

SnapDrive® 6.3 for Windows®

Installation and Administration Guide

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

Part number: 215-05261_A0
July 2010

Contents

Copyright information	13
Trademark information	15
About this guide	17
Audience	17
Terminology	17
Keyboard and formatting conventions	18
Special messages	19
How to send your comments	19
SnapDrive overview	21
What SnapDrive does	21
What SnapDrive does not do	22
Recommendations for using SnapDrive	22
SnapDrive components	23
SnapDrive licensing	24
How LUNs work	24
How the storage system interacts with the LUN	24
How Windows hosts interact with a LUN	24
LUN capabilities and limitations	25
Protocols for LUN access	25
How data is accessed from LUNs	25
Disk allocation considerations	25
RAID group configuration	25
Hot spare disks	26
How many hot spares you should have	26
How aggregates work	26
How volume space is used	27
Volume size rules	27
Volume and storage system options set by SnapDrive	27
What space reservation is	28
Disk space usage with space reservation	29
What fractional reserve is	29
SnapDrive for Windows GUI icon descriptions	31

Features added in SnapDrive 6.3 for Windows	35
Features supported	37
Support for VMDKs in NFS and VMFS datastores	37
SnapDrive VMDK support limitations	38
Support for space reclamation in VMDK files in NFS datastores	38
SnapDrive support in Windows Server 2008 Server Core	39
Server Core limitations	39
Requirements for managing SnapDrive on Windows Server Core systems	40
Support for dynamically adding and removing pass-through disks on Hyper-V virtual machines	40
Hyper-V pass-through disk support limitations	41
Support for restoring data at the file level	41
Support for storage system access control	42
Using storage system access control	42
Support for ESX iSCSI initiators with SnapDrive for Windows	43
ESX iSCSI initiator limitations	44
SnapDrive changes with MMC 3.0	44
Using MMC 3.0 Action pane	44
Error messages in MMC 3.0	45
MultiStore support	45
HTTP and HTTPS transport protocol support	45
Adding storage system capabilities for HTTP users	46
IPv6 support	47
SnapVault support	47
VMware support	47
VMware-related limitations	48
Enabling and disabling vCenter or ESX logon from SnapDrive MMC	48
Minimum vCenter permissions required for SnapDrive operations	49
VMware VMotion support	49
GPT partition support	50
LUN boot disk (SAN booting) support	50
Cluster support	50
Microsoft clusters on ESX reference	51
Support for Microsoft cluster shared volumes	51
Support for Microsoft clusters using FC RDM LUNs	52

Overview of installing or upgrading SnapDrive	55
Preparing to install or upgrade SnapDrive for Windows	57
Documents to read before installing SnapDrive	58
Considerations for determining SnapDrive configurations	59
Preparing hosts for SnapDrive	59
Minimum SnapDrive host requirements	60
Minimum SnapDrive requirements for VMware ESX Guest OS	62
Determining whether HBA or MPIO components are installed	64
Preparing storage systems for SnapDrive	64
Minimum SnapDrive storage system requirements	64
Determining which licenses are enabled on a storage system	65
Preparing a volume for SnapDrive	65
Configuring access for SnapDrive	66
SnapDrive service account requirements	66
When pass-through authentication might be required	67
Configuring SnapDrive pass-through authentication	67
User account requirements for SnapDrive Web services	68
Preparing to upgrade SnapDrive	69
Installing or upgrading SnapDrive	71
Installing or upgrading the FC or iSCSI components	71
Installing or Upgrading the iSCSI Software Initiator	72
Installing or upgrading the SnapDrive components	73
Preparing to install SnapDrive on Windows Server 2008 Server Core	76
Enabling remote administration on the Server Core system	77
Renaming the Server Core system	77
Joining the Server Core system to a domain	77
Disabling Windows Server Core firewall	78
Installing Microsoft Visual C++ 2008 Redistributable Package on the Server Core system	78
Installing .NET Framework on Windows Server 2008 R2 Server Core	78
Installing SnapDrive on Windows Server 2008 Server Core	79
Performing unattended SnapDrive installations	80
Enabling SnapDrive to communicate through the Windows Firewall	80
Managing SnapDrive	83
Managing host-side SnapDrive licenses	83
Enabling SnapDrive notification settings	84

Setting a preferred IP address	85
Stopping and starting the SnapDrive service	85
Adding and removing initiators with SnapDrive	86
Administering SnapDrive remotely	86
Adding a remote SnapDrive instance	87
Deleting a remote SnapDrive instance	88
Managing SnapDrive remotely using Connect to another computer	88
Enabling RBAC for use with SnapDrive for Windows	89
Using role-based access control (RBAC) with DataFabric Manager server	89
Enabling RBAC on the storage system	91
Configuring SnapDrive for Windows to use RBAC	91
Creating SnapDrive user roles on DataFabric Manager server	92
Assigning roles to SnapDrive users on DataFabric Manager server	93
Managing iSCSI sessions	95
iSCSI software initiator node naming standards	95
Establishing an iSCSI session to a target	96
How SnapDrive uses CHAP authentication	97
Disconnecting an iSCSI target from a Windows host	97
Disconnecting a session to an iSCSI target	98
Examining details of an iSCSI session	99
Creating LUNs	101
Rules for creating LUNs	101
About volume mount points	102
Creating a dedicated LUN	102
Creating a shared LUN	106
Creating a LUN as a quorum on a Windows 2003 cluster	110
Windows Server 2008 failover cluster support	113
Configuring a Windows Server 2008 failover cluster witness disk	113
Creating an RDM LUN on a guest OS	114
Creating a highly available Hyper-V virtual machine using SnapDrive	118
Managing LUNs	121
Guidelines for connecting LUNs	121
Connecting to a LUN	122
Guideline for managing RDM LUNs not created in SnapDrive	124
Connecting to an RDM LUN on a guest OS	124
Making drive letter or path modifications to a LUN	127

Adding, removing, or changing a drive letter or path for an existing LUN	127
Moving a mount point with Windows Explorer	128
Guidelines for disconnecting or deleting LUNs	128
Disconnecting a LUN	129
Deleting a LUN	130
Deleting folders within volume mount points	131
Guidelines for resizing disks	131
Resizing a disk	132
Resizing a quorum disk	133
Managing LUNs not created in SnapDrive	133
Guidelines for renaming LUNs	135
Managing space on storage system volumes	137
What SnapDrive fractional space reservation monitoring does	137
Configuring space reservation monitoring	137
Using the storage access control tool to enable thinly provisioned LUNs	138
What Space Reclaimer does	139
Guidelines for using Space Reclaimer	139
Starting Space Reclaimer	140
Stopping Space Reclaimer manually	141
Reasons for SnapDrive to automatically stop Space Reclaimer	141
Managing Snapshot copies	143
Reasons for creating Snapshot copies	143
Restrictions on Snapshot copy creation	144
Creating a Snapshot copy	144
Scheduling Snapshot copies	145
About using FlexClone volumes in SnapDrive	146
Prerequisites for using FlexClone volumes with SnapDrive	147
About read/write connections	147
Snapshot copy cautions	147
Connecting to a LUN in a Snapshot copy	148
How LUN restoration from Snapshot copies works	149
About the Data ONTAP LUN clone split (rapid LUN restore) feature	150
Restoring a LUN from a Snapshot copy	150
Checking LUN restore status	151
About volume-based Snapshot copy restoration with SnapDrive	152

Deleting a Snapshot copy	152
Problems deleting Snapshot copies due to busy snapshot error	153
Overview of archiving and restoring Snapshot copies	153
Using SnapVault with SnapDrive	155
Considerations for using SnapVault	155
Initiating SnapVault backups from SnapDrive	155
SnapDrive integration with Protection Manager	157
How SnapDrive integrates with Protection Manager	157
Dataset concepts	157
Understanding the Volume Shadow Copy Service	159
Overview of VSS	159
SnapDrive VSS requirements	160
Typical VSS backup process	160
Troubleshooting the VSS Hardware Provider	161
Viewing installed VSS providers	161
Verifying that the VSS Hardware Provider was used successfully	162
Verifying your VSS configuration	162
SAN booting with SnapDrive	165
What SAN booting is	165
How SnapDrive supports SAN booting	165
Using SnapMirror with SnapDrive for Windows	167
SnapMirror overview	167
Types of SnapMirror replication	167
How SnapDrive manages rolling Snapshot copies	168
How rolling Snapshot copies are named	169
Requirements for using SnapMirror with SnapDrive	169
Initiating replication manually	170
Connecting to a LUN in a mirrored destination volume	171
Restoring a volume on a SnapMirror destination	172
Recovering a cluster from shared LUNs on a SnapMirror destination	173
Configuring the cluster service to start manually	173
Creating a temporary quorum disk	174
Starting the cluster service with the -fixquorum option	174
Connecting to the new quorum disk	174
Connecting to a shared LUN on the SnapMirror destination volume	175
Unattended SnapDrive installation reference	177

SnapDrive command line installation syntax	177
SnapDrive command line installation switches	178
SnapDrive unattended installation examples	185
Typical SnapDrive configurations	187
SnapDrive iSCSI configurations	187
Single host direct-attached to a single storage system using iSCSI	187
Single host attached to a single storage system through a GbE switch	188
Single host attached to a single storage system through a dedicated switch	188
Windows cluster connected to a storage system cluster through a dedicated GbE switch	189
SnapDrive FC configurations	190
Single host direct-attached to a single storage system using FC	190
Single host attached to a single storage system through an FC switch	190
Windows cluster attached to a storage system active/active configuration through an FC switch	191
SnapDrive MPIO configurations	191
Single host direct-attached to a single storage system using MPIO	192
Windows cluster attached to a storage system active/active configuration through a GbE switch using MPIO	192
Windows cluster attached to a storage system active/active configuration through an FC switch using MPIO	193
Storage system access control reference	195
Storage system access control operations list	195
Storage system access control roles	196
Storage system access control commands	198
Storage system access control command examples	198
SnapDrive for Windows to DataFabric Manager role mappings	201
SnapDrive command-line reference	205
About sdcli commands	205
Executing sdcli commands	206
Common command switches	207
Configuration commands	208
The sysconfig list command	208
License commands	209
The license set command	209

The license list command	209
The license remove command	209
Initiator group management commands	210
The igroup list command	210
The igroup create command	210
The igroup rename command	211
The igroup delete command	211
Fractional space reservation monitoring commands	212
The spacemon list command	212
The spacemon set command	212
The spacemon snap_delta command	213
The spacemon snap_reclaimable command	213
The spacemon vol_info command	214
The spacemon delete command	214
SnapManager for Virtual Infrastructure commands	214
The smvi_config list command	214
The smvi_config set command	215
The smvi_config delete command	215
Space reclamation commands	215
The spacereclaimer start command	215
The spacereclaimer stop command	216
The spacereclaimer analyze command	216
The spacereclaimer status command	217
Preferred IP address commands	217
The preferredIP set command	217
The preferredIP list command	217
The preferredIP delete command	218
iSCSI connection commands	218
The iscsi_target disconnect command	218
The iscsi_target list command	218
iSCSI initiator commands	219
The iscsi_initiator list command	219
The iscsi_initiator establish_session command	219
The iscsi_initiator terminate_session command	220
LUN commands	220
The disk create command	221

The disk connect command	222
The disk delete command	223
The disk disconnect command	223
The disk resize command	224
The disk expand command	224
The disk add_initiator command	225
The disk remove_initiator command	225
The disk list command	226
The disk add_mount command	227
The disk remove_mount command	227
Snapshot copy commands	228
The snap create command	228
The snap delete command	229
The snap list command	229
The snap mirror_list command	230
The snap mount command	230
The snap rename command	231
The snap restore command	231
The snap unmount command	232
The snap update_mirror command	233
The snap restore_volume_check command	233
The snap restore_volume command	234
SnapVault commands	234
The snapvault verify_configuration command	235
The snapvault snapshot_rename command	235
The snapvault snapshot_delete command	235
The snapvault archive command	236
The snapvault relationship_status command	236
The snapvault snap_list command	236
DataFabric Manager commands	237
The dfm_config list command	237
The dfm_config set command	237
The dfm_config delete command	237
The dfm_config rbaccache command	238
Transport protocol commands	238
The transport_protocol list command	238

The transport_protocol set command	239
The transport_protocol delete command	239
Virtual server commands	240
The vsconfig list command	240
The vsconfig set command	240
The vsconfig dslist command	240
The vsconfig delete command	241
Index	243

Copyright information

Copyright © 1994–2010 NetApp, Inc. All rights reserved. Printed in the U.S.A.

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

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

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

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

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

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

Trademark information

All applicable trademark attribution is listed here.

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

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>.

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

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

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetCache is certified RealSystem compatible.

About this guide

You can use your product more effectively when you understand this document's intended audience and the conventions that this document uses to present information.

This guide applies to Microsoft Windows servers running SnapDrive for Windows.

Next topics

[Audience](#) on page 17

[Terminology](#) on page 17

[Keyboard and formatting conventions](#) on page 18

[Special messages](#) on page 19

[How to send your comments](#) on page 19

Audience

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

This guide is for system administrators with a working knowledge of Microsoft Windows server. The discussion assumes familiarity with the following topics:

- Microsoft Windows server administration
- Network functions and operations
- Basic concepts for moving data over a network
- Your operating system, network, and storage system
- FCP and iSCSI LUN protocols

Terminology

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

array LUN	The storage that third-party storage arrays provide to storage systems running Data ONTAP software. One array LUN is the equivalent of one disk on a native disk shelf.
LUN (logical unit number)	A logical unit of storage identified by a number.
native disk	A disk that is sold as local storage for storage systems that run Data ONTAP software.

native disk shelf	A disk shelf that is sold as local storage for storage systems that run Data ONTAP software.
storage controller	The component of a storage system that runs the Data ONTAP operating system and controls its disk subsystem. Storage controllers are also sometimes called <i>controllers</i> , <i>storage appliances</i> , <i>appliances</i> , <i>storage engines</i> , <i>heads</i> , <i>CPU modules</i> , or <i>controller modules</i> .
storage system	The hardware device running Data ONTAP that receives data from and sends data to native disk shelves, third-party storage, or both. Storage systems that run Data ONTAP are sometimes referred to as <i>filers</i> , <i>appliances</i> , <i>storage appliances</i> , <i>V-Series systems</i> , or <i>systems</i> .
third-party storage	The back-end storage arrays, such as IBM, Hitachi Data Systems, and HP, that provide storage for storage systems running Data ONTAP.

Keyboard and formatting conventions

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

Keyboard conventions

Convention	What it means
The NOW site	Refers to <i>the NetApp Support site at now.netapp.com/</i> .
<i>Enter, enter</i>	- Used to refer to the key that generates a carriage return; the key is named Return on some keyboards. - Used to mean pressing one or more keys on the keyboard and then pressing the Enter key, or clicking in a field in a graphical interface and then typing information into the field.
hyphen (-)	Used to separate individual keys. For example, Ctrl-D means holding down the Ctrl key while pressing the D key.
type	Used to mean pressing one or more keys on the keyboard.

Formatting conventions

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

Special messages

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

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

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

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by e-mail to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the name of your product and the applicable operating system. For example, *FAS6070—Data ONTAP 7.3*, or *Host Utilities—Solaris*, or *Operations Manager 3.8—Windows*.

SnapDrive overview

SnapDrive for Windows enables you to automate storage provisioning tasks and to manage data in Microsoft Windows environments. You can run SnapDrive on Windows hosts in either a physical or virtual environment.

Next topics

- [*What SnapDrive does*](#) on page 21
- [*What SnapDrive does not do*](#) on page 22
- [*Recommendations for using SnapDrive*](#) on page 22
- [*SnapDrive components*](#) on page 23
- [*SnapDrive licensing*](#) on page 24
- [*How LUNs work*](#) on page 24
- [*Disk allocation considerations*](#) on page 25
- [*How volume space is used*](#) on page 27
- [*Volume and storage system options set by SnapDrive*](#) on page 27
- [*What space reservation is*](#) on page 28
- [*Disk space usage with space reservation*](#) on page 29
- [*What fractional reserve is*](#) on page 29
- [*SnapDrive for Windows GUI icon descriptions*](#) on page 31

What SnapDrive does

SnapDrive software integrates with Windows Volume Manager so that storage systems can serve as virtual storage devices for application data in Windows Server 2003 and Windows Server 2008 environments.

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

SnapDrive provides the following additional features:

- It enables online storage configuration, LUN expansion, and streamlined management.
- It enables connection of up to 168 LUNs.
- It integrates Data ONTAP Snapshot technology, which creates point-in-time images of data stored on LUNs.
- It works in conjunction with SnapMirror software to facilitate disaster recovery from either asynchronously or synchronously mirrored destination volumes.
- It enables SnapVault updates of qtrees to a SnapVault destination.

- It enables management of SnapDrive on multiple hosts.
- It enables support on Microsoft cluster configurations.
- It enables iSCSI session management.

What SnapDrive does not do

Some functionality is currently not supported in SnapDrive for Windows.

- A LUN managed by SnapDrive cannot be configured as a “dynamic” disk (a storage device that is divided into volumes rather than partitions); it can serve only as a “basic” disk (a storage device for host-side application data).
- A LUN cannot be configured as an extended partition. SnapDrive supports only a single, primary partition on a LUN.
- LUNs created in System Manager MMC application, FilerView, or at the storage system command line cannot be managed unless certain steps are taken to prepare these disks for SnapDrive.
- SnapDrive supports LUNs on qtrees, but you cannot manage quotas from SnapDrive. LUNs can be created within a qtree and quota limits for that qtree are enforced; therefore, you cannot create a LUN or expand an existing LUN beyond the quota limit set for that qtree.
- SnapDrive supports the use of SnapMirror to replicate volumes but not individual qtrees.

Related tasks

[Managing LUNs not created in SnapDrive](#) on page 133

Recommendations for using SnapDrive

Follow these recommendations whenever you use SnapDrive for Windows.

- Use SnapDrive to create and manage all the LUNs on your storage system.
- Use the System Manager MMC application or FilerView to set up and configure your storage system and to provision volumes for use with SnapDrive.
- If you want to dedicate all free space on a volume to LUNs, *do* set the snap reserve setting on the storage system to 0 percent.
- Place all LUNs connected to the same host on a dedicated volume accessible by just that host.
- Unless you can be sure that name resolution publishes only the storage system interface you intend, configure each network interface by *IP address*, rather than by name.
- If you use Snapshot copies, you cannot use the entire space on a storage system volume to store your LUN.

The storage system volume hosting the LUN should be the size of all the LUNs on the volume, with enough additional space for the Snapshot copies of the volume. The additional space should be based on the change rate of the LUNs in the volume and the retention policy for the Snapshot copies.

- Do not create any LUNs in /vol/vol0. This is a storage system limitation.
This volume is used by Data ONTAP to administer the storage system and should not be used to contain any LUNs.

SnapDrive components

Several components are integrated into the SnapDrive for Windows software. This topic describes those components.

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

SnapDrive “snap-in”	This software module integrates with the Microsoft Management Console (MMC) 3.0 to provide a graphical interface for managing LUNs on the storage system. The module does the following: • Resides in the Windows Server 2003 or 2008 computer management storage tree • Provides a native MMC snap-in user interface for configuring and managing LUNs • Supports remote administration so that you can manage SnapDrive on multiple hosts • Provides SnapMirror integration • Provides AutoSupport integration, including event notification
SnapDrive command-line interface	The sdcli.exe utility enables you to manage LUNs from the command prompt of the Windows host. You can do the following tasks with the sdcli.exe utility: • Enter individual commands • Run management scripts
Underlying SnapDrive service	This software interacts with software on the storage system to facilitate LUN management for the following: • A host • Applications running on a host
Data ONTAP Volume Shadow Copy Service (VSS) Hardware Provider on Windows 2003 and 2008 hosts	The Data ONTAP VSS Hardware Provider is a module of the Microsoft VSS framework. The Data ONTAP Hardware Provider enables VSS Snapshot technology on storage systems when SnapDrive is installed on Windows 2003 and 2008 hosts.

Related concepts

[*SnapDrive command-line reference*](#) on page 205

[*Understanding the Volume Shadow Copy Service*](#) on page 159

SnapDrive licensing

Your SnapDrive license can reside either on the local host or on the storage systems that you are using SnapDrive to manage.

If you choose to install SnapDrive with licensing per storage system rather than with a host-side license, you can execute SnapDrive operations only on storage systems that have a SnapDrive or SnapManager license installed. Licensing SnapDrive on the storage system requires Data ONTAP 7.2.6 or later.

How LUNs work

The following section describes how LUNs work by interacting with Windows hosts and with storage systems.

Next topics

[*How the storage system interacts with the LUN*](#) on page 24

[*How Windows hosts interact with a LUN*](#) on page 24

[*LUN capabilities and limitations*](#) on page 25

[*Protocols for LUN access*](#) on page 25

[*How data is accessed from LUNs*](#) on page 25

How the storage system interacts with the LUN

To the storage system, a LUN is a logical representation of a physical unit of storage.

The storage system handles each LUN as a single storage object. The size of this LUN is slightly larger than the raw disk size reported to the Windows host. SnapDrive must be used to expand the disk because SnapDrive expands both the LUN and the Windows partition.

How Windows hosts interact with a LUN

You manage LUNs on the storage system just as you manage other Windows disks that store application data.

LUNs on the storage systems are automatically formatted by SnapDrive the same way that you format other Windows disks. Moreover, a Windows host interacts with all user data files on the LUN as if they were NTFS files distributed among the disks of a locally attached RAID array.

LUN capabilities and limitations

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

SnapDrive can also make a Snapshot copy of LUNs when they are used for data storage, and it can work with SnapMirror at the volume level and SnapVault at the qtree level for data protection.

Protocols for LUN access

You can access the SnapDrive-created LUNs using either FC or iSCSI protocol, or both.

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

How data is accessed from LUNs

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

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

Disk allocation considerations

Resources you should consider when you plan disk allocation on the storage system include RAID groups, hot spare disks, and aggregates.

Next topics

[RAID group configuration](#) on page 25

[Hot spare disks](#) on page 26

[How many hot spares you should have](#) on page 26

[How aggregates work](#) on page 26

RAID group configuration

Plan RAID groups carefully to ensure the best performance and availability of data on your storage system.

You can assign more than one RAID group to a single storage system aggregate; in fact, you should do so if the aggregate contains more than 14 disks. This ensures data integrity and availability if multiple disks fail simultaneously within the same aggregate.

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

Hot spare disks

A hot spare disk should always be available on your storage system in the event that an active disk fails.

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

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

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

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

Note: To receive proactive alerts about the status of disks in your storage system, enable the Data ONTAP AutoSupport feature.

How many hot spares you should have

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

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

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

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

How aggregates work

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

Each aggregate has its own RAID configuration, plex structure, and set of assigned disks or array LUNs.

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

Related information

[*TR 3437: Storage Best Practices and Resiliency Guide*](#)

How volume space is used

SnapDrive uses space on a storage system volume for LUNs and their data, and also for the data that changes between Snapshot copies, the LUN's active file system, and for metadata.

Volume size rules

Storage system volumes that will hold LUNs must be large enough to hold all the LUNs in the volume, as well any Snapshot copies if Snapshot copies are created.

The following factors govern the appropriate minimum size for a volume that holds a LUN:

- If the LUNs are space reserved, then the volume must be more than twice the combined size of all the LUNs on the volume if a Snapshot copy of the volume is created. This enables the volume to hold the LUNs in a fractional reservation area.

No matter how much the contents of the LUNs change between Snapshot copies, the entire contents of the disks are written to the volume.

- The volume must also provide enough additional space to hold the number of Snapshot copies you intend to keep online.

The amount of space consumed by a Snapshot copy depends on the amount of data that changes after the Snapshot copy is taken. The maximum number of Snapshot copies is 255 per storage system volume.

Volume and storage system options set by SnapDrive

SnapDrive for Windows automatically checks and resets some storage system and volume options.

Key points when SnapDrive checks and resets options:

- When you start SnapDrive
- When you create a LUN
- When you connect a LUN to a host

The following table shows the defaults that are reset and when those resets take place; you should *not* change these values.

Option type	Option	SnapDrive setting	When
LUN	LUN reserved	LUN reservation set to Enabled	• Disk creation
Volume	nosnapdir	Off	• Disk creation • Disk connection

Option type	Option	SnapDrive setting	When
Volume	Snapshot copy schedule	Off	• Disk creation • Disk connection
Volume	create_ucose convert_ucose Note: These volume options are no longer used, but they are set to maintain backwards compatibility with older versions of SnapDrive.	On	• Disk creation • Disk connection

What space reservation is

When space reservation is enabled for one or more LUNs, Data ONTAP reserves enough space in the volume (traditional or FlexVol) so that writes to those LUNs do not fail because of a lack of disk space.

Note: LUNs in this context refer to the LUNs that Data ONTAP serves to clients, not to the array LUNs used for storage on a storage array.

For example, if you create a 100-GB space reserved LUN in a 500-GB volume, that 100 GB of space is immediately allocated, leaving 400 GB remaining in the volume. In contrast, if space reservation is disabled on the LUN, all 500 GB in the volume remain available until writes are made to the LUN.

Space reservation is an attribute of the LUN; it is persistent across storage system reboots, takeovers, and givebacks. Space reservation is enabled for new LUNs by default, but you can create a LUN with space reservations disabled or enabled. After you create the LUN, you can change the space reservation attribute by using the `lun set reservation` command.

When a volume contains one or more LUNs with space reservation enabled, operations that require free space, such as the creation of Snapshot copies, are prevented from using the reserved space. If these operations do not have sufficient unreserved free space, they fail. However, writes to the LUNs with space reservation enabled will continue to succeed.

Disk space usage with space reservation

When space reservation is enabled, the amount of space available on a volume containing LUNs determines whether Snapshot copy creation can take place.

When you first create a LUN with space reservation enabled, it is granted a space reservation equal to its size. This reserved space is subtracted from the total available disk space on the storage system volume on which the LUN resides.

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

By monitoring the remaining available space in the storage system volume, the available space in the volume determines whether Snapshot copy creation is allowed. When the amount of available space on the storage system volume falls to below the threshold you set to prevent overwriting space reserved LUNs, Snapshot creation is blocked.

What fractional reserve is

Fractional reserve is a volume option that enables you to determine how much space Data ONTAP reserves for Snapshot copy overwrites for LUNs, as well as for space-reserved files when all other space in the volume is used.

The fractional reserve setting defaults to 100%, but you can use the `vol options` command to set fractional reserve to any percentage from zero to 100.

It is best to use the autodelete function, but there may occasionally be circumstances under which fractional reserve can be used, including:

- When Snapshot copies cannot be deleted
- When preserving existing Snapshot copies is more important than creating new ones

Fractional reserve can be used on the following types of volumes:

- Traditional volumes
- FlexVol volumes with a space guarantee of `volume` or
- FlexVol volumes with a space guarantee of `none`. You can only set fractional reserve for a volume with a space guarantee of `none` with Data ONTAP version 7.3.3 and later and version 8.0.1 and later.

Note: If the `guarantee` option for a FlexVol volume is set to `none` or `volume`, then fractional reserve for that volume can be set to the desired value. For the vast majority of configurations, you should set fractional reserve to zero when the `guarantee` option is set to `none` because it greatly simplifies space management. If the `guarantee` option for a FlexVol volume is set to `file`, then fractional reserve for that volume is set to 100 percent and is not adjustable.

If fractional reserve is set to 100%, when you create space-reserved LUNs, you can be sure that writes to those LUNs will always succeed without deleting Snapshot copies, even if all of the space-reserved LUNs are completely overwritten.

Setting fractional reserve to less than 100 percent causes the space reservation held for all space-reserved LUNs in that volume to be reduced to that percentage. Writes to the space-reserved LUNs in that volume are no longer unequivocally guaranteed, which is why you should use `snap autodelete` or `vol autogrow` for these volumes.

Fractional reserve is generally used for volumes that hold LUNs with a small percentage of data overwrite.

Note: If you are using fractional reserve in environments in which write errors due to lack of available space are unexpected, you must monitor your free space and take corrective action to avoid write errors. Data ONTAP provides tools for monitoring available space in your volumes.

Note: Reducing the space reserved for overwrites (by using fractional reserve) does not affect the size of the space-reserved LUN. You can write data to the entire size of the LUN. The space reserved for overwrites is used only when the original data is overwritten.

Example

If you create a 500-GB space-reserved LUN, then Data ONTAP ensures that 500 GB of free space always remains available for that LUN to handle writes to the LUN.

If you then set fractional reserve to 50 for the LUN's containing volume, then Data ONTAP reserves 250 GB, or half of the space it was previously reserving for overwrites with fractional reserve set to 100. If more than half of the LUN is overwritten, then subsequent writes to the LUN could fail due to insufficient free space in the volume.

Note: When more than one LUN in the same volume has space reservations enabled, and fractional reserve for that volume is set to less than 100 percent, Data ONTAP does not limit any space-reserved LUN to its percentage of the reserved space. In other words, if you have two 100-GB LUNs in the same volume with fractional reserve set to 30, one of the LUNs could use up the entire 60 GB of reserved space for that volume.

See the *Technical Report* on thin provisioning for detailed information on using fractional reserve .

Related information

Technical Report: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment - <http://media.netapp.com/documents/tr3483.pdf>

SnapDrive for Windows GUI icon descriptions

The SnapDrive for Windows graphical user interface (GUI) uses icons to represent objects that are available in SnapDrive, the state of those objects, and actions you can perform from MMC.

