- ◆ If your host is running SP3, you must install hot fix 816990 on your host before you install SnapDrive. This hot fix must be requested directly from Microsoft Product Support Services: <http://support.microsoft.com>.

This hot fix eliminates an erroneous error message when you shut down your Windows 2000 host. For details, read Knowledge Base article 816990 at the Microsoft Web site: <http://support.microsoft.com>.

- ◆ If your host is running MPIO on either Windows 2000 Server or Advanced Server, you must install SP3, then you must install both hot fixes 816990 and 815198 before you install SnapDrive.

Hot fix 815198, which is described in the Microsoft Knowledge Base article of the same number, eliminates certain incorrect displays of WMI information when MPIO is installed. This hot fix must be requested directly from Microsoft Product Support Services: <http://support.microsoft.com>.

Filer requirements

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

Note

Be sure to read the important qualifications that follow this table.

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

Note

<<Reviewer:: I changed “VLD” to “iSCSI” in this note. Are these statements now correct?] 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.

Similarly, the iSCSI and FCP licenses supplied with SnapDrive enable all the NFS functionality necessary for using virtual disks. If you also want *full-featured, direct NFS access* to a particular filer, you must install a separate NFS 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 44.)

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

Note

When you specify the SnapDrive service account, be sure to assign an account with a password that does not change. If you do change the password, remember to do so through the Services icon on the Windows control panel.

- ◆ Both the filer and the Windows domain to which the host belongs must be able to access the service account.nly.)
- ◆ 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.
- ◆ CIFS setup must be run on the filer.

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)
Volume	create_ ucode	On	◆ Disk creation ◆ Disk connection
Volume	convert_ ucode	On	◆ Disk creation ◆ Disk connection

Option type	Parameter	SnapDrive setting	When
Filer	Snapshot schedule	Off	◆ Disk creation ◆ Disk connection

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

Users should remain aware of the following SnapDrive 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 jumbo frames.
- ◆ SnapDrive does not support the use of NIC Teaming on Windows hosts.
- ◆ SnapDrive does not support the use of NIC virtual interfaces (VIFs) on filers.
- ◆ SnapDrive does not support the use of LUN cloning.
- ◆ A Windows host running SnapDrive can connect directly to the physical, “hosting” filer (vfiler0) created by the Data ONTAP MultiStore™ feature, but it cannot connect to any virtual filer partitions.

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.

- ◆ The Spanning Tree protocol should be disabled to keep virtual disk reconnection times to a minimum after the host reboots.

Note

Dedicated virtual-disk volumes are particularly important for filers running Data ONTAP 6.4.2, which uses file-based space reservation. Because all virtual disks in the dedicated volumes have space reservations, they are always written to disk. By contrast, non-virtual disk files that lack space reservations might not get written properly to disk.

- ◆ Volumes used to store files on virtual disks should not be shared with non-host machines or applications not running on a host.
- ◆ 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.

Understanding SnapDrive 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 2000 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 a connection initiated by running %SystemRoot%\System32\termsrv.exe at the command prompt of a Windows 2000 computer on the same network as the SnapDrive host. This type of session enables you to create a desktop session on the host—and applications accessible from that desktop.

Be aware of the following significant potential drawbacks to Terminal Service sessions:

- ❖ Not all the error messages visible on the host console (session 0) are visible within a Terminal Service session.
- ❖ Virtual disks created through a Terminal Service session are not always visible in the SnapDrive plug-in, and when they are, the sdcli disk disconnect command sometimes appears to fail when you execute it.
- ❖ The list of available drive letters will not be up-to-date, especially if new virtual disks were created (either by your Terminal Service session or some other agency) since you last logged onto the host using the SnapDrive service account.

To compensate for the preceding problems, you can log off the Terminal Service session and then log on again. The newly created or disconnected disks should appear in their proper states.

SnapDrive interface capabilities

Not all 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

SnapDrive-related operation	Recommended interface
Creating and managing virtual disks	◆ Host console ◆ Remote Management session to the host ◆ Terminal Service (See the final bulleted item in the section preceding this table.)

Index

Symbols

/etc/hosts file 45
/etc/hosts.equiv file 45

C

CIFS v
cmd 66

D

df -r (filer command) 12
disk
 hot spare 10
 reconstruction 10
document
 intended audience v

F

failover 5, 19
 definition 2
FCP 3
 adapter ports on filers 8
 connections 8
 definition 2, 3
 driver 6
 HBA Attach Kit 6
 SCSI commands 8
 SnapDrive feature availability 20
filer
 BUILTINadministrators group 44
 command execution v
 licence 33
 options 33
 preparation 32
 requirements 22
filer console
 definition 173
FilerView v, 12, 33, 35, 36, 38, 42, 43, 45, 78, 122,
132, 174
 definition 173

H

host console 174, 175
 definition 173
hot spare disk 10

I

IP address 46

L

LUNs
 conversion to 59

N

NTFS 7

R

RAID array 7, 10
Remote Administration 5, 44, 78, 173
 definition 173
 requirements 114
 reunning 114
rsh
 enabling 45

S

SAN 8
SnapDrive
 cautions and recommendations 34
 command-line interface 5
 feature availability 20
 limitations 34
 selecting configurations 19
 service account 44
snapshot 13
snapshots
 archiving 132
 deleting 131
space reservation 12

T

Telnet v, 33, 35, 37, 38, 48, 49
 description 173
Terminal Service 71, 78, 114, 173, 174, 175
 definition 174

V

virtual disk
 converting 59
 definition 7
VLD
 conversion to LUN 59
volume

configuration recommendations 35
creation 36
creation guidelines 35
preparation 35
storage requirements 11

W

WAFL 7
Windows host
 preparing 29
 requirements 29
WordPad 46