Icon	Description
	LUN
	Create disk
	Connect disk
	Manage igroups
	Disk properties
	Snapshot copy
	Consistent Snapshot copy
	Inconsistent Snapshot copy
	Create Snapshot copy
	Resize disk

Icon	Description
	Delete disk
	Disconnect disk
	Force disconnect disk
	Change drive letter and path
	Update SnapMirror
	Add/remove initiator
	Start Space Reclaimer
	Stop Space Reclaimer
	LUN refresh
	Snapshot copy refresh
	Restore disk
	Rename Snapshot copy

Icon	Description
	Delete Snapshot copy
	SnapVault update
	Host connected
	Host not connected
	Add SnapDrive server
	iSCSI management
	Disconnect iSCSI target
	Disconnect iSCSI session
	Establish iSCSI session
	iSCSI sessions
	Transport protocol
	Cluster shared disk

Icon	Description
	Cluster shared SnapMirror disk
	Dedicated SnapMirror disk
	SAN boot LUN

Features added in SnapDrive 6.3 for Windows

SnapDrive 6.3 for Windows introduces support for virtual machine disks (VMDK) in an NFS or VMFS datastore, support for space reclamation when using VMDK with NFS, and support for DataFabric Manager caching with RBAC.

Related concepts

[*Support for VMDKs in NFS and VMFS datastores*](#) on page 37

[*Support for space reclamation in VMDK files in NFS datastores*](#) on page 38

Related references

[*The dfm_config rbaccache command*](#) on page 238

Features supported

SnapDrive for Windows supports a variety of protocols and applications, and it offer a number of features to enable LUN provision and Snapshot copy management in virtual and non-virtual Windows environments.

Next topics

- [*Support for VMDKs in NFS and VMFS datastores*](#) on page 37
- [*SnapDrive VMDK support limitations*](#) on page 38
- [*Support for space reclamation in VMDK files in NFS datastores*](#) on page 38
- [*SnapDrive support in Windows Server 2008 Server Core*](#) on page 39
- [*Support for dynamically adding and removing pass-through disks on Hyper-V virtual machines*](#) on page 40
- [*Support for restoring data at the file level*](#) on page 41
- [*Support for storage system access control*](#) on page 42
- [*Support for ESX iSCSI initiators with SnapDrive for Windows*](#) on page 43
- [*SnapDrive changes with MMC 3.0*](#) on page 44
- [*MultiStore support*](#) on page 45
- [*HTTP and HTTPS transport protocol support*](#) on page 45
- [*IPv6 support*](#) on page 47
- [*SnapVault support*](#) on page 47
- [*VMware support*](#) on page 47
- [*GPT partition support*](#) on page 50
- [*LUN boot disk \(SAN booting\) support*](#) on page 50
- [*Cluster support*](#) on page 50

Support for VMDKs in NFS and VMFS datastores

You can use SnapDrive for Windows with SnapManager for Virtual Infrastructure when you want to perform Snapshot copy operations in VMDKs on NFS and VMFS datastores.

The following conditions must exist before you can use SnapDrive with VMDKs in an NFS or VMFS datastore:

- SnapManager for Virtual Infrastructure is installed and the appropriate IP address and port number is configured in SnapDrive for Windows.
SnapDrive provides a configuration panel in the installation Wizard.
- Data ONTAP 7.3.4 or later is installed on your storage system for SnapDrive to use the space reclamation feature in VMDK files.
- SnapManager for Virtual Infrastructure server is installed in the same location as vCenter.

- The SnapManager for Virtual Infrastructure server is available and reachable from the virtual machine on which SnapDrive is installed.
- The storage system IP address is configured in the SnapManager for Virtual Infrastructure server to enable identification of VMDKs created across NFS and VMFS datastores.

For more information about configuring SnapManager for Virtual Infrastructure, see the *SnapManager for Virtual Infrastructure Installation and Administration Guide*.

SnapDrive VMDK support limitations

SnapDrive has some limitations of which you should be aware before using SnapDrive to perform Snapshot copy operations on VMDKs.

The following VMDK limitations exist:

- VMDKs must not be created on SnapManager for Virtual Infrastructure mounted datastores.
- Snapshot copy operations cannot be performed on VMDKs when VMware snapshots exist on a virtual machine.

If you try to create Snapshot copy using SnapDrive when a VMware snapshot exists, SnapDrive will give you an error indicating that backup creation has failed, and Snapshot copy mount and restore operations cannot occur.

Support for space reclamation in VMDK files in NFS datastores

You can use the Space Reclaimer feature to reclaim space left by recently freed blocks in VMDK files located in NFS datastores when you use SnapDrive for Windows with SnapManager for Virtual Infrastructure in an ESX environment.

You can run Space Reclaimer on VMDK files using SnapDrive MMC and sdcli.exe.

SnapDrive provides support for VMDK file space reclamation in NFS datastores in the following cases:

- VMDK files with simple extent type FLAT is supported.
Space reclamation is not supported on sparse extents and VMFS datastores.
- SnapManager for Virtual Infrastructure must be present to discover VMDK files.
If SnapManager for Virtual Infrastructure is not available, SnapDrive is unable to discover VMDKs and, therefore, cannot reclaim space on VMDK files.
- SnapDrive is configured with either ESX server or vCenter credentials.
- Data ONTAP 7.3.4 or later is installed on your storage system.

SnapDrive support in Windows Server 2008 Server Core

Windows Server 2008 Server Core, including Windows Hypervisor (Hyper-V), is supported by SnapDrive for Windows, and it enables remote LUN management using SnapDrive `sdcli.exe` and MMC from a standard Windows server.

A Windows Server 2008 Server Core installation provides a scaled-back environment for running specific server roles. The minimum environment reduces maintenance and management requirements, and also reduces the attack surface for the server roles. There is no GUI, which allows the server to run faster; however, you can create virtual machines (VMs) on the Server Core, and Windows Server can be installed in those VMs.

After you install SnapDrive on the Server Core system, you can manage SnapDrive remotely from a non-server core SnapDrive system by using the Add SnapDrive Server option in the SnapDrive MMC. You can then perform all SnapDrive management tasks using either SDCLI or MMC.

You can determine whether Hyper-V VMs have a virtual hard disk configured on a Data ONTAP LUN by using the `sdcli disk list` command. The command output indicates whether or not a Hyper-V VM is present on a LUN.

Next topics

[Server Core limitations](#) on page 39

[Requirements for managing SnapDrive on Windows Server Core systems](#) on page 40

Related tasks

[Creating a highly available Hyper-V virtual machine using SnapDrive](#) on page 118

[Preparing to install SnapDrive on Windows Server 2008 Server Core](#) on page 76

[Installing SnapDrive on Windows Server 2008 Server Core](#) on page 79

Related references

[SnapDrive command line installation switches](#) on page 178

Server Core limitations

Windows Server 2008 Server Core has some limitations you should keep in mind when using SnapDrive in a Server Core environment.

- There is no Windows shell in the operating system and there is limited GUI functionality.
- Windows Server 2008 Server Core does not support .NET; however, the .NET framework is supported on Windows Server 2008 R2 Server Core systems.
- SnapDrive is supported only on X64 Server Core.
SnapDrive is not supported on X86 Server Core.
- Microsoft supports Hyper-V only on X64-based systems; therefore, SnapDrive will support only X64 installations for Hyper-V support.

- To comply with Microsoft best practices, SnapDrive will support only one Hyper-V virtual machine per LUN in a failover cluster.

Requirements for managing SnapDrive on Windows Server Core systems

You must verify the requirements for remotely managing SnapDrive on a Windows Server Core system.

The following conditions must exist in order to manage SnapDrive remotely on a Windows Core Server system.

- The remote Windows system and the Server Core system must both have the same CPU type. For instance, they must both use an IA64 CPU or they must both use an x64 CPU.
- The remote Windows system and the Server Core system must be in the same domain.

Support for dynamically adding and removing pass-through disks on Hyper-V virtual machines

SnapDrive supports the feature introduced in Windows Server 2008 R2 that enables you to add or remove a pass-through disk on a Hyper-V virtual machine without shutting down that virtual machine. This is sometimes called the hot add and remove feature.

A *pass-through* disk is a disk that is physically connected to a Hyper-V parent host and is assigned to a Hyper-V virtual machine as a SCSI hard disk for use by that virtual machine.

The following configuration requirements must be met to use this feature:

- You must be using Windows Server 2008 R2.
- .NET 3.5 SP1 or higher must be installed on the Hyper-V parent hosts.
- A version of SnapDrive that supports the dynamically adding and removing pass-through disks must be installed on all Hyper-V parent hosts and on all targeted Hyper-V virtual machines.
- Data ONTAP 7.3.1 or later must be installed on the storage system.
- If iSCSI is used for the pass-through disk, the iSCSI groups must already be configured and the iSCSI session between the storage system and the Hyper-V parent host must already exist.
- The SCSI controller must be added to target virtual machines in advance.
Adding a SCSI controller requires virtual machine downtime.
- The Hyper-V parent host and the virtual machine must have TCP/IP network communication to all parent hosts and vice versa.
- A virtual machine must not have MPIO enabled.

Note: If you uninstall SnapDrive for Windows, all SnapDrive registry key entries are removed from your Windows host. If you reinstall SnapDrive, you must reconfigure pass-through disks.

Related references

The disk create command on page 221

The disk connect command on page 222

Hyper-V pass-through disk support limitations

SnapDrive supports Hyper-V pass-through disks; however, there are some limitations related to this feature.

- SnapDrive does not support direct attached storage to a Hyper-V parent host. Only Data ONTAP iSCSI and FC LUNs are supported.
- SnapDrive does not support LUNs already mapped to a Hyper-V parent host. A pass-through disk must be freshly provisioned from a storage system to be added dynamically.
- Windows 2008 R2 does not support pass-through disks using IDE. Windows 2008 R2 supports only SCSI disks.
- Microsoft cluster shared volume (CSV) disks are not supported.
- Hyper-V does not support the SnapDrive space reclaimer feature.
- Pass-through LUN creation fails when Data ONTAP DSM is installed on Hyper-V virtual machines.

Note: Removing MPIO will not remove MPIO iSCSI sessions that SnapDrive might have been using. After removing MPIO, you must remove existing iSCSI sessions and, if needed, create new iSCSI sessions.

- Due to a Microsoft limitation, if a pass-through disk is down, the virtual machine to which the disk is assigned cannot be rebooted. To reboot the virtual machine, you must bring the pass-through disk back up, or remove it from the virtual machine using Microsoft Hyper-V Manager or another Microsoft remote server management tool.
- If DataFabric Manager role-based access control is enabled on a SnapDrive for Windows Hyper-V parent host, you cannot dynamically add or remove pass-through disks with SnapDrive in a Hyper-V virtual machine.
- Windows Server 2008 Server Core does not support the ability to dynamically add and remove Hyper-V pass-through disks because Server Core does not support Windows Communication Foundation (WCF) Web services that are required to dynamically add and remove pass-through disks.

Support for restoring data at the file level

You can use SnapDrive command-line interface to restore one or more files from a Snapshot copy.

You can use the file-level restore feature in the following cases:

- To restore generic files on a LUN from its corresponding Snapshot copy

A file being restored on a LUN can be a virtual hard disk, a database file, or any large, generic file, provided that no applications or systems are affected by the restoration of those files

- To restore a individual database files provided that the administrator ensures that the files being restored do not cause the database to become inconsistent

Attention: SnapDrive guarantees data consistency of files restored from a consistent Snapshot copy; however, application consistency is outside the function of SnapDrive for Windows. Files restored using file-level restore operation might result in application inconsistency. Use file-level restoration with caution, following the recommended practices for the operating system or applications using the files. The file-level restore operation must be used by experienced administrators with full knowledge of the operating system and applications using the files.

Related references

[The *snap restore command*](#) on page 231

Support for storage system access control

SnapDrive provides support for storage system access control to separate server administrator and storage administrator functions, and to limit SnapDrive actions and operations that depend on the user.

SnapDrive enables you to control storage system access by reading a file called AccessControl.xml created by the storage system administrator. The file is created in the /etc directory of the storage system root volume and lists the operations and storage resources that are allowed access by users who are assigned specific roles. The access control file associates access rights with specific storage resources. A tool called storacl.exe is used to edit the access control file.

Related references

[Storage system access control operations list](#) on page 195

[Storage system access control roles](#) on page 196

[Storage system access control commands](#) on page 198

[Storage system access control command examples](#) on page 198

Using storage system access control

SnapDrive uses the AccessControl.xml file on the storage system to determine what roles are assigned to a user and what operations are allowed for specific roles.

Before you begin

- Install the storage access control (storacl.exe) tool on any Windows host to create and manage the AccessControl.xml file on your storage system in the /etc directory of the root volume. The executable is part of your SnapDrive installation and is located in the SnapDrive directory on your host.

- HTTPS must be enabled using the options `ssl.enable` command and `secureadmin setup ssl` command on the storage system.
HTTP is also supported for use with vFiler units when using the MultiStore feature of Data ONTAP software.
- You must be logged in as root on the storage system.

About this task

Attention: Always use `storacl.exe` to modify the `AccessControl.xml` file. Using a standard XML editor might corrupt the file and cause SnapDrive operations to fail.

Steps

1. Run `storacl.exe` from your Windows host to create a default `AccessControl.xml` file on the specified storage system.

An `AccessControl.xml` file is created containing a default set of roles and operations with no resources or access rights.

2. Using `storacl.exe`, edit the `AccessControl.xml` file to add or change users and to grant or deny access rights to the storage system resources. You can also use the default entries.

SnapDrive opens and reads the `AccessControl.xml` file and caches the information on the Windows host. SnapDrive uses this information to check resource access for all SnapDrive operations, and grants or denies access depending on the role assigned to the user.

SnapDrive performs an `rbac-access-check` operation to compare the file timestamp on the cached `AccessControl.xml` file with the timestamp on the `AccessControl.xml` file on the storage system. If a change exists on the storage system version of the `AccessControl.xml` file, SnapDrive refreshes the cached version.

Support for ESX iSCSI initiators with SnapDrive for Windows

SnapDrive for Windows enables the use of ESX iSCSI initiators to provide LUN provisioning and Snapshot copy management operations in a guest OS.

Note: The iSCSI initiators must be configured on the ESX server before you can use them with SnapDrive. See your VMware documentation for more information on configuring ESX iSCSI initiators on the ESX server.

SnapDrive provides support for ESX iSCSI initiators for the following:

- LUN enumeration using either the SnapDrive MMC or `sdcli.exe`.
- LUN migration with VMotion for LUNs connected with ESX iSCSI initiators
- Creation of initiator groups using ESX iSCSI initiators

- Physical mode RDMs using iSCSI initiators
A maximum of 56 LUNs are supported in the guest OS.

ESX iSCSI initiator limitations

SnapDrive supports the use of ESX iSCSI initiators, but there are some limitations you must keep in mind.

- SnapDrive does not support iSCSI session management using ESX iSCSI initiators.
You can add targets from the initiator list during LUN creation and connection.
- Multipathing using both FC HBA and ESX iSCSI initiators is not supported.
- Multipathing using both Microsoft iSCSI Software initiators and ESX iSCSI initiators is not supported.
ESX iSCSI initiators require RDM files to provision a LUN, but Microsoft iSCSI Software initiators do not have this requirement.

VMware limitations

- RDMs are not supported on an NFS datastore; however, you can store RDMs in any connected VMFS datastore if the virtual machine is stored on NFS.
- MPIO is not supported in a guest OS.
- Windows Server 2008 failover clustering is not supported using ESX iSCSI RDM LUNs.
- RDM LUNs larger than 2 TB are not supported.
- IA64-bit operating system is not supported as a guest OS.

SnapDrive changes with MMC 3.0

SnapDrive's implementation of MMC 3.0 introduces some changes from previous versions of SnapDrive, including the introduction of a new Action pane and improved error messages.

Next topics

[Using MMC 3.0 Action pane](#) on page 44

[Error messages in MMC 3.0](#) on page 45

Using MMC 3.0 Action pane

You can use the new MMC 3.0 Action pane in SnapDrive to perform all the available operations for a specific node or disk; however, the Action pane is not displayed by default on Windows Server 2003 hosts, so you must enable it manually.

Steps

1. If the Action pane is not displayed (to the right of the main MMC Details pane), click the Show/Hide Action Pane icon at the top of MMC.

The Action pane is displayed.

2. In the left MMC pane, click the instance of SnapDrive or a LUN for which you want to perform an operation.

The available operations are displayed in the Action pane.

Error messages in MMC 3.0

SnapDrive uses new functionality in MMC 3.0 that enables SnapDrive to notify you when you type incorrect information in a text box or field.

Rather than displaying an error message in a pop-up window, an error message icon is displayed next to the field, along with an error description. Additional error details are viewed by using the mouse to hover over the error icon.

MultiStore support

SnapDrive is supported on vFiler units when using the iSCSI protocol.

If a storage system uses the optional MultiStore feature of Data ONTAP software to create virtual storage systems (vFiler units), SnapDrive can create, connect to, and manage LUNs on the vFiler units in the same way it does on the physical storage system. You accomplish this by providing the name for the vFiler unit rather than the name of the physical storage system to create a connection. It is transparent to the host whether the attached storage system is a physical storage system or a virtual vFiler unit.

If a LUN is in a vFiler unit on storage system with a FlexClone license, SnapDrive attempts to connect to a Snapshot copy using a flexible clone. With Data ONTAP 7.2.2 and later, you have to set the value of the Data ONTAP configuration option `vfiler.vol_clone_zapi_allow` to On in order to connect to a Snapshot copy of a volume or LUN in a vFiler unit.

Note: SnapDrive is supported on vFiler units only when using the iSCSI protocol.

Note: The HTTPS protocol is not supported with MultiStore.

HTTP and HTTPS transport protocol support

SnapDrive for Windows allows you to use HTTP or HTTPS in addition to the default RPC protocol for storage system communication. This feature, along with CIFS share dependency removal, means you are no longer required to have root access on the storage system for SnapDrive-related operations.

SnapDrive enables configuration of HTTP or HTTPS for individual storage systems. It also allows you to set a default transport protocol in case one has not been specified for individual storage systems.

Transport protocols can be configured either during SnapDrive installation or after SnapDrive has been installed.

The `httpd.admin.enable` option must be set on the storage system in order for SnapDrive to use the HTTP or HTTPS protocol.

Note: Using the domain Administrator account for authentication results in significantly reduced performance. To avoid this issue, use a storage system account for authentication instead of the domain account.

Note: HTTPS is not supported with MultiStore.

Adding storage system capabilities for HTTP users

You can enable HTTP capabilities for users who want to communicate with a storage system and SnapDrive using the HTTP transport protocol.

About this task

A storage system administrator must assign the appropriate capabilities to users who do not have administrator access on the storage system.

Steps

1. Create a local group on the storage system to which you want to enable HTTP communication with SnapDrive.
2. Associate the new group to a role with the following capabilities:
 - `api`
 - `login`
3. Add the SnapDrive user to the new storage system group.

Example of how to add storage system capabilities

This examples creates a role on Storage1 called `snaphttp2` with `api` and `login` capabilities, creates a group called `snapadmins` with the `snaphttp2` role capabilities, and adds the user `snapadmin1` to the `snapadmins` group.

```
Storage1> useradmin role add snaphttp2 -a api-*,login-http-admin
The role 'snaphttp2' has been added.
Role <snaphttp2> added.
```

```
Storage1> useradmin group add snapadmins -r snaphttp2
The group 'snapadmins' has been added.
Group <snapadmins> added.
```

```
Storage1> useradmin user add snapadmin1 -g snapadmins
```

```
The user 'snapadmin1' has been added.  
User <snapadmin1> added.
```

IPv6 support

SnapDrive supports IPv6 in a Windows Server 2008 environment when you are using Data ONTAP 7.3.1 or later on your storage system.

When SnapDrive asks you to provide a host name or IP address, it can look up the name or accept an IP in either IPv4 or IPv6 format. Addresses in IPv6 format are accepted in both expanded and compressed forms.

Note: A link-local IPv6 address can be used for iSCSI session management and for communication between a host and a target only when both are in the same subnet.

SnapVault support

SnapDrive provides SnapVault backup support of existing SnapVault configurations when your storage system is running Data ONTAP 7.2.6 or later. If you are using SnapVault with MultiStore, Data ONTAP 7.3 or later is required.

SnapDrive uses the SnapVault feature of Data ONTAP to back up Snapshot copies to a secondary storage system.

Related concepts

[Using SnapVault with SnapDrive](#) on page 155

VMware support

SnapDrive for Windows provides LUN provisioning and Snapshot copy management support with VMware ESX 3.0.2 or later guest OS on x86, and x64 platforms when using either the Microsoft iSCSI Software Initiator 2.04 or later, FC HBAs, or ESX iSCSI software initiators or iSCSI HBAs.

SnapDrive provides support in the VMware guest OS for the following configurations:

- Windows Server 2003 SP2 for x86 and x64 platforms, and Windows Server 2008 for x86, and x64 platforms.
- Microsoft cluster configurations up to a maximum of 8 nodes supported on VMware when using the Microsoft iSCSI Software Initiator, or up to 2 nodes using FC.
- A maximum of 56 RDM LUNs with four LSI Logic SCSI controllers.

Next topics

[VMware-related limitations](#) on page 48

[Enabling and disabling vCenter or ESX logon from SnapDrive MMC](#) on page 48

[Minimum vCenter permissions required for SnapDrive operations](#) on page 49

[VMware VMotion support](#) on page 49

Related tasks

[Creating an RDM LUN on a guest OS](#) on page 114

[Connecting to an RDM LUN on a guest OS](#) on page 124

Related references

[Minimum SnapDrive requirements for VMware ESX Guest OS](#) on page 62

[Virtual server commands](#) on page 240

VMware-related limitations

SnapDrive is supported on VMware ESX server; however, there are some limitations you must keep in mind.

- Installing SnapDrive on a Microsoft cluster on virtual machines using ESX credentials is not supported.
Use the vCenter credentials when installing SnapDrive on clustered virtual machines.
- RDM LUNs greater than 2 TB are not supported.
- MPIO is present on the ESX and is not required on the VMware guest OS.
- iSCSI and FC initiators are not supported together on a VMware guest OS.

Enabling and disabling vCenter or ESX logon from SnapDrive MMC

You can use SnapDrive MMC to enable and disable VMware vCenter or ESX logon settings after SnapDrive is installed on your Windows host.

About this task

Keep the following information in mind when setting vCenter or ESX logon from SnapDrive MMC:

- You cannot disable vCenter or ESX logon from SnapDrive MMC when RDM LUNs are present. You must disconnect or delete RDM LUNs before you can disable ESX logon.
- If you migrate a virtual machine from one ESX server to another, you must configure SnapDrive with vCenter account information.

Steps

1. In the left MMC pane, select the instance of SnapDrive for which you want to enable or disable vCenter or ESX logon.
2. From the menu choices at the top of MMC, navigate to **Action > VirtualCenter or ESX Server Login Settings**.

The **VirtualCenter or ESX Server Log On** window is displayed.

3. To enable vCenter or ESX logon, in the **VirtualCenter or ESX Server Log On** window, select the "Enable VirtualCenter or ESX server settings" checkbox.
4. Type the IP address or hostname, user name, and password for the vCenter or ESX to which you want to log in.
5. Click **OK**.
6. To disable vCenter or ESX logon, complete Steps 1 and 2 and then clear the "Enable VirtualCenter or ESX server settings" checkbox.

The vCenter or ESX settings are unavailable (grayed out).

Note: When you disable vCenter or ESX settings, SnapDrive cannot display WWPNs for FC HBAs on the ESX server.

Minimum vCenter permissions required for SnapDrive operations

The vCenter credentials used by SnapDrive must have minimum permissions set on the host and on the virtual machine to enable SnapDrive operations to succeed.

The following minimum credentials must be set on the host:

- **Configuration > Storage Partition Configuration**

The following minimum credentials must be set on the virtual machine:

- **Configuration > Raw Device**
- **Configuration > Change Resource**

If SnapDrive is installed with vCenter credentials, you must ensure the following requirements:

- The user must be a vCenter user.
- The roles with required minimum privileges must be assigned to the user at the vCenter level.

If SnapDrive is installed with ESX credentials, you must ensure the following:

- The user must be an ESX server user.
- The roles with required minimum privileges must be assigned to the user at the ESX server level.

VMware VMotion support

SnapDrive supports VMware VMotion, which enables the live migration of running virtual machines from one physical machine to another without interrupting service to those machines.

The following VMotion requirements must be met to use VMotion with SnapDrive:

- Use VMware vCenter instead of the ESX during SnapDrive installation.
- If SnapDrive was installed to communicate directly with the ESX, modify settings using **VirtualCenter or ESX Server login Settings** in the SnapDrive MMC.

- Manually create an igroup that has all WWPNs from the source and the destination ESX. Use the same igroup for all RDM LUN create and connect operations.

Note: When you perform a VMotion operation, the RDM LUN validation might fail. Perform an HBA rescan from the virtual infrastructure client and retry the operation.

GPT partition support

SnapDrive supports the GUID partition table (GPT) partitioning style on new LUNs created by SnapDrive when you have Data ONTAP 7.2.6 or later installed on your storage system.

GPT shared LUNs are supported with Windows Server 2008 and with Windows Server 2003 when Microsoft hotfix 919117 is installed.

Neither SnapDrive nor Data ONTAP support MBR LUNs that are converted to GPT-style LUNs. If you have an existing MBR-style LUN, rather than converting, you must create a new GPT LUN using SnapDrive, then copy all the data from the MBR LUN to the GPT LUN.

Note: GPT LUNS have a Microsoft reserved partition (MSR), which is invisible to applications like Disk Management and the Windows Explorer. When you create a LUN that has the GPT partition style, the LUN size appears smaller than the size you specified when you created it. This is due to the space used by the MSR. To create a GPT LUN that is less than 16 GB, you must have at least 32 MB of space available for the MSR. For GPT LUNs greater than or equal to 16 GB, you must have at least 128 MBs for MSR space.

Related information

[The Microsoft support page - support.microsoft.com/kb/919117](http://support.microsoft.com/kb/919117)

LUN boot disk (SAN booting) support

SnapDrive supports both bootable LUNs (SAN booting) and nonbootable LUNs.

SnapDrive differentiates between bootable and nonbootable LUNs and prevents you from performing some of the operations you would normally perform on a nonbootable LUN.

Cluster support

SnapDrive for Windows can be deployed in a variety of cluster configurations.

SnapDrive is supported with the following cluster technologies:

- Windows clusters

To protect against node failure, Windows clustering fails over applications from the host node to the surviving node. In Windows 2003, this is called Microsoft Cluster Server (MSCS). In Windows 2008, this is Windows failover clustering.

- Active/active storage system configurations

If a storage system fails, the partner storage system takes over the functions of the failed storage system, thus protecting data and ensuring continued storage availability.

Note: SnapDrive LUNs are supported in an active/active storage system configuration; however, during cluster takeover and giveback, SnapDrive operations will fail for LUNs located on the active/active storage systems until the takeover and giveback process is completed.

Next topics

[Microsoft clusters on ESX reference](#) on page 51

[Support for Microsoft cluster shared volumes](#) on page 51

[Support for Microsoft clusters using FC RDM LUNs](#) on page 52

Microsoft clusters on ESX reference

There are many documents and knowledge base articles that discuss the use of Microsoft clusters on ESX. You can find additional information about configuring your Microsoft cluster on an ESX server by reading these documents.

The following documentation is located on the VMware Web site:

- KB article 1009287, *ESX machines hosting passive MSCS nodes report reservation conflicts during storage operations*
- Knowledge base article 1011796, *VMware ESX 3.5, Patch ESX-350-200906401-BG*
- Knowledge base article 1004617, *Microsoft Cluster Service (MSCS) Support on ESX*
- *Setup for Microsoft Cluster Service*
- *Setup for Failover Clustering and Microsoft Cluster Service*
- *VMware ESX Server 3i version 3.5 Update 4 Installable Release Notes*

Support for Microsoft cluster shared volumes

SnapDrive for Windows supports LUN provisioning and Snapshot copy management on Microsoft cluster shared volumes (CSVs) using Hyper-V with Windows Server 2008 R2.

Cluster shared volume is a new feature in Windows Server 2008 R2 that enables all nodes in the same Microsoft cluster concurrent access to files on each CSV-enabled shared LUN. CSV allows multiple virtual hard disks from different virtual machines to be stored on a single LUN.

Note: If you enable CSV after installing SnapDrive for Windows, you must restart the SnapDrive service and close and reopen SnapDrive MMC.

Related references

[*LUN commands*](#) on page 220

Support for Microsoft clusters using FC RDM LUNs

SnapDrive provides support for Microsoft clusters using FC RDM LUNs on two different virtual machines that belong to two different ESX servers. This is also known as across-the-box clusters.

The following configuration requirements must be met in order to use FC RDM LUNs on virtual machines in a Microsoft cluster:

- The virtual machines must be running the same Windows server version.
Virtual machines must both be running either Windows server 2003 or Windows server 2008.
- ESX server versions must be the same for each VMware parent host.
- Each parent host must have at least two network adapters.
- VMware recommends that the shared datastore should be created on an FC SAN; however, the shared datastore can also be created over iSCSI.
- The shared RDM LUN must be in physical compatibility mode.
- A SCSI controller must be configured on each virtual machine in the cluster in physical compatibility mode.

Windows Server 2003 requires you to configure the LSI Logic SCSI parallel controller on each virtual machine, and Windows Server 2008 requires you to configure the LSI Logic SAS SCSI controller on each virtual machine.

SCSI controllers of type paravirtual are not supported on VMware Microsoft clusters.

Note: When you add a SCSI controller to a shared LUN on a virtual machine in physical compatibility mode, you must select the **Raw Device Mappings** option and not the **Create a new disk** option in the VMware Infrastructure Client.

- Microsoft virtual machine clusters cannot be part of a VMware cluster.
- You must use VCenter credentials and not ESX credentials when you install SnapDrive for Windows on virtual machines that will belong to a Microsoft cluster.
- A single initiator group must be created for both nodes in the cluster.

You can create the initiator group automatically during disk creation or connection using the SnapDrive MMC. SnapDrive automatically selects an FC initiator from each of the ESX servers in the cluster. You can also create the initiator groups manually. If initiator groups do not already exist, you must create one manually on the storage system.

Microsoft cluster support limitations using FC RDM LUNs

SnapDrive supports Microsoft clusters using FC RDM LUNs on different virtual machines belonging to different ESX servers, but there are some instances when this feature is not supported.

- SnapDrive does not support clusters on ESX iSCSI and NFS datastore.
- SnapDrive does not support mixed initiators in a clustered environment.
Initiators must be either FC or Microsoft iSCSI, but not both.

Note: ESX iSCSI initiators and HBAs are not supported on shared disks in a Microsoft cluster.

- SnapDrive does not support MSCS on VMware guest OS virtual machine cluster nodes belonging to two different vCenters.
- SnapDrive does not support virtual machine migration with VMotion if the virtual machine is part of a Microsoft cluster.
- SnapDrive does not support MPIO on virtual machines in a Microsoft cluster.

Overview of installing or upgrading SnapDrive

This procedure gives an overview of the steps you need to follow to install or upgrade the SnapDrive for Windows application software.

Steps

1. Read the recommended documentation before beginning your installation or upgrade.
2. If you are installing SnapDrive for the first time, familiarize yourself with supported configurations and decide which configuration you want to deploy.
3. Prepare each Windows host in your SnapDrive configuration.
4. Prepare each storage system in your SnapDrive configuration.
5. Configure the required access for SnapDrive.
6. If you are upgrading an existing SnapDrive installation, perform the recommended upgrade preparations.
7. Install or upgrade the FC or iSCSI components.
8. Install the SnapDrive components.

Related concepts

[*Documents to read before installing SnapDrive*](#) on page 58

[*Considerations for determining SnapDrive configurations*](#) on page 59

Related tasks

[*Preparing hosts for SnapDrive*](#) on page 59

[*Preparing storage systems for SnapDrive*](#) on page 64

[*Configuring access for SnapDrive*](#) on page 66

[*Preparing to upgrade SnapDrive*](#) on page 69

[*Installing or upgrading the FC or iSCSI components*](#) on page 71

[*Installing or upgrading the SnapDrive components*](#) on page 73

Preparing to install or upgrade SnapDrive for Windows

Before you install or upgrade SnapDrive, you should determine what protocols you plan to use, the Windows server version you will be installing the application on, and you should read the related documentation.

Next topics

[Documents to read before installing SnapDrive](#) on page 58

[Considerations for determining SnapDrive configurations](#) on page 59

[Preparing hosts for SnapDrive](#) on page 59

[Preparing storage systems for SnapDrive](#) on page 64

[Configuring access for SnapDrive](#) on page 66

[Preparing to upgrade SnapDrive](#) on page 69

Documents to read before installing SnapDrive

Because SnapDrive for Windows installation requirements and procedures vary according to the protocols you use to create LUNs, before you begin your installation, you should familiarize yourself with documents related to each protocol you plan to use.

To create this type of LUNs...	Read the following documentation...
iSCSI-accessed LUNs	• This document. • If you are using the Microsoft iSCSI Software Initiator, the Microsoft iSCSI Software Initiator documentation, available at the Microsoft site. For the latest software compatibility information, see the Interoperability Matrix at: http://now.netapp.com/matrix/. • The iSCSI Host Attach Kit for Windows, the iSCSI Host Attach Kit for Windows Installation and Setup Guide; otherwise, the vendor documentation for your Windows Hardware Quality Lab (WHQL) signed iSCSI HBA. • <i>Data ONTAP Block Access Management Guide for iSCSI and FC</i>, which is available from the NOW site at now.netapp.com/NOW/products/interoperability/. • If you are using iSCSI on your storage system, the <i>Fibre Channel and iSCSI Configuration Guide</i> for the Data ONTAP version you are using.
FC-accessed LUNs	• This document. • FC Windows Host Utilities for Native OS Setup Guide, which shipped with your storage system. For the latest software compatibility information, see the Interoperability Matrix at: http://now.netapp.com/matrix/. • <i>Data ONTAP Block Access Management Guide for iSCSI and FC</i>, which is available on the NOW site at now.netapp.com/. • If you are using FC on your storage system, the <i>Fibre Channel and iSCSI Configuration Guide</i> for the Data ONTAP version you are using.

Considerations for determining SnapDrive configurations

SnapDrive for Windows supports a variety of configurations with differing requirements, so you should familiarize yourself with each and decide which configuration you plan to use before installing SnapDrive.

The following factors can help you decide which SnapDrive configuration to deploy:

- LUN access protocol—iSCSI, FC, or both
- Host operating system
- Host operating system Service Pack level
- Host operating system hotfix level (various combinations of mandatory and optional hotfixes, which are determined by host operating system, Service Pack level, and special SnapDrive options)
- Special options (Windows clustering, storage system cluster failover, MPIO)

Consider the following recommendations:

- Follow Microsoft's best practices recommendations for Windows server cluster network configuration. To find the best practices guides for your servers, search for "Windows server technical library" in the Microsoft TechNet Library, and choose the library for your operating system.

To determine the feasibility of SnapDrive configurations not described in this documentation, contact technical support.

Related references

Typical SnapDrive configurations on page 187

Related information

Microsoft TechNet Library - <http://technet.microsoft.com/en-us/library/>

Preparing hosts for SnapDrive

Before installing SnapDrive for Windows, you must prepare each Windows host in your SnapDrive configuration.

Steps

1. Verify that the host meets the minimum requirements for use with SnapDrive.
2. Determine whether the Microsoft iSCSI Software Initiator program is installed.

Note: If you are running Windows Server 2008, the iSCSI Software Initiator comes built in with the operating system, but needs to be enabled.

3. Determine whether SnapDrive has been previously installed.
4. Determine which FC or iSCSI HBA or MPIO components are already installed.

Next topics

[Minimum SnapDrive host requirements](#) on page 60

[Minimum SnapDrive requirements for VMware ESX Guest OS](#) on page 62

[Determining whether HBA or MPIO components are installed](#) on page 64

Minimum SnapDrive host requirements

Each Windows host in a SnapDrive for Windows configuration must meet minimum hardware, software, and OS requirements.

Hardware requirements

Component	Requirement
CPU	32-bit OS • 2.8 GHz Pentium 4 or compatible 64-bit OS • x64: Intel Xeon or AMD Opteron • IA64: Intel Itanium (for Windows Server 2008)
Memory	1 GB
NIC	The NIC you use to facilitate data transfer for the Microsoft iSCSI Software Initiator can come from any vendor, but it must be approved by Microsoft for use with Windows Server.

Operating system requirements

The host must be running either Windows Server 2008 Core Server or non-Core Server (x86, x64, or IA64), Windows Server 2008 Hyper-V (x64 only), Windows Server 2008 R2 Core or non-Core Server, or Windows Server 2003 Standard or Enterprise Edition with Service Pack 2 (x86 or x64), with the following hotfixes.

Note: For a list of the latest Service Packs and hotfixes required by SnapDrive, see the product description page in the software download section of the NOW site at now.netapp.com/.

Operating system and Service Pack level	Required hotfixes
Windows Server 2003 SP2 (x86 or x64)	919117 931300 932755 937382
Windows Server 2008, Server Core and non-Server Core installations (x86, x64, or IA64)	950927 955656
Windows Server 2008 (x64 only)	956697
Windows Server 2008 R2	

Software requirements

The exact number and type of HBAs and NICs required by each host depend on your specific SnapDrive configuration.

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

Component	Requirement
.NET Framework	.NET 3.5 SP1 or later Note: When you use .NET 3.5, SnapDrive requires the Net.Tcp Port Sharing Service to use the Local Service account, which is the default account, to enable the SnapDrive service to start properly. Note: .NET is not supported on Windows Server 2008 Server Core; it is, however, supported on Windows Server 2008 R2 Server Core.
NetApp Host Agent	If you are using NetApp Host Agent, you must upgrade to NetApp Host Agent 2.6 or later before upgrading to SnapDrive 6.3 on 32-bit systems.
MPIO	Data ONTAP DSM for Windows MPIO 3.3.1
FC driver and firmware	The latest FC driver and firmware is available on the NOW site at now.netapp.com/ . From this gateway, navigate to the SAN Host Attach Kit for Fibre Channel Protocol on Windows download page.

HBAs and software initiators	
FC	See the FC Host Utilities (Attach Kits) for Windows in the software download section at now.netapp.com/ .
iSCSI HBA	See the iSCSI Host Utilities (Support Kits) for Windows in the software download section at now.netapp.com/ .
Microsoft iSCSI Software Initiator	The Microsoft iSCSI Software Initiator must be downloaded from the Microsoft site at http://www.microsoft.com/downloads/ .

Minimum SnapDrive requirements for VMware ESX Guest OS

Each VMware guest OS host in a SnapDrive for Windows configuration must meet minimum software and controller requirements.

In addition to the software requirements detailed below, you should have the following information ready before beginning a SnapDrive installation:

- ESX server root credentials and IP address
- ESX vCenter credentials (if vCenter is installed)

Software requirements

Note: For the latest requirement updates, see the SnapDrive for Windows pages on the NOW site at now.netapp.com/.

Component	Requirement
VMware ESX server	Version 3.5 Update 5 or later, or 4.0 Update 1 or later.
Windows guest OS	• Windows Server 2003 SP2 or Windows Server 2008, x86 or x64, with the hotfixes specified in the SnapDrive host requirements • .NET Framework 3.5 SP1 or later
FC HBA	FC HBA in the ESX server with the FC ESX Host Utilities 5.1. See the Interoperability Matrix at now.netapp.com/NOW/products/interoperability/ for the latest supported FC HBAs.

Component	Requirement
iSCSI initiator	- Microsoft iSCSI Software Initiator in the guest OS For the latest supported version of the Microsoft iSCSI Software Initiator, see the iSCSI Host Utilities (Support Kits) for Windows in the software download section at now.netapp.com/. - ESX iSCSI initiator
Storport Miniport Driver LSI Logic SCSI Controller	Required if you are using RAW-device mapped LUNs; if you are connecting LUNs using the Microsoft iSCSI Software Initiator, you do not need the Storport Miniport Driver. The SCSI Port Miniport Driver is the default LSI Logic SCSI Controller included when Windows Server 2003 SP2 is installed as the Guest OS in ESX server. For proper SnapDrive operations with RAW-device mapped LUNs, the LSI Logic SCSI Controller must be updated with the Storport Miniport Driver. You can download the x86 or x64 version of this driver from http://www.lsi.com by searching for "LSI Logic Fusion-MPT SCSI Driver (StorPort)." Note: Windows Server 2008 includes the Storport Miniport Driver and does not need to be updated. For more recent updates on the controller requirements, see the SnapDrive Release Notes.
SCSI controllers	To support more than fifteen LUNs, the virtual machine must be preconfigured with four SCSI controllers creating a total of 60 LUNs. However, one RDM LUN or VMDK is assigned to each SCSI controller leaving 56 LUNs available for SnapDrive provisioning. Note: When you add a new SCSI controller to a virtual machine when using ESX 4.0, you must restart the SnapDrive service for SnapDrive to recognize the new controller.
VMware Tools	VMware Tools must be installed before beginning the SnapDrive installation in the guest OS.

Determining whether HBA or MPIO components are installed

You can use MMC to check if HBA or MPIO components are already installed on your Windows host.

Steps

1. In the left MMC pane, select **Device Manager**.
2. In the right MMC pane, double-click **Storage controllers**.

A list of installed FC and iSCSI controller components is displayed.

Preparing storage systems for SnapDrive

Before installing SnapDrive for Windows, you must prepare each NetApp storage system in your SnapDrive configuration.

Steps

1. Verify that the storage system meets the minimum requirements for use with SnapDrive.
2. After you verify that licenses for FC, iSCSI, or both are enabled on your storage system, you must start the services by entering the `fcpl start` command or the `iscsi start` command at the storage system command line.

See the *Data ONTAP Block Access Management Guide for iSCSI and FC* for more information.

3. Prepare a volume on the storage system to hold SnapDrive LUNs.

Next topics

[Minimum SnapDrive storage system requirements](#) on page 64

[Determining which licenses are enabled on a storage system](#) on page 65

[Preparing a volume for SnapDrive](#) on page 65

Minimum SnapDrive storage system requirements

Each storage system in a SnapDrive for Windows configuration must meet minimum component and license requirements.

Component	Requirement
Operating system	Data ONTAP 7.2 or later

Component	Requirement
HBAs and NICs	Verify that the HBAs and NICs in the storage system meet the requirements for your particular host-target SnapDrive configuration. Note: For information about the latest supported HBAs and NICs, see the System Configuration Guides page on the NOW site at now.netapp.com/now.netapp.com/.

License	Requirement if you want to...
iSCSI	Use iSCSI-accessed LUNs
FC	Use FC-accessed LUNs
SnapRestore	Restore LUNs from Snapshot copies
SnapMirror	Use the SnapMirror option
FlexClone	Enable volume clone functionality on flexible volumes
SnapVault	Use SnapVault for archiving LUN backup sets
MultiStore	Create LUNs on vFiler units

Note: The iSCSI and FC licenses supplied with SnapDrive enable all the CIFS functionality necessary for using SnapDrive with the RPC transport protocol. If you also want full-featured, direct CIFS access to a particular storage system, you must install a separate CIFS license on that storage system.

Determining which licenses are enabled on a storage system

You can use System Manager or FilerView to determine which licenses are enabled on your storage system, and to enable additional licenses. Follow this procedure to manage licenses with FilerView.

Steps

1. Using your Web browser, open a FilerView session to the storage system.
2. Navigate to **Filer > Manage Licenses**.

Preparing a volume for SnapDrive

You must create a storage system volume that can hold the LUNs to be managed by SnapDrive for Windows.

Considerations for preparing a SnapDrive volume

When you create a storage system volume to hold LUNs managed by SnapDrive for Windows, you should keep several things in mind.

Consider the following guidelines:

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

Note: Do not create LUNs on the /vol/vol0 volume.

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

- When multiple hosts share the same storage system, each host should have its own dedicated volume on that storage system to hold all the LUNs connected to that host.
- When multiple LUNs exist on a storage system volume, the dedicated volume on which the LUNs reside must contain the LUNs for just one host, and must not contain any other files or directories. Creating LUNs on different dedicated volumes is necessary to ensure that Snapshot copies are consistent and to avoid the possibility of busy Snapshot copies. To optimize Snapshot copy space usage, it is better to have fewer LUNs per volume, with one LUN per volume being the optimum configuration.

Configuring access for SnapDrive

Before installing SnapDrive for Windows, you must establish a SnapDrive service account and ensure that the authentication requirements are met.

Next topics

[SnapDrive service account requirements](#) on page 66

[When pass-through authentication might be required](#) on page 67

[Configuring SnapDrive pass-through authentication](#) on page 67

[User account requirements for SnapDrive Web services](#) on page 68

SnapDrive service account requirements

To perform functions related to SnapDrive for Windows on either the host or a storage system, SnapDrive needs to be able to use a service account that has specific types of access established.

The SnapDrive service account must meet the following requirements.

- The service account must be created using US-ASCII characters only, even when you use non-ASCII operating systems.
- You must be able to log in to the host using the service account.

Note: If at any time you change the password for this account (for example, from the Windows login panel), remember that you must make the same change to the password the SnapDrive

service uses to log in. You can configure the SnapDrive service using the Services and Applications option in MMC.

- The service account must have administrative rights on the host.

During SnapDrive installation, you are prompted to configure the default transport protocol as RPC, HTTP, or HTTPS.

- If you are using RPC authentication, the service account must have administrator privileges on both the storage system and the host and must belong to the BUILTIN\Administrators group on the storage system.
- If you are using RPC, the service account must be a domain account, or you can configure pass-through authentication.
- If you are using RPC, the host and storage system must belong to the same domain as the service account or to domains that have direct or indirect trust relationships with the domain to which the service account belongs, or you can configure pass-through authentication.

When pass-through authentication might be required

If you are using RPC authentication, you might need to configure pass-through authentication for SnapDrive for Windows between a Windows host and a storage system.

Pass-through authentication might be required in the following situations:

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

Configuring SnapDrive pass-through authentication

If you are using RPC authentication, you must ensure that pass-through authentication is configured correctly for SnapDrive for Windows on both the Windows host and on the storage system.

Before you begin

- You must have root privileges on the storage system.
- You must have administrator privileges on the Windows host.
- If you have a clustered SnapDrive configuration, you must use a domain account to run the cluster service, and all nodes of the cluster must be in the same domain. However, the storage system can be in a different domain or workgroup.

Steps

1. Create a user account on the storage system by entering the following command:

```
useradmin user add user_name -g group
```

user_name is the name of the SnapDrive user.

-g is the option you use to specify a user group.

group is the name of the group to which you want to add the new user.

Example

The following example adds a user called "snapdrive" to the BUILTIN\Administrators group on the storage system:

```
useradmin user add snapdrive -g Administrators
```

Note: You will need to provide this user name in a later step in this procedure. Therefore, make a note of the user name, including the letter case (lowercase or uppercase) of each character in the user name.

2. Enter a password, when prompted to do so, for the user account you are creating. You are prompted to enter the password twice.

Note: You need to provide this exact password in a later step in this procedure, so make a note of the password, including the letter case.

3. Check to ensure that the user account you just created belongs to the local administrator's group on the storage system by entering the following command:

```
useradmin user list
```

For additional information, see the section about creating local groups on the storage system in the *Data ONTAP File Access and Protocols Management Guide*.

4. On each Windows host that needs access to the storage system, create a local user account with administrative rights on the host, using the same user name and password that you specified in Step 1 and Step 2.

Note: Set up the local user account so that the password for the account never expires.

For detailed instructions on how to create local user accounts, see your Windows documentation.

5. If you are using Windows Server 2008, set the SnapDrive service on each host to use the local user account you created in Step 4.

User account requirements for SnapDrive Web services

To use SnapDrive for Windows via the Web services feature, you must log in to a user account that has specific types of access established.

The user account must meet the following requirements.

- If your SnapDrive host is stand-alone, the user account must have administrator privileges on the host or be a member of a group named "SnapDrive Administrators" on the host.
- If your SnapDrive host is part of a Windows domain, the user account can have local or domain administrator privileges, or be a member of a local or domain "SnapDrive Administrators" group.

Preparing to upgrade SnapDrive

Perform these preparations if you are upgrading SnapDrive for Windows from an existing installation.

Before you begin

You must be running SnapDrive 4.x , 5.x, or an earlier 6.x version to upgrade to SnapDrive 6.3.

Steps

1. Plan and announce downtime.

Pick a time for the upgrade when loss of access will have the least effect on your users. When the time you have set arrives, make sure that nobody is using the system and there are no SnapDrive operations running.

2. Back up your application data.

If you have SnapManager, use SnapManager rather than SnapDrive to create a backup. Make sure that you have a valid and up-to-date SnapManager backup and that no SnapManager backups are scheduled to occur while you are upgrading. If there are backups scheduled, cancel them.

3. If you are upgrading a server cluster, prepare the hosts by upgrading the operating systems on the cluster nodes to the required Service Pack and hotfix level if necessary.

If you need to apply a new Service Pack or hotfix, you will have to reboot the cluster.

4. Create a full backup, including system state, and create an Emergency Repair Disk for your single system, or for each node in a server cluster.

5. If you are using SnapDrive 4.1 or earlier with MPIO (ntapdsm.sys), and you want to upgrade both, you must uninstall the earlier version of SnapDrive without uninstalling the earlier MPIO drivers, or the installation fails.

MPIO is not installed with SnapDrive 6.3, and path management will not be available until a new version of MPIO is installed. To upgrade both SnapDrive and Data ONTAP DSM for Windows MPIO, complete the following steps.

a. Uninstall SnapDrive 4.1 or earlier using the Add/Remove Programs (or Programs and Features) utility in the Windows Control Panel.

This uninstalls SnapDrive without removing the legacy MPIO drivers.

b. Install Data ONTAP DSM for Windows MPIO.

For more information and to download the installation package, go to Multipath I/O on the NOW site.

- c. You are prompted to reboot.
6. If you are upgrading a server cluster, make sure that the Cluster Groups are online and that you can perform a “move group” operation back and forth between nodes.
Note: If the cluster service is not running, SnapDrive will be unable to collect data necessary for disk enumeration and will cause warning messages to be logged in the Event Viewer.
7. If you are running NetApp Host Agent, stop the NetApp Host Agent service.
Note: You might have to upgrade NetApp Host Agent, depending on the version you are running. See the SnapDrive 6.3 for Windows Release Notes for more information.
8. If you use SnapManager, stop SnapManager before upgrading SnapDrive.

Installing or upgrading SnapDrive

The SnapDrive for Windows installation wizard guides you through the process of installing or upgrading the SnapDrive application software.

Next topics

Installing or upgrading the FC or iSCSI components on page 71

Installing or upgrading the SnapDrive components on page 73

Preparing to install SnapDrive on Windows Server 2008 Server Core on page 76

Installing SnapDrive on Windows Server 2008 Server Core on page 79

Performing unattended SnapDrive installations on page 80

Enabling SnapDrive to communicate through the Windows Firewall on page 80

Installing or upgrading the FC or iSCSI components

SnapDrive supports three protocols for creating and managing LUNs: iSCSI, FC, and FCoE. Before you install SnapDrive for Windows, you need to install or upgrade these components on the host computer.

About this task

For the latest software compatibility information, see the Interoperability Matrix at: <http://now.netapp.com/matrix/>.

Step

1. Install or upgrade the required components for the protocols you plan to use.

If...	Then...
You will be using the iSCSI protocol and software initiator to create and manage LUNs	a. Install or upgrade the Microsoft iSCSI Software Initiator. b. Install the iSCSI Host Utilities on your hosts. Note: If you are running Windows Server 2008, the iSCSI Software Initiator comes built in with the operating system, but needs to be enabled.
You will be using the iSCSI protocol and hardware initiator to create and manage LUNs	a. Upgrade or install the iSCSI driver and firmware. b. Install the iSCSI Host Utilities on your hosts. For a list of supported iSCSI HBAs, see the iSCSI Support Matrix on the NOW site.

If...	Then...
You will be using the FC protocol to create and manage LUNs	Upgrade or install the FC driver and firmware. For more information, see the FC Windows Host Utilities for Native OS documentation on the NOW site. Note: The FC upgrade stops the SnapDrive service. SnapDrive restarts when the system is rebooted. If you proceed without a reboot, restart the SnapDrive service manually.

Installing or Upgrading the iSCSI Software Initiator

Use this procedure to install or upgrade the Microsoft iSCSI Software Initiator.

Before you begin

- Stop the SnapDrive for Windows service.
- If you are running SnapManager for Microsoft Exchange, stop any application-specific services that have iSCSI dependencies (for example, Microsoft Exchange System Attendant).

Note: You can also remove iSCSI dependencies using the SnapManager for Microsoft Exchange Configuration Wizard; however, this option is not recommended and should only be used if you are unable to stop the application-specific services.
- If you are installing or upgrading a cluster, first close MMC, then install the new iSCSI Software Initiator components on each node, starting with the nodes that do not own the cluster resources and rotating which system is the owner until all nodes in the cluster have the new iSCSI initiator installed.

Steps

1. Download the Microsoft iSCSI Software Initiator from the Microsoft site.

For more information about installing and configuring the Microsoft iSCSI Initiator, see the *iSCSI Host Utilities Guide* on the NOW siteThe NOW site.

2. Run the install package executable and proceed through the Installation wizard.
3. If you are going to use the iSCSI Initiator to create and manage LUNs, make sure that the Initiator Service and Software Initiator check boxes are selected on the **Installation Options** screen.

Note: The Virtual Port Driver option is unavailable because it is automatically installed during the Microsoft iSCSI Initiator installation and upgrade.

4. If you want to use MPIO, check the Microsoft MPIO Multipathing Support for iSCSI check box on the **Installation Options** screen.
5. Follow the prompts to complete the installation.

After you finish

Restart the SnapDrive service on the stand-alone host or on each node in the cluster.

Related tasks

Stopping and starting the SnapDrive service on page 85

Installing or upgrading the SnapDrive components

Use this procedure to install or upgrade the SnapDrive for Windows components.

Before you begin

- Make sure that you have prepared your host for SnapDrive and that all the minimum requirements are met.
- Perform this procedure from the system console, not from a Terminal Service client.
- If you are upgrading SnapDrive on a server cluster, install SnapDrive on all nodes, starting with the nodes that do not own the cluster resources and rotating which system is the owner until all nodes in the cluster have the same version of SnapDrive installed.
- If you are running NetApp Host Agent, stop the NetApp Host Agent service.
- If a version of SnapDrive is already installed on your system, stop the SnapDrive service, if you have not already done so, and close the Microsoft Management Console (MMC) window.
- If VMware vCenter or guest OS is present, the vCenter or ESX server user name that you enter must be assigned a vCenter role that has at least the minimum required privileges.
Use vCenter credentials if the virtual machines on which SnapDrive is being installed will belong to a Microsoft cluster.
- If you want to enable Snapshot copy management of VMDKs on NFS and VMFS datastores, ensure that VMtools is installed.
Have your SnapManager for Virtual Infrastructure server configured and have the SnapManager for Virtual Infrastructure IP address or server name and the TCP port number available when prompted.
- If you want to enable Hyper-V pass-through disk provisioning, have your Hyper-V server IP address and TCP port number available and enter when prompted.

Steps

1. Browse to the location of the SnapDrive installation package and double-click the executable file.
2. Click **Next** on the **Welcome to the SnapDrive Installation Wizard** screen.
3. If this is a new SnapDrive installation, read and accept the license agreement, and then click **Next**.
4. If you are upgrading SnapDrive, the **Program Maintenance** panel appears. Select **Modify/Upgrade**, and then click **Next**.

5. The **SnapDrive License** panel is displayed. Select which type of licensing you want to use, enter your license key in the space provided if you are using host-side (per server) licensing, and then click **Next**. (If you are upgrading, the license information will already be filled in.)

If you choose storage system licensing, you can install SnapDrive without entering a license key, and you will be able to execute SnapDrive operations only on storage systems that have a SnapDrive or SnapManager license installed.

6. If this is a new installation, follow the procedure in this step. If you are upgrading, skip to the next step.
 - a. In the **Customer Information** panel, type your user name and organization name, and then click **Next**.
 - b. The **Destination Folder** panel prompts you for a directory in which to install SnapDrive on the host. By default, this is C:\Program Files\NetApp\SnapDrive\ for new installations.

To accept the default, click **Next** and then proceed to the next step.

To specify a different location, click the **Change** button. In the **Change Current Destination Folder** panel, either type the path to the target directory in the Folder Name text box, or navigate to the folder you prefer and select it. When the correct target location appears in the Folder Name text box, click **OK** to return to the **Destination Folder** panel, and then click **Next**.

Note: If you are upgrading SnapDrive from a version earlier than 4.1, the default installation directory is C:\Program Files\SnapDrive\.

7. If the VMware ESX guest OS is detected, you are prompted to enter the IP address and a user name having the appropriate vCenter or ESX server privileges. On the **VirtualCenter or ESX Server Web Service Credentials** screen, type in the IP address of the vCenter or ESX server and the user name and password for SnapDrive to use for Web service authentication. If you want to be able to use VMotion, make sure you use the vCenter.

Note: Selecting "Enable VirtualCenter or ESX Server Settings" enables SnapDrive to use RDM pass-through LUNs. Select this option if you plan to use RDM pass-through disks. This option is not selected by default.

8. If SnapManager for Virtual Infrastructure is detected, you are prompted to enter the SnapManager for Virtual Infrastructure server IP address and the TCP port number if it is something other than the default of 8043.
9. On the **SnapDrive Management Service Credentials** screen, if you are upgrading and the account name is already filled in, type the account password in both the Password and Confirm Password text boxes, and then click **Next**. Otherwise, you can type in the account you want to use, or complete the following steps to select a user account.
 - a. Click **Add**.

The **Select User** window is displayed.

- b. In the "From this location" field, verify that the location is set to the proper domain if your storage system is in a domain, or click the **Locations** button and select the local host if your storage system is in a workgroup.
- c. In the "Enter the object name to select" text box, type the user name with administrator privileges that you want to use, and then click the **Check Names** button to verify the user you entered. Click **OK**.

Note: If you are installing SnapDrive for use with a storage system in a workgroup, enter the name of the user that you configured for pass-through authentication.

- d. Type the account password in both the Password and Confirm Password text boxes, and then click **Next**.
10. In the **SnapDrive Web Service Configuration** window, leave the default ports unless any of them are already being used exclusively by another service. Click **Next**.
11. In the **Transport Protocol Default Setting** window, leave the default setting of RPC unless your environment requires the use of HTTP or HTTPS.
- a. If you choose to use HTTP or HTTPS, type the user name and password for SnapDrive to use for authentication. The default ports of 80 for HTTP or 443 for HTTPS are filled in automatically.

Note: If you set up SnapDrive to use HTTP or HTTPS to communicate with storage systems, using the domain Administrator account for authentication results in significantly reduced performance. To avoid this issue, use a storage system account for authentication instead of the domain account.

- b. Click **Next**.
12. If you want to enable SnapDrive to communicate with Operations Manager, complete the following steps on the **Operations Manager Configuration** screen.
- a. Select the Enable Protection Manager Integration checkbox.
 - b. Type the name or IP address of the Operations Manager server in the Operations Manager Name/IP Address field.
 - c. Select HTTP or HTTPS.
 - d. Leave the default port of 8088 for HTTP or 8488 for HTTPS, unless Operations Manager is configured to use a different port.
 - e. Type the user name and password for SnapDrive to use for authentication.
 - f. Click **Next**.

Note: If you do not enable Protection Manager integration during the installation, you can configure these settings later using the SnapDrive command-line interface.

13. On the **Ready to** panel, click **Install** or **Upgrade**.

14. When the *SnapDrive Installation Completed* screen appears, click *Finish*.

Note: If you are upgrading a server cluster and you try to use MMC after upgrading SnapDrive on the first node and before upgrading SnapDrive on the remaining nodes, you get an error message indicating that the SnapDrive service is unavailable owing to an invalid tag. This message is the result of the temporary presence of two versions of SnapDrive on the same cluster. No corrective action is needed; just upgrade SnapDrive on the other nodes.

Result

A shortcut to the standalone SnapDrive for Windows Management Console is added to the Start Menu, and you can also access the SnapDrive snap-in in MMC.

After you finish

- If you are running Windows Server 2008, you must configure the Windows Firewall to allow SnapDrive communications.
- If you are upgrading or installing SnapDrive to support a SnapManager installation, and you use verification servers, you must install SnapDrive on the verification servers as well as on the production systems, and both the verification server and the production servers must be using the same version of SnapDrive.
- If a verification server will be connecting to LUNs over an iSCSI session, make sure you also install the Microsoft iSCSI Software Initiator on the verification server and establish a session from the verification server to the iSCSI target on the storage system where the database to be verified resides. This connection enables the verification server to connect to the Snapshot copy LUN that contains the database, and you must create it explicitly before the verification server attempts to connect to the LUN.

Related tasks

[*Preparing hosts for SnapDrive*](#) on page 59

[*Installing or Upgrading the iSCSI Software Initiator*](#) on page 72

[*Stopping and starting the SnapDrive service*](#) on page 85

[*Enabling SnapDrive to communicate through the Windows Firewall*](#) on page 80

Preparing to install SnapDrive on Windows Server 2008 Server Core

Before you can install SnapDrive for Windows on a Windows Server 2008 or a Windows Server 2008 R2 Server Core system, you must enable remote administration, rename the server, join the domain, and disable the server firewall.

Next topics

[*Enabling remote administration on the Server Core system*](#) on page 77

Renaming the Server Core system on page 77

Joining the Server Core system to a domain on page 77

Disabling Windows Server Core firewall on page 78

Installing Microsoft Visual C++ 2008 Redistributable Package on the Server Core system on page 78

Installing .NET Framework on Windows Server 2008 R2 Server Core on page 78

Enabling remote administration on the Server Core system

Before you install SnapDrive for Windows on the Server Core system, you must enable remote administration so you can manage the core SnapDrive instance from a Windows GUI SnapDrive instance.

Steps

1. At the Windows Server Core command prompt, enter the following command:

```
netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
```

2. Enter the following command:

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

Renaming the Server Core system

Before you install SnapDrive for Windows on the Server Core system, you should rename the server to something more meaningful.

Step

1. At the Windows Server Core command prompt, enter the following command:

```
netdom renamecomputer ComputerName /NewName:NewComputerName
```

Joining the Server Core system to a domain

Before you install SnapDrive for Windows on the Server Core system, you must add the server to the appropriate domain.

Step

1. At the Windows Server Core command prompt, enter the following command:

```
netdom join ComputerName /domain:DomainName/userid:UserName /password:Password
```

Disabling Windows Server Core firewall

Before you install SnapDrive for Windows on the Server Core system, you must disable the firewall to enable SnapDrive communications.

Step

1. At the Windows Server Core prompt, enter the following command:

```
netsh firewall set opmode mode=disable
```

Installing Microsoft Visual C++ 2008 Redistributable Package on the Server Core system

Before you install SnapDrive for Windows on the Server Core system, you must install Microsoft Visual C++ 2008 Redistributable Package (x64) or your SnapDrive installation will fail.

About this task

This task applies only when you install SnapDrive on Windows Server 2008 Server Core. It does not apply when you install SnapDrive on Windows Server 2008 R2 Server Core.

Steps

1. On a full Windows Server 2008 installation, create a share to the Server Core system using Microsoft Management Console.
2. Download Microsoft Visual C++ 2008 Redistributable Package (x64) from the Microsoft site at www.microsoft.com/downloads/ to a folder on the remote server.
3. Copy the package to the share you created on the remote server.
4. Install the package from the Server Core system command prompt.

Installing .NET Framework on Windows Server 2008 R2 Server Core

Before you install SnapDrive on Windows Server 2008 R2 Server Core, you must install the .NET Framework or your SnapDrive installation will fail.

Steps

1. Using Deployment Image Servicing and Management (DISM.exe), enter the following command at the Microsoft command prompt:

```
Dism /online /enable-feature /featurename:NetFx2-ServerCore
```

2. To complete the .NET Framework installation, enter the following command:

```
Dism /online /enable-feature /featurename:NetFx3-ServerCore
```

Installing SnapDrive on Windows Server 2008 Server Core

You can install SnapDrive for Windows on Windows Server 2008 and Windows Server 2008 R2 Server Core systems to enable LUN provisioning and Snapshot copy management from a remote instances of SnapDrive for Windows running on a non-core system.

Before you begin

The following conditions must exist before you install SnapDrive on a Server Core system:

- Remote administration is enabled.
- The Server Core system is renamed in a meaningful way.
- The Server Core system is a member of the Windows domain.
- The firewall is disabled.
- The Microsoft Visual C++ 2008 Redistributable Package (x64) is installed.
- If you are installing SnapDrive on Windows Server 2008 R2 Server Core, .NET is installed, including WCF activation.

About this task

The `SERVER_CORE_SYSTEM=1` switch must be used only with Windows Server 2008 Server Core installations. Do not use the `SERVER_CORE_SYSTEM=1` switch if you are installing SnapDrive on Windows Server 2008 R2 Server Core.

Steps

1. On a full Windows Server 2008 installation, create a share to the Server Core system using Microsoft Management Console.
2. Download `snapdrive.exe` to a folder on the remote Windows server.
3. Copy `snapdrive.exe` to the share you created on the remote server.
4. Create a file called `install.bat` on your Server Core system and copy the following unattended install command into the file. Add the serial number, password and username as necessary.

```
snapdrive6.3.exe /s /v"/qn SILENT_MODE=1 SERVER_CORE_SYSTEM=1 /Li
SDInstall.log LPSM_SERIALNUMBER=serialnumber INSTALLDIR=\"c:\Program
Files\NetApp\SnapDrive\" SVCUSERNAME=domain\username
SVCUSERPASSWORD=password SVCCONFIRMUSERPASSWORD=password"
SDW_WEBSRV_TCP_PORT=808 SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2 TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password"
```

5. Run `install.bat` from the Server Core system command prompt. Alternately, you can enter the unattended install command from the command prompt.

Performing unattended SnapDrive installations

Using batch file scripts can greatly simplify the task of installing, upgrading, or uninstalling SnapDrive for Windows on multiple systems.

Before you begin

SnapDrive does not support unattended upgrade or removal of SnapDrive versions earlier than 4.0, nor does it support unattended upgrade of earlier MPIO (ntapdsm.sys) versions to Data ONTAP DSM for Windows MPIO.

Steps

1. Copy the SnapDrive executable to your Windows host.
2. Create a batch file (a file with a .bat extension) containing the appropriate switch combinations for the type of unattended install you would like to perform.

Related references

[*Unattended SnapDrive installation reference*](#) on page 177

Enabling SnapDrive to communicate through the Windows Firewall

If the Windows Firewall is enabled on your host, you need to configure it to allow SnapDrive for Windows communications. The Windows Firewall is enabled by default in Windows Server 2008.

Steps

1. Navigate to **Control Panel > Windows Firewall > Allow a program through Windows Firewall > Exceptions**.
2. If you will be using HTTP or HTTPS, select the World Wide Web Services (HTTP) or Secure World Wide Web Services (HTTPS) checkboxes.
3. Click **Add program**.
4. Click **Browse** and browse to C:\Program Files\NetApp\SnapDrive\, or to wherever you installed SnapDrive if you did not use the default location.
5. Select SWSvc.exe and click **Open**, then click **OK** in the **Add a Program** window and in the **Windows Firewall Settings** window.

Note: If Windows Firewall is enabled on your SnapDrive host and you want to use the -m option in the command-line interface to execute a command from a remote host, you must add

sdcli to the allowed programs list for Windows Firewall. Follow the same procedure as for adding SWSvc.exe.

6. To verify that SWsvc.exe and sdcli.exe are in the list of inbound rules, in MMC, navigate to **Windows Firewall > Inbound Rules**.

Managing SnapDrive

SnapDrive includes features that enable you to perform general SnapDrive management tasks.

Next topics

[Managing host-side SnapDrive licenses](#) on page 83

[Enabling SnapDrive notification settings](#) on page 84

[Setting a preferred IP address](#) on page 85

[Stopping and starting the SnapDrive service](#) on page 85

[Adding and removing initiators with SnapDrive](#) on page 86

[Administering SnapDrive remotely](#) on page 86

Managing host-side SnapDrive licenses

You can view, change, or disable your SnapDrive license after you have installed it on your local host, using either the SnapDrive MMC snap-in or the SnapDrive command line interface (`sdccli.exe` command). You can also manage licenses on remote hosts if you have added those hosts to your SnapDrive MMC.

Steps

1. Expand the SnapDrive option in the left MMC pane.

Local and remote SnapDrive hosts are displayed.

2. Right-click the SnapDrive host for which you want to manage a SnapDrive license and select **SnapDrive Licenses**.

The **SnapDrive Licenses** window is displayed.

3. View, change, or disable the license as needed.

Note: If you disable the host-side license, you can execute SnapDrive operations only on storage systems that have a SnapDrive or SnapManager license installed.

Related references

[License commands](#) on page 209

Enabling SnapDrive notification settings

SnapDrive enables you to set up e-mail notification and to enable storage system AutoSupport in the event of a SnapDrive message or storage system error.

Before you begin

To use storage system AutoSupport with SnapDrive Notification Settings, you must enable AutoSupport on the storage system.

About this task

When you set up notification, you can specify the following information:

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

Steps

1. Select the appropriate SnapDrive instance, then from the menu choices on top of MMC, click **Action > Notification Settings**.
2. Select **Use Storage System AutoSupport** if you want to enable a subset of the Windows System Events for AutoSupport on the storage system.
3. In the Notification Settings panel, select **Enable SnapDrive E-mail Notification**.
4. Under E-mail Settings, type the outgoing SMTP server, and the From and the To e-mail addresses.

Note: The e-mail address must be in a valid SMTP format, for example, administrator@mycompany.com.

5. Under Event Category, select one or more event categories about which you want to be notified.
6. Under Event Type, select one or more event types about which you want to be notified when the specified event types take place.
7. Click **OK**.

Setting a preferred IP address

If your storage system has more than one IP address, you can configure SnapDrive for Windows to use one of those addresses as the preferred IP address for management traffic.

About this task

Even if your storage system has only one IP address, setting a preferred IP address prevents issues from occurring if additional interfaces are added later.

Note: Setting a preferred IP address is not a substitute for proper name resolution. The host and storage system names must still be resolved by DNS.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then select **Disks**.
2. Right-click **Disks** and select **Properties** from the menu.
3. In the **Disks Properties** window, click the **Preferred Storage System IP Addresses** tab.
4. Enter the storage system name and preferred IP address for that storage system in the spaces provided.

Note: If you are using an iSCSI HBA in your storage system, do not set the IP address of the target HBA as the preferred IP address. Instead, use the IP address of the storage system's management port.

5. Click **Apply**.
6. Repeat Step 3 and Step 4 for each storage system on which you want to set a preferred IP address.
7. Click **OK**.

Stopping and starting the SnapDrive service

You can stop or start the SnapDrive for Windows service using MMC.

Steps

1. In the left MMC pane, expand the **Services and Applications** option and select **Services**.
2. In the right MMC pane, scroll down the list of service and locate the SnapDrive service.
3. Double-click **SnapDrive**.

The **SnapDrive Properties** window is displayed.

4. Under "Service status", click **Stop** or **Start**, then click **OK** to exit the **SnapDrive Properties** window.

Adding and removing initiators with SnapDrive

You can use SnapDrive to add or remove initiators for LUNs created using SnapDrive.

Steps

1. Double-click SnapDrive in the left MMC pane, and then, if the Disks option is not already expanded, double-click Disks.

The currently connected disks are displayed.

2. Select the disk for which you want to add or remove initiators.
3. From the menu choices on top of MMC, click **Action > Add/Remove Initiator**.

The **Initiators Management** screen is displayed.

Note: You do not have the option to add or remove initiators for LUNs created on a VMware Guest OS.

4. To add or remove initiators, follow the instructions in the **Initiators Management** screen.

Note: If you remove an initiator that belongs to an igroup to which other initiators have been added, a dialog box informs you that all initiators will be removed. Click **Yes** to remove all initiators. If you try to remove an initiator that belongs to an igroup that contains initiators from another host, the operation will fail. SnapDrive does not support this configuration.

5. Click **OK**.

Administering SnapDrive remotely

You can simplify management of multiple SnapDrive installations using the "Add SnapDrive Server" and "Connect to another computer" features to add and delete remote SnapDrive installations.

Next topics

[*Adding a remote SnapDrive instance*](#) on page 87

[*Deleting a remote SnapDrive instance*](#) on page 88

[*Managing SnapDrive remotely using Connect to another computer*](#) on page 88

Adding a remote SnapDrive instance

Use the **Add SnapDrive Server** option to add remote SnapDrive instances to a local SnapDrive MMC to manage SnapDrive on multiple servers from a single server.

Before you begin

To add remote instances of SnapDrive to MMC, the remote Windows host must meet the following requirements:

- The host must exist.
- SnapDrive must be installed and the SnapDrive service must be running.
- The same version of SnapDrive that is installed on your local host must be installed on your remote machine.

Note: There is no requirement regarding the OS type that is running on either the local or remote hosts.

Steps

1. In the left MMC pane, select **SnapDrive**.
2. From the menu choices at the top of MMC, navigate to **Action > Add SnapDrive Server**.

The **Add SnapDrive Server** window is displayed.

3. In the **Add SnapDrive Server** window, type the name of the SnapDrive server you want to manage.
4. If the SnapDrive server you are adding belongs to a Microsoft cluster, select "Add SnapDrive instances from all the Microsoft cluster nodes."

Note: By default, SnapDrive uses the local host's SnapDrive Web service TCP/IP endpoint port number. Ensure that all nodes in the cluster use the same port number; otherwise, do not select this option then add each cluster node separately.

5. Click **Add**.
6. If the server name you entered resides in a domain that is not one of the local server's trusted domains, enter the username and password for that domain.

Note: When you manage a remote instance of SnapDrive that is not in a trusted domain, you will not be able to see the remote system's Event Viewer and you will receive the error "Access Denied." You can ignore this error and continue to perform SnapDrive management operations.

The remote SnapDrive instance is listed under **SnapDrive Instances Managed** in the center MMC pane, and in the left MMC pane beneath the local SnapDrive instance.

SnapDrive saves the list of SnapDrive instances that have been added to MMC and loads the list whenever MMC is restarted.

7. To add additional remote SnapDrive server instances, repeat Step 1 through Step 4.

Note: SnapDrive does not limit the number of remote instances you can add to the local SnapDrive server.

Deleting a remote SnapDrive instance

Delete a remote SnapDrive instance from a local SnapDrive MMC when you no longer want to manage that instance.

Steps

1. In the left MMC pane, select the remote SnapDrive server instance you want to delete.
2. From the menu choices at the top of MMC, navigate to **Action > Remove SnapDrive Server**.
3. Click **Yes** in the **Remove SnapDrive Server** pop-up window.

The remote SnapDrive instance is removed from the local SnapDrive MMC.

Managing SnapDrive remotely using Connect to another computer

Use the Connect to another computer feature to manage SnapDrive on a remote computer MMC.

Before you begin

To perform remote administration of SnapDrive, the remote Windows administration host machine must meet the same software requirements as the production host machine, except that you do not need to install the LUN drivers. Check that the following specific requirements are met:

- The same version of SnapDrive must be installed on both the production machine and the remote machine.
- When prompted during installation for the account used to access the storage system, you must specify the same account used for access from the production host machine.

Steps

1. In MMC, select **Computer Management**.
2. From the menu selections at the top of MMC, navigate to **Action > Connect to Another Computer**.
3. Enter the host name of the remote SnapDrive server you want to manage, and then click **OK**.

The remote host machine's MMC window appears on your local machine, enabling you to manage SnapDrive remotely.

Enabling RBAC for use with SnapDrive for Windows

Before you can use DataFabric Manager role-based access control (RBAC) with SnapDrive for Windows, you must make this feature available by first enabling the service on your storage system, then configuring your SnapDrive for Windows system with the appropriate DataFabric Manager server credentials, and finally adding and assigning roles to SnapDrive for Windows users.

Next topics

[*Using role-based access control \(RBAC\) with DataFabric Manager server*](#) on page 89

[*Enabling RBAC on the storage system*](#) on page 91

[*Configuring SnapDrive for Windows to use RBAC*](#) on page 91

[*Creating SnapDrive user roles on DataFabric Manager server*](#) on page 92

[*Assigning roles to SnapDrive users on DataFabric Manager server*](#) on page 93

Using role-based access control (RBAC) with DataFabric Manager server

SnapDrive provides support for role-based access control with DataFabric Manager server to separate server administrator and storage administrator functions, and to limit SnapDrive actions and operations depending on the role or job function of the user.

Role-based access control enables an application or Windows server administrator to provision and manage storage for their resources without needing the storage system root password.

When SnapDrive is configured for role-based access control, SnapDrive serves as the policy decision point. For every SnapDrive operation, an RBAC access check to DataFabric Manager is performed. The RBAC access check verifies whether a SnapDrive user can perform a SnapDrive operation on a storage system resource. The SnapDrive MMC displays only the object types to which a user has been granted access to perform a task.

If DataFabric Manager encounters a short service outage, SnapDrive is not affected. If a prolonged outage occurs, however, SnapDrive will no longer operate.

Note: If DataFabric Manager server is down, the SnapDrive administrator can request the storage system administrator to disable role-based access control.

The following requirements must be met in order for SnapDrive to use role-based access control:

- DataFabric Manager server must be present and configured in the IP network in which the storage system and the SnapDrive hosts exist.
- DataFabric Manager server must be version 3.7 or later.

- The DataFabric Manager server must have pre-defined roles, operations and capabilities for SnapDrive.
- The storage system administrator must enable the DataFabric Manager server RBAC flag in the `AccessControl.xml` file located in the root volume of the storage system.
- SnapDrive must be configured by the host administrator with the DataFabric Manager server name and credentials in order to use role-based access control; otherwise, SnapDrive continues to use the original access control method, if one was configured.

DataFabric Manager server name and credentials can be entered during SnapDrive installation or by using `sdcli.exe`.

- To enable backup operations to proceed, a role with `SD.Config.Read` and `SD.Config.Write` capabilities must be created and applied by the storage administrator at the storage system level. For example, at the STORACL prompt, use the following command to create a new role:

```
role add -rn SDConfigRole -OPN SD.Config.Read SD.Config.Write
```

To apply the new role to the domain user on the specified storage system use the following command:

```
user add -rsn StorageSystemName -rtype stor -un domain\user -RN SDConfigRole
```

- For disk create and connect operations to succeed using either the automatic igroup creation option or the manual igroup creation option with SnapDrive, the following permissions must be set:
 - If you choose the automatic igroup creation option, `SD.Config.Write`
 - If you choose the manual igroup creation option, `SD.Config.Read`

See the *Operations Manager Administration Guide* for your version of DataFabric Manager server for more information about roles and capabilities and how they are used. See the *Storage Access Control Tool User's Guide* for more information about the `storacl.exe` tool.

Related tasks

[Enabling RBAC on the storage system](#) on page 91

[Configuring SnapDrive for Windows to use RBAC](#) on page 91

[Creating SnapDrive user roles on DataFabric Manager server](#) on page 92

[Assigning roles to SnapDrive users on DataFabric Manager server](#) on page 93

Related references

[SnapDrive for Windows to DataFabric Manager role mappings](#) on page 201

[DataFabric Manager commands](#) on page 237

[The `dfm\_config rbaccache` command](#) on page 238

Enabling RBAC on the storage system

The first step toward enabling RBAC for use with SnapDrive for Windows is having the storage administrator enable the feature on the storage system.

Steps

1. Download `storac1.exe` from the ToolChest on the NOW site to your Windows host.
2. Run `storac1.exe` from the location to which you downloaded it on your Windows host.
3. At the `STORACL>` prompt, enter the following command:

```
create -stor StorageSystem -user UserName -pwd password
```

The `AccessControl.xml` file is created in the `/etc` directory of your storage system root volume.

4. At the `STORACL` prompt, enter the following command:

```
dfmrbac set -val true
```

.

See the *Operations Manager Administration Guide* for your version of DataFabric Manager server for more information about RBAC.

After you finish

You will next configure SnapDrive for Windows to use the DataFabric Manager RBAC feature.

Configuring SnapDrive for Windows to use RBAC

After your storage administrator enables RBAC on the storage system, you must configure your SnapDrive for Windows host with the proper DataFabric Manager server credentials.

Before you begin

The following conditions must exist before you configure SnapDrive to use RBAC:

- The SnapDrive service account has administrative privileges on both the storage system and the host.
- The user you specify from SnapDrive is configured with `DFM.Core.AccessCheck` capability in the global scope in DataFabric Manager server.

Step

1. If you did not configure your SnapDrive for Windows host with your DataFabric Manager server information when you installed SnapDrive, use the `sdcli dfm_config` command to enter the hostname, username, and password of the user accessing DataFabric Manager.

After you finish

You will next create SnapDrive user roles using DataFabric Manager.

Related tasks

[Configuring access for SnapDrive](#) on page 66

Creating SnapDrive user roles on DataFabric Manager server

After you configure SnapDrive for Windows to use RBAC, you must create roles on the DataFabric Manager server to grant access to SnapDrive for Windows users according to the SnapDrive operations you want them to perform.

Before you begin

The domain or workgroup users to whom you want to assign roles must already be created.

About this task

Perform these steps on DataFabric Manager using the Operations Manager interface. See the *Operations Manager Administration Guide* for your version of DataFabric Manager server for more information about creating roles using the Operations Manager interface.

Steps

1. Select **Roles** from the **Setup** menu.
2. Click **Add Capabilities...**, and from the **Capabilities** window, select a resource from the resource tree.
3. Select the capabilities you want for the new role you are creating in one of two ways:
 - Select the operations that you want to allow for the resource.
 - To inherit roles, select that role from the **Inherit Capabilities** list on the left, and click >> to move it to the list on the right.
4. Click **Add Role**.

After you finish

You will next assign roles to SnapDrive users.

Assigning roles to SnapDrive users on DataFabric Manager server

After you create roles on DataFabric Manager server, you must assign the roles to SnapDrive users.

About this task

Perform these steps on DataFabric Manager using the Operations Manager interface. See the *Operations Manager Administration Guide* for your version of DataFabric Manager server for more information about assigning roles using the Operations Manager interface.

Steps

1. Select **Administrative Users** from the **Setup** menu.
2. Type the name of the administrator or Windows group to which you want to assign a role.
3. Select the role from the list on the left and click >> to move it to the list on the right.
4. Click **Add**.

Managing iSCSI sessions

SnapDrive enables you to manage iSCSI sessions on the storage system.

Next topics

[*iSCSI software initiator node naming standards*](#) on page 95

[*Establishing an iSCSI session to a target*](#) on page 96

[*Disconnecting an iSCSI target from a Windows host*](#) on page 97

[*Disconnecting a session to an iSCSI target*](#) on page 98

[*Examining details of an iSCSI session*](#) on page 99

iSCSI software initiator node naming standards

While it is possible to rename iSCSI software initiator nodes on a SnapDrive for Windows host, Data ONTAP requires standard iSCSI software initiator node names.

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

The following are the formats for standard initiator node names.

IQN-type node name uses the following format:

`iqn.yyyy-mm.reverse_domain_name:any`

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

Note: A dash (-) is allowed in the IQN name; however, an underscore (_) is not allowed.

IQN-type node name example

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

EUI-type node name example

`eui.02004567A425678D`

Establishing an iSCSI session to a target

Before creating a LUN, you need to have an iSCSI session to the target on which you will manage the LUN.

Before you begin

Verify that the iSCSI service is started.

About this task

- An iSCSI sessions can be established only between the same IP versions. The iSCSI session must be either IPv6 to IPv6 or it must be IPv4 to IPv4. The iSCSI sessions cannot be a combination of the two IP versions.
- A link-local IPv6 address can be used for iSCSI session management and for communication between a host and a target only when both are in the same subnet.

Steps

1. Perform the following actions to launch the Create iSCSI Session wizard:
 - a. In the left MMC pane, select the instance of SnapDrive you want to manage.
 - b. Select **iSCSI Management**.
 - c. From the menu choices at the top of MMC, navigate to , **Action > Establish Session**.
2. In the **iSCSI Session** wizard, click **Next**.
The **Provide Storage System Identification** panel is displayed.
3. In the **Provide Storage System Identification** panel, enter the storage system name or IP address of the storage system management port you want to establish the iSCSI session with, and then click **Next**.

Note: The IP address you enter is the storage system management port IP address, not the target portal IP address to which SnapDrive will establish an iSCSI session. You will select the IP address for establishing an iSCSI session in Step 5.

The **Provide iSCSI HBA** panel is displayed.

4. In the upper pane of the **Provide iSCSI HBA** panel, click the radio button next to an available iSCSI HBA to specify the initiator portal you want to use.
5. In the lower pane of the **Provide iSCSI HBA** panel, perform the following actions:
 - a. Select the target portal to which SnapDrive will establish the iSCSI session by clicking the radio button next to the IP address of the target portal you want to use.

- b. If your target requires authentication, select **Use CHAP**, and then type the user name and password that iSCSI will use to authenticate the initiator to the target.
- c. Click Next.

The **Completing the iSCSI Session Wizard** panel is displayed.

6. In the **Completing the iSCSI Session Wizard**, perform the following actions:
 - a. Review the information to make sure it is accurate.
 - b. If the information is not accurate, use **Back** to go back to previous panels of the wizard to modify information.
 - c. Click **Finish**.

Result

An iSCSI session to the target is established.

How SnapDrive uses CHAP authentication

If it is required by your storage system, use CHAP authentication to validate the identity of the login information being sent to the storage system from an iSCSI initiator when you create an iSCSI session.

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

Note: SnapDrive requires that the CHAP password contains at least 12 characters.

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

Disconnecting an iSCSI target from a Windows host

You can disconnect an iSCSI target from a Windows host if there are no LUNs connected to it.

Before you begin

You must disconnect any LUNs connected to the target before the target can be disconnected.

Steps

1. Perform the following actions to disconnect an iSCSI target:

- a. In the left MMC pane, select the instance of SnapDrive from which you want to disconnect an iSCSI target .
- b. Double-click **iSCSI Management**.
- c. Select the iSCSI session that you want to disconnect.
- d. From the menu choices at the top of MMC, navigate to **Action > Disconnect Target**.

A SnapDrive pop-up box is displayed prompting you to confirm your action. Additionally, if you have LUNs connected to the iSCSI target, a warning pop-up box is displayed prompting you to confirm that all access to the LUNs on the iSCSI target can be terminated.

2. Click **Yes**.

Result

The selected iSCSI target is disconnected from the Windows host.

Disconnecting a session to an iSCSI target

You can disconnect an iSCSI session to an iSCSI target when you have more than one session and you do not want to disconnect the target or other sessions connected to that target.

Steps

1. Perform the following actions to disconnect a session to an iSCSI target:
 - a. In the left MMC pane, select the instance of SnapDrive for which you want to disconnect an iSCSI session.
 - b. Double-click **iSCSI Management**.
 - c. Select the iSCSI target from which you want to disconnect a session.
2. In the center MMC pane, select the iSCSI session you want to disconnect.
3. From the menu choices at the top of MMC, navigate to **Action > Disconnect Session**.

Note: If you have only one iSCSI session connected to the iSCSI target, performing this procedure will disconnect the iSCSI target from the Windows host.

A SnapDrive pop-up box is displayed prompting you to confirm your action. Additionally, if you disconnect the last session to the iSCSI target and you have LUNs connected to the target, a warning pop-up box is displayed prompting you to confirm that all access to the LUNs on the iSCSI target can be terminated.

4. Click **Yes**.

Result

The selected iSCSI session is disconnected from the iSCSI target.

Examining details of an iSCSI session

You can view details for each of the iSCSI sessions in SnapDrive.

Steps

1. In the left MMC pane, select the instance of SnapDrive you want to examine.
2. Double-click **iSCSI Management**.
3. Select the connected iSCSI target whose details you want to view.

Session details are displayed in the lower pane of the center MMC panel.

Creating LUNs

SnapDrive enables you to quickly create LUNs on a storage system for use in a Windows environment.

Next topics

[Rules for creating LUNs](#) on page 101

[About volume mount points](#) on page 102

[Creating a dedicated LUN](#) on page 102

[Creating a shared LUN](#) on page 106

[Creating a LUN as a quorum on a Windows 2003 cluster](#) on page 110

[Windows Server 2008 failover cluster support](#) on page 113

[Configuring a Windows Server 2008 failover cluster witness disk](#) on page 113

[Creating an RDM LUN on a guest OS](#) on page 114

[Creating a highly available Hyper-V virtual machine using SnapDrive](#) on page 118

Rules for creating LUNs

To avoid problems creating LUNs when using SnapDrive, you must keep some rules in mind.

- Create LUN names using US-ASCII characters only, even when you are using non-ASCII operating systems.
- If you are adding the LUN to a Windows Server 2003 or 2008 cluster, make sure to create the LUN on the node that owns the cluster group in which you are creating a new physical disk resource.

Note: Shared disks on Windows Server 2003 cluster nodes that do not own the disks often display as unknown and unreadable, and as offline on Windows 2008, in MMC Disk Management utility; however, the disks will continue to function normally on all nodes in the cluster.

- To ensure that Snapshot copies can be made, follow these guidelines:
 - Do not attempt to create a LUN on a storage system volume that holds anything other than LUNs.
 - Conversely, do not put anything other than LUNs on a storage system volume that contains LUNs.
 - All LUNs in the same storage system volume should be created using SnapDrive or, if they were created outside of SnapDrive, prepared for management in SnapDrive.

About volume mount points

Volume mount points enable you to surpass the 26-drive-letter limitation.

A *volume mount point* is a drive or volume in Windows that is mounted to a folder that uses NTFS. A mounted drive is assigned a drive path instead of a drive letter.

SnapDrive supports the creation of up to 128 LUNs. By using volume mount points, you can graft, or mount, a target partition into a folder on another physical disk. After you create a volume mount point in SnapDrive, the volume mount point drive path or label displays in Microsoft MMC **Disk Management** pane, as well as in SnapDrive MMC **Disk List** pane. For more information about volume mount points, see Microsoft article 280297 and 205524.

Volume mount point limitations

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

- The mounted volume must be of the same type as its root; that is, if the root volume is a shared cluster resource, the mounted volume must also be shared, and if the root volume is dedicated, the mounted volume must also be dedicated.
- You cannot create mount points to the quorum disk.
- If you have a mount point from one shared disk to another, SnapDrive will verify that they are in the same cluster group and that the mounted disk resource is dependent on the root disk source.

Creating a dedicated LUN

You can use SnapDrive to create dedicated FC-accessed or iSCSI-accessed LUNs.

Before you begin

- Create the dedicated volumes to hold your LUNs on the storage system.
- Verify that the FC or iSCSI services have been started on the storage system.
- Before creating a LUN in a VMware guest OS and when using VMotion, you must manually create initiator groups either by using System Manager, FilerView, or at the storage system console.

About this task

Keep the following considerations in mind when creating a LUN:

- Unless the LUN is shared within a Windows cluster, the LUN must not be connected to more than one host.
- LUNs should be created using SnapDrive.

- SnapDrive filters volumes, qtrees, and LUNs depending on storage system access control settings that might exist in the `AccessControl.xml` file on your storage system. During LUN creation, SnapDrive displays the message "Checking access control" to indicate it is checking these access control settings.
- ALUA is supported on ESX 4 and later.
When you create a disk on an ESX 4 virtual machine with FC initiators and you choose **Automatic igroup management** to map the disk to the storage system, ALUA is enabled by default on the igroup.

Steps

1. Perform the following actions to launch the **Create Disk Wizard**:
 - a. Select the SnapDrive instance for which you want to create a disk.
 - b. Select **Disks**.
 - c. From the menu choices at the top of MMC, navigate to **Action > Create Disk**.

The **Create Disk Wizard** is launched.
2. In the **Create Disk Wizard**, click **Next**.
The **Provide Storage System Name, LUN Path and Name** panel is displayed.
3. In the **Provide a Storage System Name, LUN Path and Name** panel, perform the following actions:
 - a. In the "Storage System Name" field, type the storage system name where the LUN will be created or select an existing storage system using the pull-down menu.
 - b. In the "LUN Path" field, type the LUN path or select the path on the storage system you added in Step a.
 - c. In the "LUN Name" field, enter a name for the LUN and click **Next**.

The **Select a LUN Type** panel is displayed.
4. In the **Select a LUN Type** panel, select **Dedicated**, and then click **Next**.
5. In the **Select LUN Properties** panel, either select a drive letter from the list of available drive letters or type a volume mount point for the LUN you are creating. When you create a volume mount point, type the drive path that the mounted drive will use: for example, `G:\mount_drive1\`.

Note: The root of the volume mount point must be owned by the node on which you are creating the new disk.

Note: You can create cascading volume mount points (one mount point mounted on another mount point); however, in the case of a cascading mount point created on an MSCS shared disk, you might receive a system event warning indicating that disk dependencies might not be

correctly set. This is not the case, however, as SnapDrive will create the dependencies and the mounted disks will function as expected.

6. While still in the Select LUN Properties panel, complete the following actions:

- a. Click **Limit** or **Do not limit** for the option labeled “Do you want to limit the maximum disk size to accommodate at least one snapshot?”

If you keep the default, **Limit**, which is the recommended option, the disk size limits displayed are accurate only when they first appear on the Select LUN Properties panel. When this option is selected, the following actions might interfere with the creation of at least one Snapshot copy:

- Changing the option to **Do not limit** and using SnapDrive to create an additional LUN in the same storage system volume.
- Creating a LUN in the same storage system volume without using SnapDrive
- Storing data objects other than LUNs on this storage system volume.

- b. Select a LUN size, which must fall within the minimum and maximum values displayed in the panel.

- c. Click **Next**.

If the settings on the storage system volume or qtree on which you are creating the LUN do not allow SnapDrive to proceed with the create operation, the Important Properties of the Storage System Volume panel is displayed, as described in Step 7. Otherwise, Step 7 is skipped.

7. The **Important Properties of the Storage System Volume** panel displays the settings that will be used for the volume or qtree you specified in Step 4 of this procedure.

SnapDrive requires the storage system volume containing LUNs to have the following properties:

- create_ucode = on
- convert_ucode = on
- snapshot_schedule = off

Note: SnapDrive cannot proceed to create a LUN unless these settings are configured as shown. Therefore, you must accept these settings.

Note: The create_ucode and convert_ucode volume options are no longer used, but they are set to maintain backwards compatibility with older versions of SnapDrive.

Click **Next**.

The **Select Initiators** panel is displayed.

8. In the Initiator List pane, select an initiator for the LUN you are creating.

If you select an iSCSI initiator, and an iSCSI connection to the storage system on which you are creating the LUN does not exist, SnapDrive launches the Create iSCSI Session wizard, and you are prompted to select a target portal and initiator. Also, if your target requires authentication of hosts that connect to it, you can type that information here. After you click OK, the iSCSI

connection from the Windows host to the storage system is established, even if you do not complete the Create Disk wizard.

If you have MPIO installed and you are using iSCSI and FC, you have the option to select an iSCSI initiator and several FC initiators.

9. Click **Next**.

The **Select Initiator Group Management** panel is displayed.

10. In the **Select Initiator Group Management** panel, specify whether you will use automatic or manual igroup management. If you select automatic igroup management, SnapDrive uses existing igroups or, when necessary, creates new igroups for the initiator you specified in Step 8. If you select manual igroup management, you manually choose existing igroups or create new ones as needed.

If you specify...	Then...
Automatic igroup management	Click Next . SnapDrive uses existing igroups, one igroup per initiator, or, when necessary, creates new igroups for the initiators you specified in Step 8.
Manual igroup management	Click next, and then perform the following actions: a. In the Select Initiator Groups panel, select from the list the igroups to which you want the new LUN to belong. Note: A LUN can be mapped to an initiator only once. OR Click Manage Igroups and for each new igroup you want to create, type a name in the Igroup Name text box, select initiators, click Create, and then click Finish to return to the Select Initiator Groups panel. Note: b. Click Next. Note: The Next button will remain unavailable until the collection of selected igroups contains all the initiators you selected in Step 8.

You are done with igroup management.

11. In the **Completing the Create Disk Wizard** panel, perform the following actions:

- a. Verify all the settings.

If you need to change any settings, click **Back** to go back to the previous Wizard panels.

- b. Click **Finish**.

Disk creation might take several seconds to complete. SnapDrive displays disk creation status in the lower panel of the center MMC pane.

Related tasks

[Creating an RDM LUN on a guest OS](#) on page 114

[Stopping and starting the SnapDrive service](#) on page 85

[Managing LUNs not created in SnapDrive](#) on page 133

Creating a shared LUN

You can use SnapDrive to create FC- or iSCSI-accessed LUNs that are shared between clustered Windows servers.

Before you begin

- Verify that the FC or iSCSI services have been started on the storage system.

About this task

Keep the following consideration in mind when creating a LUN:

- LUNs should be created using SnapDrive.
- SnapDrive filters volumes, qtrees, and LUNs depending on storage system access control settings that might exist in the AccessControl.xml file on your storage system. During LUN creation, SnapDrive displays the message "Checking access control" to indicate it is checking these access control settings.

Steps

1. Perform the following actions to launch the Create Disk wizard:
 - a. Select the SnapDrive instance for which you want to create a disk.
 - b. Select Disks.
 - c. From the menu choices at the top of MMC, navigate to **Action > Create Disk**.

The **Create Disk Wizard** is launched.

2. In the **Create Disk Wizard**, click **Next**.

The Provide Storage System Name, LUN Path and Name panel is displayed.

3. In the **Provide a Storage System Name, LUN Path and Name** panel, perform the following actions:
 - a. In the "Storage System Name" field, type the storage system name where the LUN will be created or select an existing storage system using the pull-down menu.
 - b. In the "LUN Path" field, type the LUN path or select the path on the storage system you added in Step a.
 - c. In the "LUN Name" field, enter a name for the LUN and click **Next**.

The **Select a LUN Type** panel is displayed.

4. In the **Select a LUN Type** panel, select **Shared**, and then click **Next**.
5. In the “Information About the Microsoft Cluster Services System” panel, verify that you want the disk to be shared by the nodes listed, and then click **Next**.

The **Specify Microsoft Cluster Services Group** panel is displayed.

6. In the **Specify Microsoft Cluster Services Group** panel, perform ONE of the following actions and then click **Next**.
 - Select a cluster group from the Group Name drop-down list.
 - Select **Create a new cluster group** to create a new cluster group.

Note: When selecting a cluster group for your LUNs, choose the cluster group your application will use. If you are creating a volume mount point, the cluster group is already selected. This is because the cluster group owns your root volume physical disk cluster resources. It is recommended that you create new shared LUNs outside of the cluster group.
 - Select **Add to cluster shared volumes**.
7. In the **Select LUN Properties** panel, either select a drive letter from the list of available drive letters or enter a volume mount point for the LUN you are creating. When you create a volume mount point, enter the drive path that the mounted drive will use: for example, G:\mount_drive1\.

Note: The root of the volume mount point must be owned by the node on which you are creating the new disk.

Note: You can create cascading volume mount points (one mount point mounted on another mount point); however, in the case of a cascading mount point created on an MSCS shared disk, you might receive a system event warning indicating that disk dependencies might not be correctly set. This is not the case, however, as SnapDrive will create the dependencies and the mounted disks will function as expected.

8. While still in the **Select LUN Properties** panel, complete the following actions:
 - a. Click **Limit** or **Do not limit** for the option labeled “Do you want to limit the maximum disk size to accommodate at least one snapshot?”

If you select **Limit**, the disk size limits displayed are accurate only when they first appear on the **Select LUN Properties** panel. When this option is selected, the following actions might interfere with the creation of at least one Snapshot copy:

- The option is changed to **Do not limit** and SnapDrive is used to create an additional LUN in the same storage system volume.
 - A LUN is created in the same storage system volume without using SnapDrive
 - Data objects other than LUNs are stored on this storage system volume.
- b. Select a LUN size. The size must fall within the minimum and maximum values displayed in the panel.

c. Click **Next**.

If the settings on the storage system volume or qtree on which you are creating the LUN do not allow SnapDrive to proceed with the create operation, the **Important Properties of the Storage System Volume** panel is displayed, as described in Step 8. Otherwise, Step 8 is skipped.

9. The **Important Properties of the Storage System Volume** panel displays the settings that will be used for the volume or qtree you specified earlier in this procedure.

SnapDrive requires the storage system volume containing LUNs to have the following properties:

- create_unicode = on
- convert_unicode = on
- snapshot_schedule = off

Note: SnapDrive cannot proceed to create a LUN unless these settings are configured as shown. Therefore, you must accept these settings.

Note: The create_unicode and convert_unicode volume options are no longer used, but they are set to maintain backwards compatibility with older versions of SnapDrive.

10. Click **Next**.

11. In the **Select Initiators** panel, perform the following actions:

- a. Double-click the cluster group name to display the hosts that belong to the cluster.
- b. Click the name of a host to select it.

The available initiators for that host are displayed in the Initiator List in the lower half of the pane.

12. In the Initiator List pane, select an initiator for the LUN you are creating.

If you select an iSCSI initiator, and an iSCSI connection to the storage system on which you are creating the LUN does not exist, SnapDrive launches the Create iSCSI Session wizard, and you are prompted to select a target portal and initiator. Also, if your target requires authentication of hosts that connect to it, you can type that information here. After you click OK, the iSCSI connection from the Windows host to the storage system is established, even if you do not complete the Create Disk wizard.

If you have MPIO installed and you are using FC, you have the option to select several FC initiators.

13. Repeat Step 10 and Step 11 for all hosts, and then click **Next**.

Note: The **Next** button remains unavailable until initiators for all hosts of a cluster have been selected.

The **Select Initiator Group management** panel is displayed.

14. In the **Select Initiator Group management** panel, specify whether you will use automatic or manual igroup management. If you select automatic igroup management, SnapDrive uses existing igroups or, when necessary, creates new igroups for the initiators you specified in Step 10

through Step 12. If you select manual igroup management, you manually choose existing igroups or create new ones as needed.

If you specify...	Then...
Automatic igroup management	Click Next . You are done with igroup management.
Manual igroup management	Click Next , and then perform the following actions: a. In the Select igroups panel, select from the list the igroups to which you want the new LUN to belong. Repeat this action for each node in the cluster. Note: A LUN can be mapped to an initiator only once. OR Click Manage igroups and for each new igroup you want to create, type a name in the igroup Name text box, select initiators, click Create , and then click Finish to return to the Select igroups panel. b. Click Next . Note: The Next button will remain unavailable until the collection of selected igroups contains all the initiators you selected in Step 11.

The **Completing the Create Disk Wizard** panel is displayed.

15. In the **Completing the Create Disk Wizard** panel, perform the following actions:

a. Verify all the settings.

If you need to change any settings, click **Back** to go back to the previous wizard panels.

b. Click **Finish**.

Disk creation might take several seconds to complete. SnapDrive displays disk creation status in the lower panel of the center MMC pane.

Related tasks

Preparing storage systems for SnapDrive on page 64

Managing LUNs not created in SnapDrive on page 133

Creating a LUN as a quorum on a Windows 2003 cluster

You can use SnapDrive to create and configure a LUN as a cluster quorum disk on a new Windows Server 2003 cluster.

Before you begin

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

- You have up to eight host machines with Windows Server 2003 Standard Edition or Enterprise Edition installed. For more information about installing the Windows Server 2003 software, see your Microsoft documentation.
- Your storage system is running at least Data ONTAP 7.1.
- Make sure that the following are installed on all nodes of the cluster:
 - Appropriate FC HBA drivers, WHQL signed iSCSI HBA drivers, or the Microsoft iSCSI Software Initiator drivers
 - Either the FC or iSCSI Host Utilities, depending on your configuration
 - SnapDrive for Windows
- If you are using the Microsoft iSCSI software, establish iSCSI connections to the storage system from all nodes of the cluster using each node's MMC.
- Because this LUN will be designated as a quorum disk later in this procedure, you must create a disk of adequate size according to Microsoft's recommendations.

Steps

1. Create a shared LUN on node 1 and note the path and drive letter you assign to the LUN.
2. On node 1, launch the **Windows Server 2003 Cluster Administrator**.

If the Cluster Administrator is launched...	Then...
For the first time on this node, you are prompted to specify the action to take.	Select Create New Cluster from the Action drop-down list.
Subsequently, it does not prompt you to specify the action to take.	In that case, select File > New > Cluster from the Cluster Administrator .

The **New Server Cluster Wizard** is displayed.

3. In the **New Server Cluster Wizard**, follow the prompts to type the following information:
 - Windows domain name and cluster name
 - The node that will be the first node in the cluster
The node you are working on currently should be the selected node in the wizard.

- IP address for the server cluster
- User name and password for the cluster service account

Note: Note the user name and password you enter; you need it in a later step in this procedure.

After you have entered the above information in the New Server Cluster wizard windows, the **Proposed Cluster Configuration** panel is displayed.

4. In the **Proposed Cluster Configuration** panel, do one of the following:

If...	Then...
The LUN you created in Step 1 is automatically selected as the quorum disk	Go to Step 5.
The LUN you created in Step 1 is not selected as the quorum disk	• Click the quorum button. • Change the drive letter to that of the LUN and click Next.

5. Step through the remaining panels of the **New Server Cluster Wizard**.

After you finish using the **New Server Cluster Wizard**, the first node in the cluster is up and functional.

6. Go to the Windows host that will be the next node in the cluster and, from SnapDrive, connect to the LUN you created in Step 1 from this node, using the path and drive letter you noted in Step 1.

Note: The Shared disk option is automatically selected.

SnapDrive prompts you for the cluster name.

7. Enter the cluster name you created in Step 3. Click **OK**.
8. Launch the **Windows Server 2003 Cluster Administrator** and perform the following actions:
- Select File > Open Connection.**
 - Select **Add Nodes to Cluster**.
 - Type the name of the cluster (as in Step 3)
 - Click **Next**.

The Add Nodes wizard is displayed with the name of the node on which you are currently working.

9. In the Add Nodes wizard, follow the prompts to perform the following tasks in the wizard panels:
- If the name of the node on which you are working currently is not displayed, type the name of the node or click **Browse** to find the node. Then click **Add** to add the node to the list.
 - Select **Advanced > Advanced (minimum) Configuration**.

- c. Enter the password for the cluster service account.

Note: This password should be the same as the one you entered in Step 3.

After you enter the information, the **Proposed Cluster Configuration** panel is displayed.

10. In the **Proposed Cluster Configuration** panel, do one of the following:

If the proposed cluster configuration ...	Then...
Requires no changes	Follow the Add Nodes wizard prompts to complete the remaining steps of the wizard.
Requires changes	Make the appropriate changes, and then follow the Add Nodes wizard prompts to complete the remaining steps of the wizard.

The node is added to the cluster.

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

Note: You should perform the “move group” operation for all nodes in the cluster to ensure proper operation.

If...	Then...
The node you added to the cluster was the last node	You are done.
The node you added to the cluster was not the last node	Go to Step 6.

Result

You have added the desired number of nodes to a Windows Server 2003 cluster. The server cluster is up and operational. Now you can create shared disks for your applications.

Note: Microsoft recommends that you not add new shared resources to Cluster Group once it has been created. If you add resources to the group, you may not be able to administer the cluster effectively. For more information, see Microsoft knowledge base article 168948.

Related tasks

[Establishing an iSCSI session to a target](#) on page 96

[Creating a shared LUN](#) on page 106

[Connecting to a LUN](#) on page 122

Windows Server 2008 failover cluster support

SnapDrive supports the use of shared LUNs in a Windows Server 2008 failover cluster for all cluster configuration models using up to eight nodes.

Note: Enumeration and management of offline disk resources is not supported in a failover cluster.

For more information about failover clusters and cluster configuration models, see the Windows Server 2008 documentation and online Help.

Related tasks

[Creating a shared LUN](#) on page 106

Related information

[The Microsoft Windows Server 2008 Technical Library- technet2.microsoft.com/windowsserver2008/en/library](http://technet2.microsoft.com/windowsserver2008/en/library)

Configuring a Windows Server 2008 failover cluster witness disk

SnapDrive for Windows and Windows Server 2008 provides a simpler way of configuring a shared disk as a witness disk than in earlier versions of SnapDrive and Windows Server. While SnapDrive still supports the previous method of configuring a quorum, it is no longer necessary to create a shared disk before creating a cluster, nor is it necessary to connect that shared disk to the node before that node can be added to the cluster.

Before you begin

- Install the Windows Server 2008 failover cluster feature.
For more information, see Windows Server 2008 online Help.
- Create the failover cluster using Windows Server 2008 MMC snap-in, Failover Cluster Management.
For more information, see Windows Server 2008 online Help.
- Create a shared LUN, ensuring that you select the Microsoft Cluster Services Group named "Cluster Group" to own that disk resource.

Note: The shared LUN must be created on the node that owns "Cluster Group." To determine which node owns "Cluster Group," type the `cluster group` command at a Windows command prompt.

Steps

1. Navigating to **Start > Administrative Tools > Failover Cluster Management** to launch the Windows Server 2008 Failover Cluster Management snap-in.
2. Click the name of the failover cluster for which you want to configure the witness disk.
3. From the menu choices at the top of the snap-in, navigate to **Action > More Actions > Configure Cluster Quorum Settings**
The **Configure Cluster Quorum Wizard** is launched.
4. In the **Configure Cluster Quorum Wizard**, click **Next**.
The **Select Quorum Configuration** panel is displayed.
5. In the **Select Quorum Configuration** panel, select Node and Disk Majority, and then click **Next**.
The **Configure Storage Witness** panel is displayed.
6. In the **Configure Storage Witness** panel, select the shared LUN you created in SnapDrive to be the witness disk, and then click **Next**.
The **Confirmation** panel is displayed.
7. In the **Confirmation** panel, click **Next** to configure the cluster quorum settings.
The quorum settings are configured and the **Summary** panel is displayed.
8. In the **Summary** panel, click **Finish** to close the wizard.

Related tasks

[Creating a shared LUN](#) on page 106

Creating an RDM LUN on a guest OS

You can use SnapDrive to create FC, iSCSI, or ESX iSCSI accessed RDM LUNs on a guest OS.

Before you begin

- Create the dedicated volumes to hold your LUNs on the storage system.
- Verify that the FC or iSCSI service has been started on the storage system.
- Before creating a LUN in a VMware guest OS, you must manually create initiator groups by using System Manager, FilerView, or at the storage system console.
When you create a shared FC or iSCSI RDM LUN, you must choose an initiator from each ESX server to create a single initiator group automatically using SnapDrive.

Steps

1. Perform the following actions to launch the Create Disk wizard:

- a. Select the SnapDrive instance for which you want to create a disk.
- b. Select Disks.
- c. From the menu choices at the top of MMC, navigate to **Action > Create Disk**.

The **Create Disk Wizard** is launched.

2. In the **Create Disk Wizard**, click **Next**.

The **Provide Storage System Name, LUN Path and Name** panel is displayed.

3. In the **Provide a Storage System Name, LUN Path and Name** panel, perform the following actions:
 - a. In the “Storage System Name” field, type the storage system name where the LUN will be created or select an existing storage system using the pull-down menu.
 - b. In the “LUN Path” field, type the LUN path or select the path on the storage system you added in Step a.
 - c. In the “LUN Name” field, enter a name for the LUN and click **Next**.

The **Select a LUN Type** panel is displayed.

4. In the **Select a LUN Type** panel, select **Dedicated**, and then click **Next**.
5. In the **Select LUN Properties** panel, either select a drive letter from the list of available drive letters or type a volume mount point for the LUN you are creating. When you create a volume mount point, type the drive path that the mounted drive will use: for example, G:\mount_drive1\.

Note: The root of the volume mount point must be owned by the node on which you are creating the new disk.

Note: You can create cascading volume mount points (one mount point mounted on another mount point); however, in the case of a cascading mount point created on an MSCS shared disk, you might receive a system event warning indicating that disk dependencies might not be correctly set. This is not the case, however, as SnapDrive will create the dependencies and the mounted disks will function as expected.

6. While still in the **Select LUN Properties** panel, complete the following actions:
 - a. Click **Limit** or **Do not limit** for the option labeled “Do you want to limit the maximum disk size to accommodate at least one snapshot?”

If you keep the default, **Limit**, which is the recommended option, the disk size limits displayed are accurate only when they first appear on the **Select LUN Properties** panel. When this option is selected, the following actions might interfere with the creation of at least one Snapshot copy:

- Changing the option to **Do not limit** and using SnapDrive to create an additional LUN in the same storage system volume

- Creating a LUN in the same storage system volume without using SnapDrive
 - Storing data objects other than LUNs on this storage system volume
- b. Select a LUN size, which must fall within the minimum and maximum values displayed in the panel.
- c. Click **Next**.

If the settings on the storage system volume or qtree on which you are creating the LUN do not allow SnapDrive to proceed with the create operation, the Important Properties of the Storage System Volume panel is displayed, as described in Step 7. Otherwise, Step 7 is skipped.

7. The **Important Properties of the Storage System Volume** panel displays the settings that will be used for the volume or qtree you specified in Step 4 of this procedure.

SnapDrive requires the storage system volume containing LUNs to have the following properties:

- create_ucose = on
- convert_ucose = on
- snapshot_schedule = off

Note: SnapDrive cannot proceed to create a LUN unless these settings are configured as shown. Therefore, you must accept these settings.

Note: The create_ucose and convert_ucose volume options are no longer used, but they are set to maintain backwards compatibility with older versions of SnapDrive.

Click **Next**.

The **Select Initiators** panel is displayed.

8. In the Initiator List pane, select an initiator for the LUN you are creating.

If you have MPIO installed, you have the option to select several FC initiators.

Note: You cannot select both iSCSI and FC initiators when creating a LUN on a guest OS.

9. Click **Next**.

The **Select Initiator Group Management** panel is displayed.

10. In the **Select Initiator Group Management** panel, specify whether you will use automatic or manual igroup management. If you select automatic igroup management, SnapDrive uses existing igroups or, when necessary, creates new igroups for the initiator you specified in Step 8. If you select manual igroup management, you manually choose existing igroups or create new ones as needed.

If you specify...	Then...
Automatic igroup management	Click Next. SnapDrive uses existing igroups, one igroup per initiator, or, when necessary, creates new igroups for the initiators you specified in Step 8.

If you specify...	Then...
Manual igroup management	Click next, and then perform the following actions: a. In the Select Initiator Groups panel, select from the list the igroups to which you want the new LUN to belong. Note: A LUN can be mapped to an initiator only once. OR Click Manage Igroups and for each new igroup you want to create, type a name in the Igroup Name text box, select initiators, click Create, and then click Finish to return to the Select Initiator Groups panel. b. Click Next. Note: The Next button will remain unavailable until the collection of selected igroups contains all the initiators you selected in Step 8.

You are done with igroup management.

11. In the **Select a Datastore** panel, perform the following steps.

If your virtual machine resides on a...	Then...
VMFS datastore	a. Choose either Store with Virtual Machine, which is the default, or choose Specify datastore to select a different VMFS datastore for your virtual machine disk format (VMDK) file to reside. b. Click Next.
NFS datastore	a. Choose Specify datastore to select a different VMFS datastore for your VMDK file to reside. The Store with Virtual Machine option is unavailable because a VMDK file cannot be stored on an NFS datastore. b. Click Next.

12. In the **Completing the Create Disk Wizard** panel, perform the following actions:

- a.** Verify all the settings.
- If you need to change any settings, click **Back** to go back to the previous Wizard panels.
- b.** Click **Finish**.
- Disk creation might take several seconds to complete. SnapDrive displays disk creation status in the lower panel of the center MMC pane.

Creating a highly available Hyper-V virtual machine using SnapDrive

You can make a Hyper-V virtual machine highly available by creating the VM on a SnapDrive shared LUN in a Windows 2008 failover cluster.

Before you begin

- Install the Windows Server 2008 failover cluster feature.
For more information, see Windows Server 2008 online Help.
- Create a shared LUN, ensuring that you select the Microsoft Cluster Services Group named "Available Storage" to own that disk resource.

Note: The shared LUN must be created on the node that owns "Available Storage." To determine which node owns "Available Storage," type the `cluster group` command at a Windows command prompt.

Steps

1. Open Hyper-V Manager and use Virtual Network Manager to create and configure your virtual networks on all physical hosts.
2. From the Actions menu, click Virtual Network Manager to create or add a virtual network.

See your Hyper-V documentation for more information.

Note: All nodes in the same cluster must use the same name for the virtual network that provides external networking for the virtual machines. The virtual network adapters must be named the same on all Hyper-V hosts to enable quick migration.

3. From the Hyper-V Manager Action menu, click **New > Virtual Machine**.
4. In the Virtual Machine wizard, choose the option to store the virtual machine in a new folder and specify the location of your shared storage.
5. Navigate to **Start > Administrative Tools > Failover Cluster Management** to launch the Windows Server 2008 Failover Cluster Management snap-in.

Note: Make sure the virtual machine is not running before you make it highly available.

6. Using the High Availability Wizard, navigate to **Failover Cluster > Services and Applications > Configure a Server or Application** and select the virtual machine you created in Steps 1 through 3 to add it to a cluster group.

You have created a virtual machine cluster group.

7. Use SnapDrive to create additional shared disks as virtual machines to add to your virtual machine cluster group.

Managing LUNs

SnapDrive for Windows enables you to manage LUNs from a Windows environment.

Next topics

[*Guidelines for connecting LUNs*](#) on page 121

[*Connecting to a LUN*](#) on page 122

[*Guideline for managing RDM LUNs not created in SnapDrive*](#) on page 124

[*Connecting to an RDM LUN on a guest OS*](#) on page 124

[*Making drive letter or path modifications to a LUN*](#) on page 127

[*Guidelines for disconnecting or deleting LUNs*](#) on page 128

[*Disconnecting a LUN*](#) on page 129

[*Deleting a LUN*](#) on page 130

[*Deleting folders within volume mount points*](#) on page 131

[*Guidelines for resizing disks*](#) on page 131

[*Resizing a disk*](#) on page 132

[*Resizing a quorum disk*](#) on page 133

[*Managing LUNs not created in SnapDrive*](#) on page 133

Guidelines for connecting LUNs

Properly connecting a LUN in SnapDrive for Windows enables you to save, delete, modify, and manage the files it contains from the Windows host. You can also make Snapshot copies of the entire disk and restore the disk, along with its contents, to the state captured by a previous Snapshot copy.

- LUNs should be created using SnapDrive. If you want to connect a LUN that was not created in SnapDrive, you will need to take some steps to prepare the LUNs for SnapDrive management.
- Unless the LUN is shared within a Windows cluster, the LUN must not be connected to more than one host.

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

Connecting to a LUN

You can connect your SnapDrive for Windows host to a LUN using the Connect Disk wizard in the SnapDrive MMC snap-in.

Before you begin

Before connecting a LUN in a VMware Guest OS, you must manually create initiator groups by using System Manager, FilerView, or from the storage system console.

About this task

SnapDrive filters volumes, qtrees, and LUNs depending on storage system access control settings that might exist in the AccessControl.xml file on your storage system. During LUN connection, SnapDrive displays the message "Checking access control" to indicate it is checking these access control settings.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage. Then, select **Disks**.
2. From the menu choices at the top of MMC, navigate to **Action > Connect Disk**.
3. In the Connect Disk wizard, click **Next**.
4. In the **Provide a Storage System Name, LUN Path and Name** panel, perform the following actions:
 - a. In the "Storage System Name" field, type the name of the storage system where the LUN will be connected, or choose a storage system from the drop-down list.
 - b. In the "LUN Path" field, type the path to the LUN. Alternatively, click Browse and navigate to the LUN you want to connect.
 - c. Click **Next**.
5. If the LUN is a dedicated disk, go to the next step; otherwise, if the LUN is a Windows cluster resource, perform the following steps in the **Specify Microsoft Cluster Services Group** panel.
6. In the **Specify Microsoft Cluster Services Group** panel, perform ONE of the following actions and then click **Next**.
 - Select a cluster group from the Group Name drop-down list.
 - Select **Create a new cluster group** to create a new cluster group.

Note: When selecting a cluster group for your LUNs, choose the cluster group your application will use. If you are connecting to a volume mount point, the cluster group is already selected. This is because the cluster group owns your root volume physical disk

cluster resources. It is recommended that you create new shared LUNs outside of the cluster group.

- Select **Add to cluster shared volumes**.

7. In the **Select LUN Properties** panel, perform the following actions:

- Either select a drive from the list of available drive letters, or enter a mount point for the LUN you are connecting. When you connect a volume mount point, enter the drive path that the mounted drive will use: for example, `G:\mount_drive1\`.

Note: The root volume of a new mount point must be owned by the node on which you are creating the new disk.

Note: You can connect cascading volume mount points (by mounting one mount point on another mount point); however, in the case of a cascading mount point connected on a MSCS shared disk, you might receive a system event warning indicating that disk dependencies might not be correctly set. This is not the case, however, and the mounted disks will function as expected.

- Click **Next**.

8. In the **Select Initiators** panel, choose an initiator for the LUN.

Note: If MPIO is installed on the system, you can select multiple FC initiator ports or one iSCSI session.

If the LUN...	Then...
Will belong to a single system	Select at least one initiator for the LUN you are creating from the list of available initiators, and then click Next .
Will be a Windows cluster resource	- Double-click the cluster name to display the hosts that belong to the cluster. - Click the name of a host to select it. - Select at least one initiator for the LUN you are creating from the list of available initiators on that host. - Repeat steps b and c for all hosts in the cluster. - Click Next. Note: The Next button remains unavailable until initiators for all hosts of a cluster are selected.

9. In the **Select Initiator Group Management** panel, specify whether you will use automatic or manual igroup management.

If you select automatic igroup management, SnapDrive uses existing igroups or, when necessary, creates new igroups for the initiators you've specified. If you select manual igroup management, you manually choose existing igroups or create new ones as needed.

If you specify...	Then...
Automatic igroup management	Select Automatic , and then click Next .
Manual igroup management	Select Manual, click Next, and then, in the Select Initiator Groups panel, perform ONE of the following actions: - Select from the list the igroups to which you want the LUN to belong. Repeat this action for each node in the cluster, then click Next. Note: A LUN can be mapped to an initiator only once. - Click Manage igroups, and for each new igroup you want to create, type a name in the Igroup Name text box, select initiators, and click Create. Then, click Finish to return to the Select Initiator Groups panel, and click Next. Note: The Next button in the Select Initiator Groups panel remains unavailable until the collection of selected igroups contains all the initiators you previously selected for use.

10. In the **Completing the Connect Disk Wizard** panel, perform the following actions:

- a. Verify all the settings.
- b. If you need to change any settings, click **Back** to go back to the previous wizard panels.
- c. Click **Finish**.

The newly connected LUN now appears under **SnapDrive > Disks** in the left MMC panel.

Guideline for managing RDM LUNs not created in SnapDrive

When you create an RDM LUN outside of SnapDrive, you must restart the SnapDrive for Windows service to enable SnapDrive to properly recognize the newly created disk. For the best results, use SnapDrive to create RDM LUNs.

Connecting to an RDM LUN on a guest OS

You can connect your SnapDrive for Windows host to an RDM LUN on a guest OS using the Connect Disk wizard in the SnapDrive MMC snap-in.

Before you begin

Before connecting a LUN in a VMware guest OS, you must manually create initiator groups by using either System Manager or FilerView, or at the storage system console.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage. Then, select **Disks**.
2. From the menu choices at the top of MMC, navigate to **Action > Connect Disk**.
3. In the Connect Disk wizard, click **Next**.
4. In the **Provide a Storage System Name, LUN Path and Name** panel, perform the following actions:
 - a. In the “Storage System Name” field, type the name of the storage system where the LUN will be connected, or choose a storage system from the drop-down list.
 - b. In the “LUN Path” field, type the path to the LUN. Alternatively, click Browse and navigate to the LUN you want to connect.
 - c. Click **Next**.
5. In the **Select a LUN Type** panel, select **Dedicated**, and then click **Next**.
6. In the **Select LUN Properties** panel, perform the following actions:
 - a. Either select a drive from the list of available drive letters, or enter a mount point for the LUN you are connecting. When you create a volume mount point, enter the drive path that the mounted drive will use: for example, G:\mount_drive1\.

Note: The root volume of a new mount point must be owned by the node on which you are connecting the new disk.

 - b. Click **Next**.
7. In the **Select Initiators** panel, choose at least one initiator for the LUN to which you are connecting from the list of available initiators, and then click **Next**.

Note: If MPIO is installed on the system, you can select multiple FC initiator ports. You cannot select both iSCSI and FC initiators when creating a LUN on a guest OS.
8. In the **Select Initiator Group Management** panel, specify whether you will use automatic or manual igroup management.

If you select automatic igroup management, SnapDrive uses existing igroups or, when necessary, creates new igroups for the initiators you have specified. If you select manual igroup management, you manually choose existing igroups or create new ones as needed.

If you specify...	Then...
Automatic igroup management	Select Automatic , and then click Next .

If you specify...	Then...
Manual igroup management	Select Manual, click Next, and then, in the Select Initiator Groups panel, perform ONE of the following actions: • Select from the list the igroups to which you want the LUN to belong, then click Next. Note: A LUN can be mapped to an initiator only once. • Click Manage igroups, and for each new igroup you want to create, type a name in the Igroup Name text box, select initiators, and click Create. Then, click Finish to return to the Select Initiator Groups panel, and click Next. Note: The Next button in the Select Initiator Groups panel remains unavailable until the collection of selected igroups contains all the initiators you previously selected for use.

9. If you selected an FC initiator on an ESX server in the **Select Initiator Group Management** panel, then the **Select a Datastore** panel is displayed.

If your virtual machine resides on a...	Then...
VMFS datastore	a. Choose either Store with Virtual Machine, which is the default, or choose Specify datastore to select a different VMFS datastore for your virtual machine disk format (VMDK) file to reside. b. Click Next.
NFS datastore	a. Choose Specify datastore to select a different VMFS datastore for your VMDK file to reside. The Store with Virtual Machine option is unavailable because a VMDK file cannot be stored on an NFS datastore. b. Click Next.

10. In the **Completing the Connect Disk Wizard** panel, perform the following actions:

- a. Verify all the settings.
- b. If you need to change any settings, click **Back** to go back to the previous wizard panels.
- c. Click **Finish**.

The newly connected LUN now appears under **SnapDrive > Disks** in the left MMC panel.

Making drive letter or path modifications to a LUN

SnapDrive for Windows enables you to add, change, or remove a drive letter or mount point path for an existing LUN.

Next topics

Adding, removing, or changing a drive letter or path for an existing LUN on page 127
Moving a mount point with Windows Explorer on page 128

Adding, removing, or changing a drive letter or path for an existing LUN

You can add, remove, or change a drive letter or mount point path for an existing LUN using the SnapDrive for Windows MMC snap-in.

Steps

- 1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand **Disks** and select the disk you want to manage.
- 2. From the menu choices at the top of MMC, navigate to **Action > Change Drive Letter and Paths**.
- 3. In the **Change Drive Letter and Paths** window, click either **Add**, **Remove**, or **Change**, depending on the action you want to take.

Note: The Change option is unavailable for mount points.

If...	Then...
You are removing a drive letter or path	Click OK to proceed with the operation.
You are adding or changing a drive letter or path	In the Add or Change Drive Letter or Path window, select a drive letter or enter path in the space provided, then click OK .

By removing the last volume mount point on a shared disk, SnapDrive for Windows removes the resource dependency from the root disk. If you are creating a mount point from one shared disk to another, SnapDrive verifies they are in the same cluster group and creates a dependency to the root disk resource if it is the first volume mount point to that root disk.

Note: When you create the first volume mount point to a root disk that is shared and is being used by MSCS, SnapDrive, as part of the resource dependency process, takes the physical disk resource offline, presenting the mounting volume. As a result, any other cluster resources that depend on the physical disk resource will also be taken offline. An example of this is the Exchange System Attendant cluster resource. SnapDrive automatically brings the physical disk resource back online but will not bring the Exchange resources back online. Exchange resources should be brought back online manually using the Cluster Administrator.

Moving a mount point with Windows Explorer

Complete these steps to move an existing LUN mount point using Windows Explorer.

Steps

1. Identify the folder that represents the volume mount point.
2. Using Windows Explorer, cut and paste the mount point folder to another folder on the same drive.

Note: You cannot cut and paste a volume mount point folder to a different drive.

Guidelines for disconnecting or deleting LUNs

You can disconnect a LUN from a host in SnapDrive for Windows without affecting the contents of the LUN, or you can permanently delete a LUN. You can also use SnapDrive for Windows to disconnect a LUN in a Snapshot copy or FlexClone volume.

- When the host is disconnected from a LUN, you cannot see or modify the LUN's contents, make Snapshot copies of the LUN, or use Snapshot technology to restore the LUN to a previous Snapshot copy; however, the LUN still exists on the storage system volume.
- You must make sure that the LUN you are disconnecting or deleting is not monitored with the Windows Performance Monitor (perfmon).
- Make sure that the LUN you want to disconnect or delete is not being used by a host.
- You can only disconnect or delete a shared LUN (that is, a non-quorum disk) after removing the cluster resource dependencies from the LUN and verifying that all nodes in the cluster are powered on and functioning properly.

Note: SnapDrive manages the dependencies to the root disk for volume mount points.

- When disconnecting or deleting LUNs on a Microsoft cluster, you must make sure that all hosts in the cluster are available to SnapDrive for the disconnect or delete operation to succeed.
- You can disconnect a quorum disk only after replacing it with another disk that takes over as a quorum disk for the cluster.
- Use the Delete Disk feature cautiously, because after you delete a LUN, you cannot use SnapDrive to undelete it.
- If you disconnect a LUN in a FlexClone volume that SnapDrive for Windows created and it is the last LUN connected on the volume, SnapDrive, deletes that volume resulting in the deletion of all LUNs in the FlexClone volume. SnapDrive displays a message warning you that the FlexClone volume might be deleted.

To avoid automatic deletion of the FlexClone volume, rename the volume before disconnecting the last LUN. When you rename the volume, be sure to change more than just the last integers in the name. For instance, if the FlexClone volume is named `sdw_cl_myvol_0`, rename it to `new_sdwvol_0`, and not to `sdw_cl_myvol_20`. If you rename only the last integers in the volume name, SnapDrive still recognizes that it created that volume and it will delete the volume when

you disconnect the last LUN. The renamed FlexClone volume is visible after you refresh SnapDrive MMC.

- If you unmap or delete a LUN from the storage system console, you must also remove any stale RDMs that result from unmapping or removing the LUN.

Disconnecting a LUN

You can use the SnapDrive for Windows MMC snap-in to disconnect a dedicated or shared LUN, or a LUN in a Snapshot copy or in a FlexClone volume.

Before you begin

- Make sure that neither Windows Explorer nor any other Windows application is using or displaying any file on the LUN you intend to disconnect. If any files on the LUN are in use, you will not be able to disconnect the LUN except by forcing the disconnect.
- If you are disconnecting a disk that contains volume mount points, change, move, or delete the volume mount points on the disk first before disconnecting the disk containing the mount points; otherwise, you will not be able to disconnect the root disk. For example, disconnect G: \mount_disk1\, then disconnect G: \.
- Before you decide to force a disconnect of a SnapDrive LUN, be aware of the following consequences:
 - Any cached data intended for the LUN at the time of forced disconnection is not committed to disk.
 - Any mount points associated with the LUN are also removed.
 - A pop-up message announcing that the disk has undergone "surprise removal" appears in the console session.

About this task

Under ordinary circumstances, you cannot disconnect a LUN that contains a file being used by an application such as Windows Explorer or the Windows operating system. However, you can force a disconnect to override this protection. When you force a disk to disconnect, it results in the disk being unexpectedly disconnected from the Windows host.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand **Disks** and select the disk you want to manage.
2. From the menu choices at the top of MMC, navigate to either **Action > Disconnect Disk** to disconnect normally, or **Action > Force Disconnect Disk** to force a disconnect.
3. When prompted, click **Yes** to proceed with the operation.

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

The icons representing the disconnected LUN disappear from both the left and right MMC panels.

Deleting a LUN

You can delete a LUN using the SnapDrive for Windows MMC snap-in.

Before you begin

If you are deleting a disk that contains volume mount points, disconnect the mounted volumes on the disk first before deleting the disk. For example, disconnect G:\mount_disk1\, then disconnect G:\. If you do not disconnect the mounted volume before you delete it, Windows keeps the volume mount point information in the Recycle Bin and both Windows and SnapDrive continue to see the mount point as valid. If your volume mount point contains data, remember that SnapDrive will not warn you that data is present when you delete the mount point.

About this task

Use the Delete Disk feature cautiously, because after you delete a LUN, you cannot use SnapDrive to undelete it.

Steps

1. Make sure that neither Windows Explorer nor any other Windows application is using or displaying any file on the LUN you intend to delete.
2. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand **Disks** and select the disk you want to manage.
3. From the menu choices at the top of MMC, navigate to **Action > Delete Disk**.
4. When prompted, click **Yes** to proceed with the operation.

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

The icons representing the deleted LUN disappear from MMC.

Deleting folders within volume mount points

You can delete a folder within a volume mount point by bypassing the Windows Recycle Bin.

About this task

When you use the Windows Explorer to delete a folder that you have created under a volume mount point, you might receive an error message similar to the following, where *Foldername* is the name of the folder you want to delete:

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

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

For more information about deleting folders within volume mount points, see Microsoft article 243514.

Steps

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

Guidelines for resizing disks

As your storage needs change, you might need to resize a disk to hold more data or shrink the disk to make space available on the storage system volume.

- The ability to shrink a disk is supported only on Windows Server 2008 and later.
- A good time to expand a disk is right after you have expanded your storage system volumes.
- A LUN cannot be expanded to more than ten times its original size.
- Remember that LUNs with MBR-style partitions have a size limit of 2 TB, and LUNs with GPT-style partitions have a storage system size limit of 16 TB.
- Understand the storage management implications of resizing the LUN volume size.
- If it is necessary to restore a LUN from a Snapshot copy made before the LUN was resized, SnapDrive for Windows automatically resizes the LUN to the size of the Snapshot copy and performs the restore.

When the disk is restored, SnapDrive reconnects the disk. If you restore a LUN from a Snapshot copy taken before the LUN was resized, the LUN will return to its former size before it was reduced or enlarged. After the restore, data added to the LUN after it was resized must be restored from a Snapshot copy taken after it was resized.

- When creating a quorum disk, make sure it is the size recommended by Microsoft for your Windows cluster setup.

- While a LUN is being resized, it might not be available for use, so plan your disk resizing at a time when applications are less likely to be accessing the disk.

Related tasks

[Managing Snapshot copies](#) on page 143

Resizing a disk

You can resize a disk using the SnapDrive for Windows MMC snap-in to either increase or decrease the amount of space it uses.

Before you begin

Take a Snapshot copy of your disk before you resize it. If necessary, you can use the Snapshot copy to restore the disk to its original size.

About this task

If the disk you want to resize is a quorum disk in a Microsoft cluster configuration, instead of performing the following steps, you need to follow the procedure to resize a quorum disk.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand **Disks** and select the disk you want to manage.
2. From the menu choices at the top of MMC, navigate to **Action > Resize Disk**.
3. Next to "Maximum size" in the **Resize Disk** window, leave "Reserve space for at least one Snapshot copy" selected.

Note: When you select this option, the disk size limits displayed are accurate only when they first appear on the **Select LUN Properties** panel.

4. In the "New size" box, either type a value, or use the slider bar to increase or decrease the amount of space the disk uses.
5. Click **OK**.
6. Create a new Snapshot copy of the resized disk.

After you finish

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

Resizing a quorum disk

You cannot resize a disk while it is serving as a quorum disk, so a few special steps are required when using SnapDrive for Windows to resize a quorum disk in a Microsoft cluster.

Before you begin

Decide whether you would like to keep the disk as quorum or designate a new disk as quorum.

About this task

If you decide to create a new LUN and designate that disk as a quorum, you can simply create a new disk, designate it as the quorum using the Cluster Administrator on the owning node of your Windows cluster, and then delete the original quorum disk. Otherwise, follow this procedure to keep the original quorum disk and resize it.

For information about how to set a disk as a quorum, see your Windows documentation.

Steps

1. Create a new disk.
2. Designate the newly created disk as the quorum using the Cluster Administrator on the owning node of your Windows cluster.
3. Resize the original quorum disk (which is now a regular LUN).
4. Designate the expanded disk as the quorum using the Cluster Administrator on the owning node of your Windows cluster.
5. Delete the disk you created in Step 1.

Related concepts

[Rules for creating LUNs](#) on page 101

Managing LUNs not created in SnapDrive

You can use SnapDrive for Windows to manage LUNs not created by SnapDrive by completing these steps to prepare the LUNs for SnapDrive management.

Before you begin

- The names of LUNs, qtrees, igroups, volumes, and storage systems must use US-ASCII characters only.
- The LUN should have a single partition on an NTFS file system.

- If the `ostype` of the LUN is mismatched to the partition style and the type of OS accessing it, there will be significant performance degradation. Refer to the following table to see which `ostype` your LUNs should have.

Windows OS and partition style	ostype
Windows Server 2003 (MBR partitioned)	<code>windows</code>
Windows Server 2003 (GPT partitioned)	<code>windows_gpt</code>
Windows Server 2008 (MBR or GPT partitioned)	<code>windows_2008</code>
Windows Server 2008 Hyper-V (MBR or GPT partitioned)	<code>hyper_v</code>

If the LUN was created with `ostype` set to a different value than you need, you can create a new LUN using SnapDrive, copy the data to it, and delete the original LUN. You can use System Manager or FilerView to check the `ostype` of the LUN. For more information about `ostype`, see the *Data ONTAP Block Access Management Guide for iSCSI and FC*.

Note: In earlier versions of SnapDrive, LUNs were required to have the `.lun` extension to be managed by SnapDrive; however, `.lun` extensions are no longer required as of SnapDrive 4.2.

Steps

1. If you have a clustered Windows configuration, complete the procedure in this step. Otherwise, go to the next step.
 - a. In SnapDrive, create a shared disk on the storage system to temporarily designate as the quorum disk.
 - b. For each resource in this cluster group, record all dependencies by using the Windows cluster management console.

Right-click the resource and select **Properties > Dependencies**.
 - c. Designate the newly created disk as the quorum on the owning node of your Windows cluster using the Windows cluster management console. For information about how to set a disk as a quorum, see your Windows documentation.
 - d. Check that space reservation is on or that there is enough space available for space reservation to be turned on.
2. Shut down the stand-alone Windows host, or all nodes in a cluster.

Note: Shutting down your Windows hosts ensures that all data has been flushed and that Snapshot copies are consistent.
3. Using System Manager, FilerView, or the storage system console, complete the following steps:
 - a. Unmap the LUN from the initiator group.
 - b. Take a Snapshot copy of the volume on which the LUNs reside.

4. Restart the stand-alone Windows host, or all nodes in a cluster.
5. If you have a clustered Windows configuration, Windows sees the unmapped LUN as a surprise disk removal, and the disk resource is reported as "failed." Before attempting to reconnect the LUN, you need to delete the shared disk resource using the Windows cluster management console.
6. Connect to the LUN using SnapDrive.
7. If you are working in a Windows cluster, complete the procedure in this step. Otherwise, go to the next step.
 - a. Designate the newly connected LUN as the quorum using the Windows cluster management console on the owning node of your cluster.
 - b. Re-create any dependencies you recorded in Step 1.
 - c. Delete the temporary disk you created in Step 1.
8. Using SnapDrive, take a Snapshot copy of the newly connected LUN.

Related concepts

[*Rules for creating LUNs*](#) on page 101

Related tasks

[*Deleting a LUN*](#) on page 130

[*Connecting to a LUN*](#) on page 122

[*Creating a LUN as a quorum on a Windows 2003 cluster*](#) on page 110

[*Managing Snapshot copies*](#) on page 143

Guidelines for renaming LUNs

You can rename an existing LUN to conform to SnapDrive for Windows naming requirements.

- LUN names must use US-ASCII characters only, even when you use non-ASCII operating systems.
- You can rename a LUN while it is connected to a host, but rename only the LUN or volume while connected.

If any other objects need to be renamed, such as qtrees or igroups, disconnect the LUN, rename the objects, then reconnect the LUN.

Managing space on storage system volumes

SnapDrive for Windows enables you to manage space on your storage system volumes.

Next topics

[What SnapDrive fractional space reservation monitoring does](#) on page 137

[Configuring space reservation monitoring](#) on page 137

[Using the storage access control tool to enable thinly provisioned LUNs](#) on page 138

[What Space Reclaimer does](#) on page 139

What SnapDrive fractional space reservation monitoring does

Fractional space reservation monitoring in SnapDrive for Windows enables you to monitor fractional space reserved for LUNs on a storage system volume.

To monitor the fractional space reserved on your storage system from your Windows host, SnapDrive lets you perform the following tasks:

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

For more information about fractional space reservation, see the *Data ONTAP Block Access Management Guide for iSCSI and FC*.

Configuring space reservation monitoring

You can configure how SnapDrive for Windows monitors the fractional space reserved for LUNs on a storage system volume.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then select **Disks**.
2. From the menu choices at the top of MMC, navigate to **Action > Properties**.

3. In the **Disks Properties** window, select the **Space Reservation Monitor** tab.
4. In the **Space Reservation Monitor** panel, perform the following actions:
 - a. Click to deselect the **Disable Space Reservation Monitoring** checkbox.
 - b. Type a value in the Monitor Time Interval field, in minutes.
Values can be between 0 (disable) and 10,080 minutes (7 days).
 - c. Under the Space Reservation Monitor Settings tree, select the storage system and volume name.
 - d. Type a value for the Reserve Available percentage threshold.
 - e. Type a value for the Rate of Change threshold and choose MB, GB, or TB for the Unit.
 - f. Select the **Alert** checkbox if you want to be notified if this condition occurs.
5. Click **OK** or **Apply** to save your changes.
6. Click **OK**.

Using the storage access control tool to enable thinly provisioned LUNs

You can use the `storacl.exe` tool on a Windows host to set the space reservation option for any volume on a storage system to manage whether LUNs are fully provisioned or thinly provisioned.

Before you begin

- Run the storage access control (`storacl.exe`) tool from any Windows host to create the `ThinProvision.xml` file on your storage system in the `/etc` directory of the root volume. The executable is part of your SnapDrive installation and is located in the SnapDrive directory on your host.
- HTTPS must be enabled using the options `ssl.enable` command and `secureadmin setup ssl` command on the storage system.
- You must be logged in as root on the storage system.

About this task

Note: The storage system access tool provides command-line Help and usage information. Enter `spacereserve help` at the `storacl.exe` prompt for a list of additional commands and how to use them.

Step

1. Run `storacl.exe` from your Windows host, and then enter the `spacereserve set` command to set space reservation on the specified storage system volume to either True or False. Setting

space reservation to True indicates that LUNs on the volume are fully provisioned, and setting space reservation to False indicates that LUNs are thinly provisioned.

A file named ThinProvision.xml is created on the storage system to store the space reservation settings you specify.

Note: The default value is set to True on storage system volumes that do not have space reserve set in the ThinProvision.xml file.

Related references

[Storage system access control reference](#) on page 195

What Space Reclaimer does

Space Reclaimer is a SnapDrive for Windows feature that optimizes LUN space by marking newly freed space that is visible to NTFS so that it is also seen as available by Data ONTAP. Using Space Reclaimer lessens the disparity in available space that is reported by the two systems.

When files are deleted or modified on a LUN, the space is tracked by NTFS, but since this information is not communicated to the Data ONTAP file system, a disparity can grow between the available space reported by a SnapDrive host and a storage system. Space Reclaimer ensures that newly freed blocks are marked as available on the storage system.

You can use Space Reclaimer on traditional LUNs and on VMDK files attached as virtual disks using NFS datastores.

Next topics

[Guidelines for using Space Reclaimer](#) on page 139

[Starting Space Reclaimer](#) on page 140

[Stopping Space Reclaimer manually](#) on page 141

[Reasons for SnapDrive to automatically stop Space Reclaimer](#) on page 141

Related references

[Space reclamation commands](#) on page 215

Guidelines for using Space Reclaimer

You should remember these guidelines when using Space Reclaimer.

- For optimum storage performance, run Space Reclaimer as often as possible and until the entire NTFS file system has been scanned.
- Space reclamation is a time-consuming operation; therefore, it is best to run Space Reclaimer on your NTFS volume when there is a large amount of unused deleted space.
- The space reclamation process is CPU intensive, so run Space Reclaimer when storage system and Windows host usage is low; for instance, at night.

- Do not run disk defragmentation at the same time Space Reclaimer is running, as doing so can slow the disk reclamation process.
- In MSCS configurations, Space Reclaimer can be initiated from the owner node only.
- Although Space Reclaimer reclaims nearly all space from newly freed blocks, it does not reclaim 100 percent of the space.

Starting Space Reclaimer

You can start space reclamation using SnapDrive for Windows MMC snap-in.

Before you begin

To use this feature, you must have Data ONTAP 7.2.7 or later installed on your storage system.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand **Disks** and select the disk you want to manage.
2. From the menu choices at the top of MMC, navigate to **Action > Start Space Reclaimer**.

If SnapDrive detects that there is...

Then a window appears...

Space to reclaim

Confirming that the LUN space can be optimized.
Continue to the next step.

No space to reclaim

Notifying you that you do not need to run Space Reclaimer on the selected disk.
Click Cancel to exit the Confirm Space Reclamation on Disk window, or go to the next step to continue with space reclamation.

Note: When you run Space Reclaimer on a disk that SnapDrive has determined has no space to reclaim, the space reclamation process can still take as long to complete as it would for a disk that does have reclaimable space. This is because SnapDrive performs NTFS block comparisons and analyzes disk infrastructure regardless of whether there is space to reclaim.

3. In the **Confirm Space Reclamation on Disk** window, limit the amount of time Space Reclaimer runs on a LUN by selecting the "Limit (in minutes) Space Reclamation operation" checkbox.

In the space provided by the check box, type the number of minutes you want Space Reclaimer to run on the LUN. By default, Space Reclaimer runs until the LUN is optimized.
4. Click **OK** to continue.

The space reclamation process runs in the background. You can monitor the Space Reclaimer progress for the selected LUN by watching the status bar in the Details pane in MMC.

Note: SnapDrive might indicate that it is necessary to run Space Reclaimer again after it has successfully completed a space reclamation process. This can happen if data is deleted from a

LUN while Space Reclaimer is running. It is strongly recommended that the space reclamation process is performed when there is little or no activity on both the storage system and the Windows host.

Related references

[The *spacereclaim* start command](#) on page 215

Stopping Space Reclaimer manually

You can stop space reclamation using SnapDrive for Windows MMC snap-in.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand **Disks** and select the disk you want to manage.
2. From the menu choices at the top of MMC, navigate to **Action > Stop Space Reclaimer**.

Related references

[The *spacereclaim* stop command](#) on page 216

Reasons for SnapDrive to automatically stop Space Reclaimer

SnapDrive for Windows automatically stops Space Reclaimer in several instances.

- During any LUN management operation on a LUN running Space Reclaimer, including LUN disconnect and LUN delete operations
- During any Snapshot copy management operation except Snapshot copy rename and delete
- On all LUNs of the same storage system volume during Snapshot copy creation
- If the SnapDrive service is stopped
- During LUN restore operations for any volume mount points directly or indirectly mounted (cascading) from the disk being restored
- During Windows host cluster failover

If a host cluster failover operation occurs on a Windows Server 2003 MSCS or Windows Server 2008 failover cluster while Space Reclaimer is running on a shared LUN, space reclamation will stop running on that LUN.
- During any MPIO path management operations, including adding or removing an initiator or active path selection

Managing Snapshot copies

You can use SnapDrive for Windows to create, schedule, restore, and delete Snapshot copies as well as some other Snapshot copy management tasks.

Next topics

[*Reasons for creating Snapshot copies*](#) on page 143

[*Restrictions on Snapshot copy creation*](#) on page 144

[*Creating a Snapshot copy*](#) on page 144

[*Scheduling Snapshot copies*](#) on page 145

[*About using FlexClone volumes in SnapDrive*](#) on page 146

[*Snapshot copy cautions*](#) on page 147

[*Connecting to a LUN in a Snapshot copy*](#) on page 148

[*How LUN restoration from Snapshot copies works*](#) on page 149

[*Deleting a Snapshot copy*](#) on page 152

[*Overview of archiving and restoring Snapshot copies*](#) on page 153

Reasons for creating Snapshot copies

You use SnapDrive to ensure that you create consistent Snapshot copies in the event you need to restore a LUN from that copy.

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

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

Restrictions on Snapshot copy creation

You must keep in mind some restrictions for creating Snapshot copies.

- You can keep a maximum of 255 Snapshot copies with Data ONTAP.
After the number of Snapshot copies has reached the limit, the Snapshot Create operation fails, and you must delete some of the old Snapshot copies before you can create any more.
- SnapDrive does not support Snapshot copies that are created from the storage system console, because such a practice can lead to inconsistencies within the NTFS file system. Therefore, use only SnapDrive to create Snapshot copies of LUNs.
- You cannot create a Snapshot copy of a LUN connected to a Snapshot copy.
- SnapDrive automatically turns off the Snapshot copy schedule on a storage system volume that stores LUNs, so that the storage system does not create automatic Snapshot copies.

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

Creating a Snapshot copy

You should always use SnapDrive to create Snapshot copies of LUNs to ensure that Snapshot copies are consistent.

Before you begin

The following requirements must be met in order to successfully create Snapshot copies using SnapDrive:

- You must create Snapshot copies through the SnapDrive MMC snap-in or through `sdcli.exe`, rather than the storage system console or the volume Snapshot copy schedule on the storage system. This is because SnapDrive must first flush NTFS so that the LUN is consistent at the moment the Snapshot copy is made. This ensures the usability of the LUN in the Snapshot copy directory.
- Snapshot names must be created using US-ASCII characters only, even when using non-ASCII operating systems.

Note: The SnapDrive service can perform only one task at a time. If you schedule multiple tasks to start at exactly the same time, the first will proceed, and SnapDrive will queue the others until the first task either succeeds or times out.

Steps

1. Perform the following actions to get to the Create Snapshot menu item:

- a. In the left MMC pane, select the instance of SnapDrive you want to manage.
- b. Double-click **Disks**.
- c. Double-click the disk for which you want to create a Snapshot copy.
- d. Select **Snapshots**.
- e. From the menu choices at the top of MMC, navigate to **Action > Create Snapshot**.

The **Create Snapshot** text box is displayed.

2. In the **Create Snapshot** text box, perform the following actions:

- a. Type an easy-to-interpret name for the Snapshot copy.

Example

expenses_db_15Jan07_4pm

Note: Snapshot copy names must be created using US-ASCII characters only, even when using non-ASCII operating systems.

- b. Click **OK**.

Note: All LUNs in the volume attached to this host are included in the Snapshot copy, as well as LUNs from other hosts that are also in the volume. The only LUNs that will be consistent, however, are those attached to the host initiating the Snapshot copy request.

Result

Your Snapshot copy is created.

Details about the Snapshot copy appear at the bottom panel of the center MMC pane.

Scheduling Snapshot copies

Create a Snapshot copy schedule to ensure that SnapDrive creates Snapshot copies at intervals appropriate to your environment.

About this task

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

Steps

1. Create a batch file (a file with a .bat extension) containing the following command on the Windows host on which you are scheduling Snapshot copies:

```
sdcli snap create [-m MachineName] -s SnapshotName -D DriveLetterList  
[. . .] [-x]
```

MachineName is the name of the Windows host on which the command will be executed. If no machine name is specified, the command is executed on the local machine.

SnapshotName is the name of the Snapshot copy to be created.

DriveLetterList is a list of space-separated drive letters.

When **-x** flag is specified, Snapshot copies are created only for the drives specified by the **-D** flag. Otherwise, Snapshot copies are created for all the disks on the storage system volumes used by the listed drives.

Example

```
sdcli snap create -s Jun_13_07 -D j k l
```

The preceding example creates a Snapshot copy named Jun_13_07 for each volume containing one or more of the LUNs mapped to the specified drives (that is, J:, K:, and L:). The Snapshot copies created are consistent for all LUNs contained by those volumes.

2. Select **Start Menu > Settings > Control Panel > Scheduled Tasks**.
3. Double-click **Add Scheduled Task**.
The **Scheduled Task Wizard** is launched.
4. In the **Scheduled Task Wizard**, click **Next**.
5. Click **Browse**, and locate the batch (.bat) file you created in Step 1.
6. Select the batch file and click **Open**.
7. In the next panel, select from the list of frequencies, then click **Next**.
8. In the next panel, type a start time and complete the detailed frequency parameters. The option details displayed on this panel vary depending on the Snapshot copy frequency you picked in the previous panel.
9. In the next panel, type the user name (the administrator account name and password, repeated for confirmation), then click **Next**.
10. Click **Finish**.

Result

Your schedule is created.

About using FlexClone volumes in SnapDrive

By default, if the prerequisites are met, SnapDrive uses FlexClone technology to connect to LUNs in a Snapshot copy.

SnapDrive connects a host to a LUN in a Snapshot copy in read/write mode by mounting a LUN that is stored in a Snapshot copy (this has been the traditional method) or by connecting to a clone of a flexible volume using a flexible volume clone (FlexClone). By default, if the prerequisites are met,

SnapDrive uses FlexClone technology to connect to LUNs in a Snapshot copy. The use of FlexClone technology by SnapDrive is helpful for conducting tests or for verifying data on a live SnapMirror destination.

Next topics

[*Prerequisites for using FlexClone volumes with SnapDrive*](#) on page 147

[*About read/write connections*](#) on page 147

Prerequisites for using FlexClone volumes with SnapDrive

There are several prerequisites that must be met in order for SnapDrive to use FlexClone volumes.

- Your storage system must be running Data ONTAP 7.2.7 or later.
- Only flexible volumes can be used to create FlexClones.
- There must be enough space available on the aggregate to create a non-space-reserved flexible volume (volume guarantee=none).
- FlexClone must be licensed on your storage system.

About read/write connections

If FlexClone volumes are not available because the prerequisites for their use have not been met, SnapDrive uses a read/write connection to a LUN in a Snapshot copy that is actually a connection to a special type of LUN.

Read/write connection to LUNs in a Snapshot copy have the following properties:

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

For details, see your Data ONTAP documentation.

Snapshot copy cautions

Keep the following points in mind when working with Snapshot copies and LUNs that are backed up by a Snapshot copy:

- Information written to the .rws file is temporary; SnapDrive deletes the .rws file when you disconnect.
- You cannot merge the data written to the .rws file with the data in the Snapshot copy referenced by the .rws file.

- You cannot delete a Snapshot copy that is in use by a LUN backed by a Snapshot copy.
- You can connect to the LUN Snapshot copy only by using read/write mode and a LUN that is backed by a Snapshot copy.
- You should avoid creating a Snapshot copy of a LUN backed by a Snapshot copy. Doing so will lock the Snapshot copy backing the LUN until the newer Snapshot copy—and all Snapshot copies of that LUN—are deleted.

Related concepts

[Problems deleting Snapshot copies due to busy snapshot error](#) on page 153

Connecting to a LUN in a Snapshot copy

You can connect to a LUN in a Snapshot copy using either a FlexClone volume or a read/write connection to a LUN in a Snapshot copy depending on what version of Data ONTAP you have installed on your storage system.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand **Disks** and select the disk you want to manage.
2. Expand the LUN whose Snapshot copy you want to connect, then click on **Snapshot Copies** to display the list of Snapshot copies. Select the Snapshot copy you want to connect.
Note: If you cannot see the Snapshot copy list, make sure that `cifs.show_snapshot` is set to on and `vol options nosnapdir` is set to off on your storage system.
3. From the menu choices at the top of MMC, navigate to **Action > Connect Disk** to launch the Connect Disk wizard.
4. In the **Connect Disk Wizard**, click **Next**.
5. In the **Provide a Storage System Name, LUN Path and Name** panel, the information for the LUN and Snapshot copy you selected is automatically filled in. Click **Next**.
6. In the **Select a LUN Type** panel, **Dedicated** is automatically selected because a Snapshot copy can be connected only as a dedicated LUN. Click **Next**.
7. In the **Select LUN Properties** panel, either select a drive letter from the list of available drive letters or type a volume mount point for the LUN you are connecting, then click **Next**.

When you create a volume mount point, type the drive path that the mounted drive will use: for example, `G:\mount_drive1\`.

8. In the **Select Initiators** panel, select the FC or iSCSI initiator for the LUN you are connecting and click **Next**.

9. In the **Select Initiator Group management** panel, specify whether you will use automatic or manual igroup management.

If you specify...	Then...
Automatic igroup management	Click Next . SnapDrive uses existing igroups, one igroup per initiator, or, when necessary, creates new igroups for the initiators you specified in the Select Initiators panel.
Manual igroup management	Click Next , and then perform the following actions: a. In the Select Initiator Groups panel, select from the list the igroups to which you want the new LUN to belong. Note: A LUN can be mapped to an initiator only once. OR Click Manage Igroups and for each new igroup you want to create, type a name in the Igroup Name text box, select initiators from the initiator list, click Create, and then click Finish to return to the Select Initiator Groups panel. b. Click Next .

10. In the **Completing the Connect Disk Wizard** panel, perform the following actions.

- a. Verify all the settings
- b. If you need to change any settings, click Back to go back to the previous Wizard panels.
- c. Click **Finish**.

Result

The newly connected LUN appears under Disks in the left MMC pane.

How LUN restoration from Snapshot copies works

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

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

Note: If it is necessary to restore a LUN from a Snapshot copy made before the LUN was resized, SnapDrive for Windows automatically resizes the LUN to the size of the Snapshot copy and performs the restore. Such a restore causes the loss of any data added to the LUN after it was resized, and it can damage virtual machines (such as Hyper-V VMs) or applications if they are running on the LUN during the restore.

Next topics

[About the Data ONTAP LUN clone split \(rapid LUN restore\) feature](#) on page 150

[Restoring a LUN from a Snapshot copy](#) on page 150

[Checking LUN restore status](#) on page 151

[About volume-based Snapshot copy restoration with SnapDrive](#) on page 152

About the Data ONTAP LUN clone split (rapid LUN restore) feature

SnapDrive uses the LUN clone split (rapid LUN restore) feature of Data ONTAP when restoring a LUN.

A LUN clone is a point-in-time, writable copy of a LUN in a Snapshot copy. After the clone is created, all read/write operations are made on the clone and read/write operations are no longer made on the original LUN.

A LUN clone shares space with the original LUN in the backing Snapshot copy. The clone does not require additional disk space until changes are made to it. When Data ONTAP splits the clone from the backing Snapshot copy, Data ONTAP copies the data from the Snapshot copy, and copies the blocks from the original LUN, to the clone. After the splitting operation, the clone becomes a regular LUN, and the original LUN is deleted by Data ONTAP.

Note: If you do not have enough disk space for both the clone and the original LUN, the split will not be initiated and no LUN restoration can occur.

Benefit of using rapid LUN restore

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

Restoring a LUN from a Snapshot copy

SnapDrive restores a LUN using the rapid LUN restore feature.

Before you begin

- Shut down all resources directly or indirectly dependent on the LUN.
Make sure that the LUN is not being used by the Windows file system or any other process, and that no user has the LUN open in Windows Explorer. Shut down any application that is using the LUN.

Attention: Make sure that the Windows Performance Monitor (perfmon) is not monitoring the LUN.

Note: Make sure that virtual machines, Microsoft Exchange, or any other applications are no longer running on a LUN before you restore that LUN from a Snapshot copy.

Steps

1. Perform the following actions:
 - a. In the left MMC pane, select the instance of SnapDrive you want to manage.
 - b. Double-click Disks to display all available disks.
 - c. Select the LUN that you want to restore and double-click it to display all the Snapshot copies list.
 - d. Select the Snapshot copy from which to restore the LUN.
2. In the menu choices at top of MMC, click **Action > Restore Disk**.

Note: You can only restore a Snapshot copy that is consistent with the active file system. Inconsistent Snapshot copies are not available for restoration and are grayed out.

The **Restore Snapshot Copy** panel is displayed.

3. In the **Restore Snapshot Copy** panel, click **Yes** to restore the LUN from the Snapshot copy you selected.

Attention: Do not attempt to manage any Windows cluster resources while the restore is in progress.

Checking LUN restore status

Check whether LUN restoration has completed by viewing the Restore Status field in the SnapDrive MMC.

Steps

1. Perform the following actions:
 - a. In the left MMC pane, select the instance of SnapDrive you want to manage.
 - b. Double-click Disks.
2. In the center MMC pane, locate the name of the disk you are restoring. The status is displayed in the lower panel of the center MMC pane.

Note: You can also check the status of a LUN restore using the disk list command of the sdcli.exe utility.

Result

If a restore is in progress, SnapDrive will display the percentage completed, otherwise; the status will display Normal.

Related references

The disk list command on page 226

About volume-based Snapshot copy restoration with SnapDrive

Use volume-based Snapshot copy restoration using the SnapDrive sdcli utility.

SnapDrive supports volume-based Snapshot copy restoration on volumes containing only non-connected LUNs, and breaks the SnapMirror connection if the operation is performed on a live SnapMirror destination.

Volume restore functions are currently available only through the sdcli.exe utility.

Related references

Snapshot copy commands on page 228

Deleting a Snapshot copy

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

Steps

1. Perform the following actions:
 - a. In the left MMC pane, select the instance of SnapDrive you want to manage.
 - b. Double-click Disks.
 - c. Select the LUN whose Snapshot copy you want to delete.
2. In the right MMC pane, select the Snapshot copy you want to delete.

Note: You can only delete a Snapshot copy that is consistent with the LUN. Inconsistent Snapshot copies are not available for deletion.
3. From the menu choices on top of MMC, click **Action > Delete**.

The **Delete Snapshot** panel is displayed.
4. In the **Delete Snapshot** panel, click **Yes** to delete the Snapshot copy you selected.

Note: If you get an error message stating that the Snapshot copy is busy or cannot be deleted, it is likely that the Snapshot copy is in use by a LUN that is backed by a Snapshot copy.

Problems deleting Snapshot copies due to busy snapshot error

If you attempt to delete a Snapshot copy and you get an error message saying that the Snapshot copy is busy and cannot be deleted, you either have a Snapshot copy that was taken of a LUN backed by another Snapshot copy or the Snapshot copy backed LUN is still connected.

If you have a Snapshot copy that was taken of a LUN backed by another Snapshot copy, you need to delete the newer Snapshot copy before the older Snapshot copy, the Snapshot copy backing the LUN, can be deleted.

If the LUN backed by a Snapshot copy is still connected, disconnect it.

Attention: Data on the LUN is no longer available when you disconnect it. If you need the data on the LUN, back it up or copy it to another LUN before you disconnect it.

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

Overview of archiving and restoring Snapshot copies

A good way to protect and retain data is to archive the SnapDrive Snapshot copies of the LUNs to offline, offsite media, such as near-line technology or alternate storage methods.

The practice of archiving Snapshot copies is particularly beneficial for disaster recovery.

What to back up

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

Ways to archive SnapDrive backups

You can use the Data ONTAP dump command or an NDMP-based backup application to archive the Snapshot copies of your LUNs.

Process for restoring LUNs from archival media

First, restore the LUN file from your archive media to the active file system. After the file is restored, use the SnapDrive management interface to connect to the LUN file using its original drive letter.

Note: You cannot use CIFS-based or NFS-based backup products to archive the Snapshot copies of your LUNs.

For more information about 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 LUN files. This holds true for all SnapManager products. For more information about recovering LUNs using SnapManager, see the current SnapManager System Administrator's Guide for your product.

Using SnapVault with SnapDrive

You can use the SnapVault feature of Data ONTAP with SnapDrive for Windows to back up Snapshot copies to a secondary storage system.

Next topics

[*Considerations for using SnapVault*](#) on page 155

[*Initiating SnapVault backups from SnapDrive*](#) on page 155

Considerations for using SnapVault

SnapVault is a Data ONTAP feature that provides a fast, efficient, and centralized backup solution for replicating Snapshot copies to a secondary storage system. There are several considerations you should remember when using the SnapVault feature with SnapDrive for Windows.

- You must have at least Data ONTAP 7.2.6 installed on your storage system.
- SnapVault must be licensed on the primary and secondary storage systems.
- SnapVault relationships must already be configured and initialized.
- A backup set might contain multiple primary storage systems and volumes, but only one secondary volume and storage system.
- Each backup set can span only one volume on a secondary storage system; if multiple volumes are required, the backup will fail.
- Only qtree SnapVault configurations are supported. SnapDrive does not support volume-based SnapVault.
- SnapVault cascaded configurations are not supported.
- There is no SnapVault restore feature.

Initiating SnapVault backups from SnapDrive

SnapVault backups can be initiated from within MMC or by using the SnapDrive for Windows CLI.

About this task

These steps describe how to initiate a backup using the Update SnapVault option in MMC.

Alternatively, you can also initiate a backup using the `sdcli snapvault archive` command.

Steps

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then select **Disks**.
2. Double-click the LUN for which you want to perform a SnapVault update.
3. Select **Primary Snapshots** to display the Snapshot copies on the primary system.
4. In the right MMC pane, right-click the Snapshot copy from which you want the SnapVault update to be initiated and select **SnapVault** from the menu.

A Snapshot copy with the same name as the Snapshot copy you selected on the primary system is created on the secondary storage system after the SnapVault update.

SnapDrive integration with Protection Manager

SnapDrive for Windows integrates with Protection Manager to provide management of SnapMirror and SnapVault deployments using datasets.

Next topics

[How SnapDrive integrates with Protection Manager](#) on page 157

[Dataset concepts](#) on page 157

How SnapDrive integrates with Protection Manager

SnapDrive for Windows supports Protection Manager datasets through the SnapManager products.

Protection Manager makes it easy to manage very large SnapMirror and SnapVault deployments by grouping data and storage systems into *datasets* and *resource pools*, enabling automation of many routine data protection tasks. You can configure SnapDrive with a set of DataFabric Manager (DFM) credentials so that it can authenticate to a DFM server. This allows a SnapManager to use SnapDrive as a conduit to support Protection Manager retention policies and schedules.

To take advantage of these Protection Manager features through SnapDrive for Windows, you must have a DFM server with version 3.7 or later, and your storage systems must be running Data ONTAP 7.3 or later.

For more information, refer to your SnapManager documentation.

Dataset concepts

Associating a data protection, disaster recovery, or provisioning policy with a dataset lets storage administrators automate tasks, such as assigning consistent policies to primary data, propagating policy changes, and provisioning new volumes, qtrees, or LUNS on primary and secondary dataset nodes. The licenses that you have installed determine which policies are available.

Configuring a dataset combines the following objects:

- Dataset** For protection purposes, a dataset is a collection of physical resources on a primary node, such as volumes, flexible volumes, and qtrees, and the physical resources for copies of backed-up data on secondary and tertiary nodes.
- For provisioning purposes, a dataset is a collection of physical resources, such as volumes, flexible volumes, qtrees, and LUNs, that are assigned to a dataset node. If the protection license is installed and the protection policy establishes a primary and one or more nonprimary nodes, each node of the dataset is a collection of physical resources that might or might not be provisioned from the same resource pool.

Resource pool	A collection of physical resources from which secondary storage is provisioned. Resource pools can be used to group storage systems and aggregates by attributes, such as performance, cost, physical location, or availability.
Data protection policy	A data protection policy defines how to protect the primary, secondary, and tertiary storage, as well as when to create copies of data and how many copies to keep.
Storage service	A storage service is a single dataset configuration package that consists of a protection policy, provisioning policies, resource pools, and an optional vFiler template (for vFiler unit creation). You can assign a single uniform storage service to datasets with common configuration requirements as an alternative to separately assigning the same protection policy, provisioning policies, resource pools, and setting up similar vFiler unit attachments to each of them.

Understanding the Volume Shadow Copy Service

The Data ONTAP VSS Hardware Provider is installed with SnapDrive for Windows and can be used with Microsoft Volume Shadow Copy Service.

Next topics

[Overview of VSS](#) on page 159

[SnapDrive VSS requirements](#) on page 160

[Typical VSS backup process](#) on page 160

[Troubleshooting the VSS Hardware Provider](#) on page 161

Overview of VSS

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

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

- VSS requestor
The VSS requestor is a backup application, such as the application or NTBackup. It initiates VSS backup and restore operations. The requestor also specifies Snapshot copy attributes for backups it initiates.
- VSS writer
The VSS writer owns and manages the data to be captured in the Snapshot copy is an example of a VSS writer.
- VSS provider
The VSS provider is responsible for the creation and management of the Snapshot copy. A provider can be either a hardware provider or a software provider:
 - A hardware provider integrates storage array-specific Snapshot copy and cloning functionality into the VSS framework. The Data ONTAP VSS Hardware Provider integrates the SnapDrive service and storage systems running Data ONTAP into the VSS framework.

Note: The Data ONTAP VSS Hardware Provider is installed automatically as part of the SnapDrive software installation.
 - A software provider implements Snapshot copy or cloning functionality in software that is running on the Windows system.

Note: To ensure the Data ONTAP VSS Hardware Provider works properly, do not use the VSS software provider on Data ONTAP LUNs. If you use the VSS software provider to

create Snapshot copies on a Data ONTAP LUN, you will be unable to delete that LUN using the VSS hardware provider.

SnapDrive VSS requirements

To use VSS with SnapDrive for Windows, your storage system and SnapDrive host must meet minimum requirements.

- Your storage system must be running at least Data ONTAP 7.2.
Note: In versions of Data ONTAP prior to 7.3, snapshots taken after a shadow copy are locked due to the existence of LUN clones in the previous Snapshot copies, making them impossible to delete. In Data ONTAP 7.3, this restriction is removed, so SnapDrive is able to delete any Snapshot copies.
- The Virtual Disk Service must be running on your Windows host.

Typical VSS backup process

A typical backup using SnapManager for Microsoft Exchange, Microsoft Exchange 2003 or 2007, and the Data ONTAP VSS Hardware Provider is outlined in the following process.

1. SnapManager determines which LUNs it wants to capture and makes sure that Exchange 2003 or Exchange 2007 is present as a valid writer.
2. SnapManager initiates the shadow copy process.
3. VSS informs Exchange and the Data ONTAP VSS Hardware Provider that a shadow copy is starting. Exchange stops writing to disk.
4. VSS ensures that NTFS is in a consistent state.
5. VSS requests the Data ONTAP VSS Hardware Provider to create a shadow copy.
6. The Data ONTAP VSS Hardware Provider requests SnapDrive to create a Snapshot copy of the storage system volume that contains the specified LUN.
7. SnapDrive requests the storage system to create a Snapshot copy of the specified volume.
8. When the shadow copy is complete, VSS returns NTFS to a normal state and informs Exchange that it can resume disk writes.
9. VSS manages the shadow copy of the LUN based on the attributes specified by the requestor. For example, VSS could mount the LUN in a Snapshot copy. In a case, however, in which SnapManager is the requestor, SnapManager tells VSS to forget about the shadow copy it just created. This enables SnapManager to have complete control of the Snapshot copy.

Troubleshooting the VSS Hardware Provider

If you attempt to create a backup on a storage system running Data ONTAP, and a Snapshot copy is not created on the storage system, you can troubleshoot the VSS Hardware Provider in several ways.

About this task

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

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

Only the Data ONTAP VSS Hardware Provider can take a Snapshot copy on a storage system. When you use a VSS requestor, such as SnapManager for Microsoft Exchange or NTBackup, to back up a LUN backed by a storage system running Data ONTAP, the Data ONTAP VSS Hardware Provider must be used for the Snapshot copy to succeed.

Steps

1. View the installed providers and verify that the Data ONTAP VSS Hardware Provider is installed.
2. Verify that the Data ONTAP VSS Hardware Provider was used to create the Snapshot copy and that it was completed successfully.
3. Verify your VSS configuration.

Next topics

[Viewing installed VSS providers](#) on page 161

[Verifying that the VSS Hardware Provider was used successfully](#) on page 162

[Verifying your VSS configuration](#) on page 162

Viewing installed VSS providers

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

Steps

1. Select **Start > Run** and enter the following command to open a Windows command prompt:
`cmd`
2. At the prompt, enter the following command:
`vssadmin list providers`

The output should be similar to the following:

```
Provider name: 'Data ONTAP VSS Hardware Provider'  
Provider type: Hardware  
Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}  
Version: 6.3.0.xxxx
```

Verifying that the VSS Hardware Provider was used successfully

To verify that the Data ONTAP VSS Hardware Provider was used successfully after a Snapshot copy was taken, complete this step.

Step

1. Navigate to **System Tools > Event Viewer > Application** in MMC and look for an event with the following values.

Source	Event ID	Description
Navsspr	4089	The VSS provider has successfully completed CommitSnapshots for SnashotSetId <i>id</i> in <i>n</i> milliseconds.

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

Verifying your VSS configuration

If the Data ONTAP VSS Hardware Provider failed to run or did not successfully complete a Snapshot copy, complete these steps.

Steps

1. Verify that SnapDrive for Windows is installed and running and can communicate with the storage system by performing the following steps.
 - a. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then select **Disks**.
 - b. From the menu choices at the top of MMC, navigate to **Action > Refresh**.

No error messages should be displayed.

2. Verify that the `lun.inquiry.mode` option is set to `legacy` and not `standard` on the storage system.

This setting applies if you are using Data ONTAP 7.2 and you are also using Exchange or SQL Server for VSS-based backups. By default, the mode is set to `legacy`.

Attention: To change or set this option, you must first stop FC and iSCSI services on your storage system, which might temporarily disrupt any operations currently in progress. Use `fcg stop` and `iscsi stop` to stop the services. Use `fcg start` and `iscsi start` to restart the services after setting the mode.

- a. To verify the setting, at the storage system prompt enter the following command:

```
options lun.inquiry.mode
```

- b. To change the setting, enter the following command:

```
options lun.inquiry.mode legacy
```

3. Verify that the drives for which the Data ONTAP VSS Hardware Provider failed are backed by a LUN on a storage system running Data ONTAP.

To do this, open MMC and verify that the drives appear under the Disks icon under SnapDrive.

4. Verify that the account used by the Data ONTAP VSS Hardware Provider is the same as the account used by SnapDrive by performing the following steps.
 - a. In the left MMC pane, select **Services and Applications > Services**.
 - b. Double-click the **SnapDrive** service in the main pane and select the **Log On** tab.
 - c. Note the account listed in the **This Account** field, then click **OK** to close the **SnapDrive Properties** window.
 - d. Double-click the **Data ONTAP VSS Hardware Provider** service in the main pane and click the **Log On** tab.
 - e. Verify that the **This Account** field is selected and that it contains the same account as the SnapDrive service.

SAN booting with SnapDrive

SnapDrive for Windows supports SAN booting, but some tasks are restricted.

Next topics

[What SAN booting is](#) on page 165

[How SnapDrive supports SAN booting](#) on page 165

What SAN booting is

SAN booting is the general term for booting a host from a storage system LUN instead of an internal hard disk.

Fiber Channel SAN booting does not require support for special SCSI operations; it is not different from any other SCSI disk operation. The HBA uses special code in the BIOS that enables the host to boot from a LUN on the storage system.

iSCSI SAN booting also uses special code in the BIOS that enables the host to boot from a LUN on the storage system. You need to set specific parameters in the BIOS to enable iSCSI SAN booting.

The general process is as follows.

1. After the HBA has accessed the BIOS, use the Emulex or QLogic BootBIOS utility to configure the LUN as a boot device.
2. Configure the PC BIOS to make the LUN the first disk device in the boot order.
3. Install the following on the LUN.
 - Windows operating system
 - HBA driver

Note: Following a system failure, the bootable virtual disk is no longer the default boot device. You need to reconfigure the hard disk sequence in the system BIOS to set the bootable virtual disk as the default boot device.

How SnapDrive supports SAN booting

SnapDrive for Windows identifies bootable LUNs and prevents you from performing some of the operations you would normally perform on a nonbootable LUN.

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

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

- Disconnect
- Delete
- Expand
- Restore

SnapDrive does support the following Snapshot copy-related actions on bootable LUNs:

- Create
- Rename
- Delete

Note: Restoring Snapshot copies of bootable LUNs is not allowed by SnapDrive. For important information about Snapshot copies of bootable LUNs, see the technical white papers on the NOW site.

Using SnapMirror with SnapDrive for Windows

You can use SnapMirror with SnapDrive for Windows to replicate data.

Next topics

[*SnapMirror overview*](#) on page 167

[*Types of SnapMirror replication*](#) on page 167

[*Requirements for using SnapMirror with SnapDrive*](#) on page 169

[*Initiating replication manually*](#) on page 170

[*Connecting to a LUN in a mirrored destination volume*](#) on page 171

[*Restoring a volume on a SnapMirror destination*](#) on page 172

[*Recovering a cluster from shared LUNs on a SnapMirror destination*](#) on page 173

SnapMirror overview

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

With asynchronous SnapMirror, data is replicated from a source volume to a partner destination volume at regular intervals.

With synchronous SnapMirror, data from a source volume or qtree is replicated on a destination volume or qtree at, or near, the same time it is written to the first storage system.

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

If a storage system volume or storage system holding one or more LUNs suffers a catastrophic failure, you can use a mirrored destination volume to recover the LUNs.

Types of SnapMirror replication

SnapMirror replicas are initiated upon normal Snapshot copy creation or when using special rolling Snapshot copies.

Replication upon Snapshot copy creation

Each time a Snapshot copy of a LUN is created—manually or because of a Snapshot copy schedule—SnapDrive determines whether the LUN from which a Snapshot copy was made resides on a SnapMirror source volume. If so, then after the Snapshot copy has been made, SnapDrive may send a

SnapMirror update request to all the destination volumes associated with the source volume for that LUN.

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

Replication using rolling Snapshot copies

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

SnapDrive creates a new rolling Snapshot copy every time you initiate a mirror update operation (using the Update Mirror option in the Action menu or the `sdcli snap update_mirror` command) for a specific LUN drive residing on a SnapMirror source volume.

To guarantee that at least one rolling Snapshot copy for each LUN is always available on the destination volume, SnapDrive maintains a maximum of two rolling Snapshot copies on the source volume.

Next topics

[*How SnapDrive manages rolling Snapshot copies*](#) on page 168

[*How rolling Snapshot copies are named*](#) on page 169

How SnapDrive manages rolling Snapshot copies

When you initiate an Update Mirror operation, SnapDrive checks for any existing rolling Snapshot copies of the LUN containing the specified LUN drive

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

Note: When you connect to a LUN in a Snapshot copy that is located on a traditional volume, SnapDrive creates a LUN backed by a Snapshot copy on the active file system. When a new Snapshot copy is created as part of a synchronous SnapMirror update, that new Snapshot copy will lock the Snapshot copy from which the LUN was connected. While the original Snapshot copy is locked, you will be unable to delete it until the next SnapMirror update when the first Snapshot copy is deleted automatically.

How rolling Snapshot copies are named

Rolling Snapshot copies can be identified by the unique names they are given.

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

@snapmir@{GUID}

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

Examples of rolling Snapshot copies

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

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

Requirements for using SnapMirror with SnapDrive

Before you can use SnapMirror with SnapDrive for Windows, your system must meet several requirements.

- SnapMirror must be licensed on the source and destination storage systems. For information on how to license and set up SnapMirror, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.
- Depending on the LUN protocols you are using, enable the iSCSI and FC licenses on the destination storage systems to enable LUN connect and LUN management operations.
- You must manually create and initialize a mirror between the source and destination volumes, but you must not create a SnapMirror replication schedule.

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

- You must create your SnapMirror relationship using storage system names (either the fully qualified DNS name or the storage system name alone), and the network interface to be used for SnapMirror transfers (for example, storage1-e0), not IP addresses.
- If you are using the optional MultiStore feature of the Data ONTAP software to create virtual storage systems (vFiler units), you must create your SnapMirror relationship on the vFiler unit, not on the physical storage system.
- The system must contain one or more SnapMirror source volumes hosting LUNs.
- The system must contain one or more SnapMirror destination volumes for each source volume.

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

- The destination volume must be at least as large as the source volume.
- The Windows domain account used by the SnapDrive service must be a member of the local BUILTIN\administrators group and must have management access to both the source and destination storage systems.
- The Windows domain account used to administer SnapDrive must have full access to the Windows domain to which both the source and destination storage systems belong.
- The source and destination storage systems must be configured to grant root access to the Windows domain account used by the SnapDrive service. That is, the `wafL.map_nt_admin_priv_to_root` option must be set to On. For information about enabling storage system options, see your Data ONTAP documentation.
- If you want to use a Windows host to access the replicated LUNs on the destination volume, the destination storage system must have at least one LUN access protocol licensed (iSCSI or FC).
- A TCP/IP connection must exist between the source storage system and the destination storage system.
- The SnapDrive service can perform one task at a time. Therefore, if you are scheduling multiple tasks on a host, make sure that you do not schedule these tasks to start at exactly the same time. If multiple tasks are scheduled at the same time, the first will proceed, and SnapDrive will queue the others until the first task either succeeds or times out.

Note: SnapMirror cascaded configurations are not supported.

Related tasks

[Configuring access for SnapDrive](#) on page 66

Initiating replication manually

SnapDrive initiates SnapMirror replication automatically when a Snapshot copy is created, but you can also initiate SnapMirror replication manually.

Before you begin

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

Note: Manual replication is not monitored by SnapDrive so you will not know if replication succeeded.

Steps

1. Perform the following actions to select the LUN that you want to replicate:
 - a. In the left MMC pane, select the instance of SnapDrive you want to manage.

- b. Double-click Disks.
2. In the right MMC panel, select the LUN that you want to replicate.
3. Click Action (from the menu choices at the top of MMC window).
4. Select Update Mirror from the drop-down menu.

Note: The Update Mirror option is not available if no live mirror copies are configured.

Result

The Update Mirror operation is initiated and a rolling Snapshot copy of the LUN is created. After the Snapshot copy has been created on the mirrored source volume, SnapDrive automatically updates the mirrored destination volume.

Connecting to a LUN in a mirrored destination volume

Connect to a LUN on a SnapMirror destination volume when you want to continue to serve data if a LUN on the source volume is inaccessible.

Before you begin

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

- SnapDrive supports the use of FlexClone volumes, which enable you to clone an independent volume from a parent FlexVol volume so that the mirror can remain unbroken.
- The LUN on an asynchronous SnapMirror destination must be restored from the most recent SnapDrive-created Snapshot copy containing a valid image of that LUN. The restoration is performed by SnapDrive as part of the LUN connect operation on an active file system or on a SnapMirror destination volume.

Note: The most recent Snapshot copy must be one created by SnapDrive to ensure data consistency. Data ONTAP creates a Snapshot copy that is more recent than the Snapshot copy created by SnapDrive; however, the Data ONTAP Snapshot copy cannot be used by SnapDrive because it is not consistent.

Steps

1. Connect to the mirrored LUN on the SnapMirror destination storage system.
2. If you want to break the mirror and connect to a SnapMirror destination volume that is online and, in the case of an asynchronous SnapMirror volume, perform a single file SnapRestore operation or rapid LUN restore, click Yes in the Connect Disk dialog box.

Note: Perform this step only if the destination volume is not “broken”. The mirror does not need to be broken if you connect to a LUN inside a Snapshot copy.

Related tasks

[Connecting to a LUN in a Snapshot copy](#) on page 148

Restoring a volume on a SnapMirror destination

The volume restore feature in SnapDrive enables you to restore all the LUNs on a volume automatically from a single SnapDrive copy when you establish a connection to the first LUN on a SnapMirror destination.

Before you begin

The following prerequisites must be met before SnapDrive can initiate a volume-based Snapshot copy restoration:

- All LUNs on the active file system must be consistent in the Snapshot copy you intend to use to restore.
- LUNs on the active file system must be of the same size and have the same name as the selected Snapshot copy.
- A SnapMirror relationship must exist.
- LUNs on the volume being restored must be disconnected from the host before they can be restored from the Snapshot copy.

About this task

Volume restore functions are currently available through the sdcli utility.

Step

1. Enter the following command from a Windows command prompt:

```
sdcli snap restore_volume [-f StorageSystemName] -volume  
StorageSystemVolumeName -s SnapshotCopyName [-force] [-m MachineName]
```

-f *StorageSystemName* is the name of the storage system on which the volume resides.

-volume*StorageSystemVolumeName* indicates name of the volume on which the restore operation will be performed.

-s *SnapshotCopyName* indicates the name of the Snapshot copy from which the volume will be restored.

-force is an optional switch that you use to ensure the volume restoration is performed even when non-LUN files or newer Snapshot copies are found on the volume.

-m*MachineName* is the host on which the operation is executed. You can use an IP address or a machine name to identify the host.

Result

The restoration is performed on the volume indicated.

Example

```
sdcli snap restore_volume -f clpubs-filer1 -volume vol3 -s my_snap
```

The preceding example restores a volume from the Snapshot copy named my_snap on a volume called vol3 that resides on a storage system called clpubs-filer1.

Recovering a cluster from shared LUNs on a SnapMirror destination

Connect to shared LUNs on a SnapMirror destination in order to recover your MSCS cluster.

Before you begin

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

- A SnapMirror replica of the source volume must exist on the destination volume prior to the failure of the physical disk resource.
 - You must know the original drive letters and paths to the shared LUNs on the SnapMirror source volume.
 - You must know the MSCS cluster name.
1. [*Configuring the cluster service to start manually*](#) on page 173
 2. [*Creating a temporary quorum disk*](#) on page 174
 3. [*Starting the cluster service with the -fixquorum option*](#) on page 174
 4. [*Connecting to the new quorum disk*](#) on page 174
 5. [*Connecting to a shared LUN on the SnapMirror destination volume*](#) on page 175

Configuring the cluster service to start manually

In order to recover a cluster from shared LUNs on a SnapMirror destination, you must first configure the cluster service to start manually.

Steps

1. Configure the cluster service to start manually on all nodes of the cluster by performing the following actions on each node of the cluster:
 - a. In the left MMC pane, expand the Services and Applications option, if it is not expanded already.

2. Using the Cluster Administrator in Windows Server 2003, make the newly connected shared disk the quorum disk.
3. Stop the cluster service, then restart the cluster service on all nodes in the cluster.
4. Remove dependencies on all failed physical disk resources, then remove the physical disk resources.

Connecting to a shared LUN on the SnapMirror destination volume

Complete this procedure after you have connected to the new quorum disk.

Steps

1. On the cluster node you used earlier, follow the steps to connect to a LUN, keeping in mind the following information to connect to a LUN:
 - a. When prompted for the LUN path in the **Provide Storage System, LUN Path, and Name** panel, specify or browse to the LUN file in the active file system (not the one in the Snapshot copy) on the SnapMirror destination volume.
 - b. After you specify the LUN path and click **Next**, you see a message that a single file SnapRestore or rapid LUN restore will be performed. Click Yes to continue.
 - c. When prompted for disk type in the **Select a LUN Type** panel, select Shared.
 - d. When prompted for a drive letter in the **Select LUN Properties** panel, select the same drive letter that was being used for the LUN on the SnapMirror source volume.
2. After you have successfully completed the Connect Disk wizard, you see one of the following two error messages. These error messages are expected and do not indicate a problem.

Error message 1:

```
Unable to connect disk. Failure in Mounting volume on the disk. Error:
Could not find the volume mounted for the LUN as there does not seem to
be any new volumes mounted by the Mount Manager
```

This error might also appear in the following form:

```
Unable to connect disk. Failure in connecting to the LUN. Error: Timeout
has occurred while waiting for disk arrival notification from the
operating system.
```

Error message 2:

```
Unable to retrieve a list of LUN snapshots. Error: The device is not
ready.
```

Note: Error message 2 is displayed instead of error message 1 when McAfee NetShield is installed on your Windows server.

Click OK to ignore the error message.

3. Repeat Step 1 and Step 2 for each shared LUN on the cluster.
4. Configure the cluster service to start automatically on the system to which you connected shared LUNs by performing the following actions:
 - a. In the left MMC pane, expand the Services and Applications option, if it is not expanded already.
 - b. Click Services.
 - c. Double-click Cluster Service.
 - d. Select Manual from the Startup Type list.
5. Restore any resource dependencies you removed earlier.

Result

You have connected to the shared LUNs in a SnapMirror destination volume.

After you finish

Use the Cluster Administrator to verify that the cluster is functioning correctly as follows:

- Ensure that all resources are online.
- Perform a “move group” operation from one node to the other and then back to the original node.
- Move the quorum disk from the temporary disk you created in Step 3 back to the original disk.
- Delete the temporary disk.

Unattended SnapDrive installation reference

You can perform unattended installations of SnapDrive for Windows for first time installations and for upgrades.

Next topics

[SnapDrive command line installation syntax](#) on page 177

[SnapDrive command line installation switches](#) on page 178

[SnapDrive unattended installation examples](#) on page 185

SnapDrive command line installation syntax

You can run the SnapDrive for Windows installation package from the command line to perform an unattended installation.

Command syntax

```
snapdrive6.3.exe /s [/x] /v"/qn SWITCH1 [SWITCH2 SWITCH3 ...]"
```

/s Invokes SnapDrive installation in unattended or silent mode.

/x Removes SnapDrive from your system.

Note: SnapDrive does not support unattended removal of versions earlier than 4.2.

/v When directly followed by "/qn", allows you to pass arguments and other SnapDrive installation-specific switches and parameters. These arguments go inside the quotation marks after the /qn.

Note: In the event that you incorrectly enter any of the unattended install command switches, a pop-up dialog box appears displaying the correct switch combination or command usage.

SnapDrive command line installation switches

You can use these command-line switches when you perform an unattended install of SnapDrive for Windows.

Switch descriptions

Switch	Values and Descriptions
SILENT_MODE=	1 Enables SnapDrive to properly execute the unattended install feature. This switch is required and must be set for all unattended installations, including first-time installs, upgrades, and complete uninstalls.

Switch	Values and Descriptions
REINSTALLMODE=	Specifies the type of reinstall mode to be used. v Indicates that the installation should be run from the source package and to cache the local package. Note: Do not use this option for first time installations of SnapDrive. a Reinstalls all SnapDrive files regardless of version, date or checksum value. o Reinstalls SnapDrive files if older versions are present or if files are missing. m Indicates that all SnapDrive required registry entries FROM HKEY_LOCAL_MACHINE and HKEY_CLASSES_ROOT should be rewritten. u Indicates that all SnapDrive required registry entries from HKEY_CURRENT_USER and HKEY_USERS should be rewritten. s Reinstalls all shortcuts and re-caches all icons, overwriting any existing shortcuts and icons.
REINSTALL=	ALL Reinstalls all SnapDrive features.
/Li	filename Specifies that a SnapDrive installation log should be generated.

Switch	Values and Descriptions
SERVER_CORE_SYSTEM=	Specifies whether you are installing on a Windows Server 2008 Server Core configuration. The default value is 0, so this switch is not required unless you are installing on a Server Core system. 0 Specifies that you are not installing on a Server Core system. 1 Specifies that you are installing on a Server Core system. Note: You should use the SERVER_CORE_SYSTEM= switch with only Windows Server 2008 Core Server. You should not use the SERVER_CORE_SYSTEM= switch with Windows Server 2008 R2 Core Server.
LPSM_SERIALNUMBER=	serialnumber Optionally specifies the LUN Provisioning and Snapshot Management license for host-side licensing. If you do not provide this license, SnapDrive will look for a license on the storage system.
INSTALLDIR=	target installation directory Specifies the target installation directory to which SnapDrive will be installed. This switch is only required when installing SnapDrive for the first time.

Switch	Values and Descriptions
SVCUSERNAME=	DOMAIN \username Specifies the domain and username that SnapDrive will use during the unattended install.
SVCUSERPASSWORD=	password Specifies the password for the SVCUSERNAME user.
SVCCONFIRMUSERPASSWORD=	password Confirms the password for the SVCUSERNAME user.
IGNORE_COMPMGMT_RUNNING=	Specifies whether the SnapDrive installation will abort if MMC is open. If no switch is specified, the SnapDrive installation will abort if MMC is open, and a message is displayed indicating that MMC must be closed. 0 Specifies that the SnapDrive installation will abort if MMC is open, and a message is displayed indicating that MMC must be closed. 1 Specifies that the SnapDrive installation will proceed even if MMC is open.
SDW_WEBSRV_TCP_PORT=	port number Specifies which port the SnapDrive WebService should use for Net.Tcp. The default port is 808. Note: This switch is used with new installations only. It is not used for upgrades.
SDW_WEBSRV_HTTP_PORT=	port number Specifies which port the SnapDrive Web Service should use for HTTP. The default port is 4094.

Switch	Values and Descriptions
SDW_WEBSRV_HTTPS_PORT=	port number Specifies which port the SnapDrive Web Service should use for HTTPS. The default port is 4095.
TRANSPORT_SETTING_ENABLE	Specifies whether the transport protocol settings are enabled. Enabled is the default. 0 Disabled 1 Enabled
TRANSPORT_PRT_SELECTION=	Specifies which transport protocol SnapDrive will use. RPC is the default in a new install or major upgrade. 1 RPC 2 HTTP 3 HTTPS
TRANSPORT_PRT_PORT=	port number Specifies which port SnapDrive should use for the HTTP or HTTPS transport protocol. (Only valid if the TRANSPORT_PRT_SELECTION switch is set to 2 or 3.) The default ports are 80 for HTTP and 443 for HTTPS.
TRANSPORT_PROTOCOL_LOGON_USERNAME=	username Specifies the user name that will be used for HTTP or HTTPS authentication. (Only valid if the TRANSPORT_PRT_SELECTION switch is set to 2 or 3.)
TRANSPORT_PROTOCOL_LOGON_PASSWORD=	password Specifies the password that will be used for HTTP or HTTPS authentication. (Only valid if the TRANSPORT_PRT_SELECTION switch is set to 2 or 3.)

Switch	Values and Descriptions
DFM_SERVER_INFO=	hostname Specifies the DFM server name or IP Address.
DFM_SERVER_COMM_PORT_SELECTION=	1 Specifies HTTP as the communication port type. 2 Specifies HTTPS as the communication port type.
DFM_SERVER_COM_PORT=	port Specifies the DFM server communication port. The default for HTTP is 8088. The default for HTTPS is 8488.
DFM_SERVER_USERNAME=	username Specifies the DFM server user name.
DFM_SERVER_PASSWORD=	password Specifies the DFM server password.
SDW_ESXSVR_ENABLE=	Specifies whether the ESX server is enabled. Enabled is the default. 0 Disabled 1 Enabled
ESXIPADDRESS	IP address Specifies the ESX server IP address.
ESXUSERNAME	username Specifies the ESX server user name.
ESXUSERPASSWORD	password Specifies the ESX server password.
ESXCONFIRMUSERPASSWORD	password Confirms the ESX server password.

Switch	Values and Descriptions
SDW_SMVISVR_ENABLE=	1 Enables the option to add SMVI configuration information.
SMVIIPADDRESS=	IP address/ name Specifies the SnapManager for Virtual Interface server IP address or host name.
SMVIPORT=	SMVIPort Specifies the port SnapDrive uses to communicate with the SnapManager for Virtual Infrastructure server.
SDW_HYPERV_ENABLE=	Specifies whether Hyper-V pass-through operations are enabled. Disabled is the default. 0 Disabled 1 Enabled
HYPERV_HOSTNAME=	hostname The hostname of the current Hyper-V parent host.
HYPERV_IP=	IP address The IP address of the current Hyper-V parent host.
HYPERV_COM_PORT=	port The SnapDrive Web Service TCP port of the current Hyper-V parent host.
CUSTOMHELP=	1 Displays usage information for all unattended install switches.

SnapDrive unattended installation examples

These examples show how to run the SnapDrive for Windows installation package from the command line to perform an unattended installation.

Examples of commands used to perform unattended SnapDrive installations

Note: Upgrading from all versions of SnapDrive is considered a major upgrade. Follow the usage examples carefully.

Note: The example provided for a complete first time SnapDrive installation on Windows Server 2008 Server Core should not be used when installing SnapDrive on Windows Server Core 2008 R2 Server Core.

Custom help:	<code>snapdrive6.3.exe /s /v"/qn CUSTOMHELP=1"</code>
Uninstall:	<code>snapdrive6.3.exe /s /x /v"/qn SILENT_MODE=1 /Li SDinstall.log"</code>
Complete first time SnapDrive installation with log:	<code>snapdrive6.3.exe /s /v"/qn SILENT_MODE=1 /Li SDInstall.log LPSM_SERIALNUMBER=serialnumber INSTALLDIR="c:\Program Files\NetApp\SnapDrive\ SVCUSERNAME=domain\username SVCUSERPASSWORD=password SVCCONFIRMUSERPASSWORD=password" SDW_WEBSRV_TCP_PORT=808 SDW_WEBSRV_HTTP_PORT=4098 TRANSPORT_PRT_SELECTION=2 TRANSPORT_PRT_PORT=80 TRANSPORT_PROTOCOL_LOGON_USERNAME=username TRANSPORT_PROTOCOL_LOGON_PASSWORD=password"</code>
Complete first time SnapDrive installation with log on Windows Server 2008 Server Core:	<code>snapdrive6.3.exe /s /v"/qn SILENT_MODE=1 SERVER_CORE_SYSTEM=1 /Li SDInstall.log LPSM_SERIALNUMBER=serialnumber INSTALLDIR="c: \Program Files\NetApp\SnapDrive\ SVCUSERNAME=domain\username SVCUSERPASSWORD=password SVCCONFIRMUSERPASSWORD=password" SDW_WEBSRV_TCP_PORT=808 SDW_WEBSRV_HTTP_PORT=4098 TRANSPORT_PRT_SELECTION=2 TRANSPORT_PRT_PORT=80 TRANSPORT_PROTOCOL_LOGON_USERNAME=username TRANSPORT_PROTOCOL_LOGON_PASSWORD=password"</code>
Major upgrade from SnapDrive installations earlier than 6.3 with log:	<code>snapdrive6.3.exe /s /v"/qn SILENT_MODE=1 /Li SDInstall.log LPSM_SERIALNUMBER=serialnumber SVCUSERNAME=domain\username</code>

```

SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password"
SDW_WEBSRV_HTTP_PORT=4098 TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password"

```

VMware-specific examples

Complete first time SnapDrive installation with log and with ESX server settings disabled:	<pre> snapdrive6.3.exe /s /v"/qn SILENT_MODE=1 /Li <i>SDInstall.log</i> LPSM_SERIALNUMBER=<i>serialnumber</i> INSTALLDIR="c:\Program Files \NetApp\SnapDrive\" SVCUSERNAME=<i>domain\username</i> SVCUSERPASSWORD=<i>password</i> SVCCONFIRMUSERPASSWORD=<i>password</i>" SDW_WEBSRV_TCP_PORT=808 SDW_WEBSRV_HTTP_PORT=4098 TRANSPORT_PRT_SELECTION=2 TRANSPORT_PRT_PORT=80 TRANSPORT_PROTOCOL_LOGON_USERNAME=<i>username</i> TRANSPORT_PROTOCOL_LOGON_PASSWORD=<i>password</i>SDW_ESXSVR_ENABLE=0" </pre>
Complete first time SnapDrive installation with log and with ESX server settings enabled:	<pre> snapdrive6.3.exe /s /v"/qn SILENT_MODE=1 /Li <i>SDInstall.log</i> LPSM_SERIALNUMBER=<i>serialnumber</i> INSTALLDIR="c:\Program Files \NetApp\SnapDrive\" SVCUSERNAME=<i>domain\username</i> SVCUSERPASSWORD=<i>password</i> SVCCONFIRMUSERPASSWORD=<i>password</i>" SDW_WEBSRV_TCP_PORT=808 SDW_WEBSRV_HTTP_PORT=4098 TRANSPORT_PRT_SELECTION=2 TRANSPORT_PRT_PORT=80 TRANSPORT_PROTOCOL_LOGON_USERNAME=<i>username</i> TRANSPORT_PROTOCOL_LOGON_PASSWORD=<i>password</i> ESXIPADDRESS=<i>IPaddress</i> ESXUSERNAME=<i>username</i> ESXUSERPASSWORD=<i>password</i> ESXCONFIRMUSERPASSWORD=<i>password</i>" </pre>

Typical SnapDrive configurations

SnapDrive for Windows supports a variety of configurations for your iSCSI, FC, or MPIO environment.

Next topics

[*SnapDrive iSCSI configurations*](#) on page 187

[*SnapDrive FC configurations*](#) on page 190

[*SnapDrive MPIO configurations*](#) on page 191

SnapDrive iSCSI configurations

SnapDrive for Windows supports several different iSCSI configurations.

Next topics

[*Single host direct-attached to a single storage system using iSCSI*](#) on page 187

[*Single host attached to a single storage system through a GbE switch*](#) on page 188

[*Single host attached to a single storage system through a dedicated switch*](#) on page 188

[*Windows cluster connected to a storage system cluster through a dedicated GbE switch*](#) on page 189

Single host direct-attached to a single storage system using iSCSI

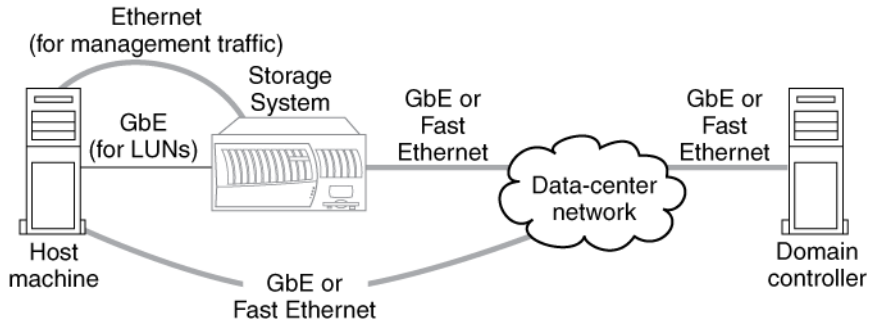
You can configure SnapDrive for Windows to use a GbE crossover cable to attach the host directly to the storage system, an arrangement that minimizes latency and eliminates unwanted network broadcasts.

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

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

Note: Both the storage system and the host must be within the same broadcast domain.

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

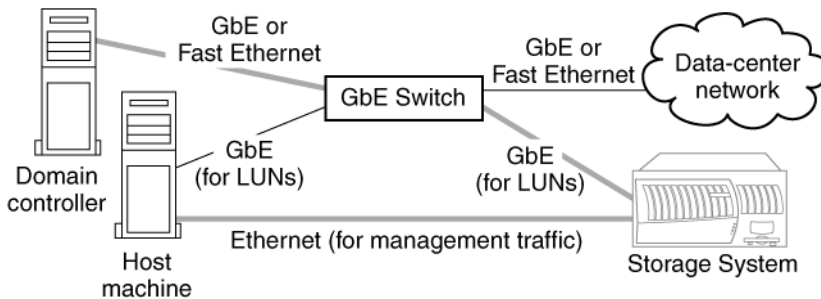


Single host attached to a single storage system through a GbE switch

You can configure SnapDrive for Windows to use a single-homed configuration that places a network switch between the storage system and the host, an arrangement that provides good performance and also segregates host-storage system traffic by directing it through a single pair of switch ports.

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

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



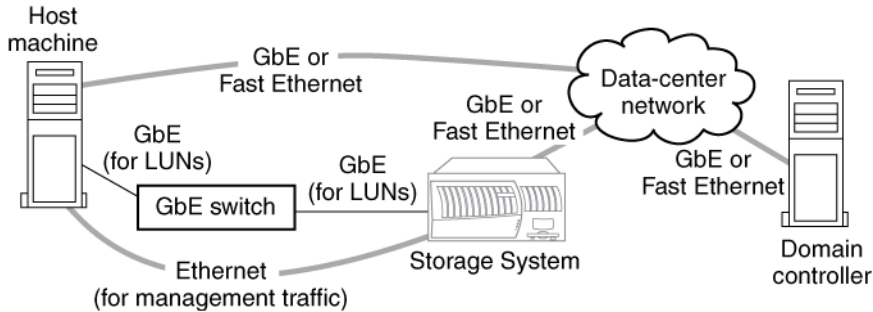
Single host attached to a single storage system through a dedicated switch

You can configure SnapDrive for Windows to use a multihomed configuration with a GbE switch between the storage system and the host, an arrangement that, in addition to providing good performance and segregating host-storage system traffic to the dedicated switch, also minimizes disruptions in situations where network routing configuration changes frequently.

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

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

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



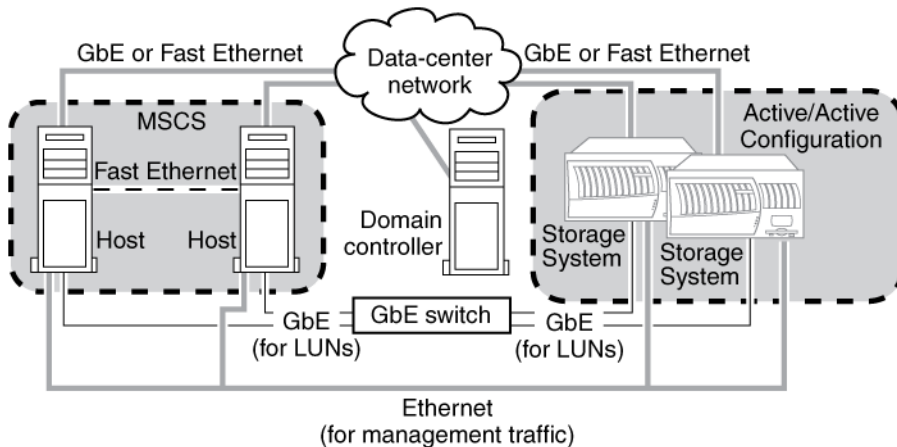
Windows cluster connected to a storage system cluster through a dedicated GbE switch

You can configure SnapDrive for Windows to use both a Windows cluster and a storage system cluster.

The following illustration shows a Windows cluster and storage system cluster with an optional but recommended “private” network that manages internal cluster traffic (rather than data traffic between host and storage system).

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

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



SnapDrive FC configurations

SnapDrive for Windows supports several different FC configurations.

Next topics

[Single host direct-attached to a single storage system using FC](#) on page 190

[Single host attached to a single storage system through an FC switch](#) on page 190

[Windows cluster attached to a storage system active/active configuration through an FC switch](#) on page 191

Single host direct-attached to a single storage system using FC

You can configure SnapDrive for Windows to use a crossover FC cable to attach the host directly to the storage system.

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

- 1 HBA to transfer LUN data between storage system and host
- 1 Fast Ethernet (or GbE) NIC to connect to the data-center fabric

Note: Both the storage system and the host must be within the same broadcast domain.

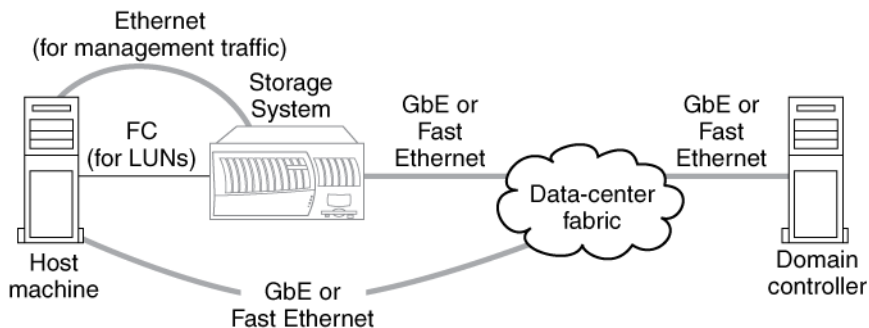


Figure 1: Single host direct-attached to single storage system using FC

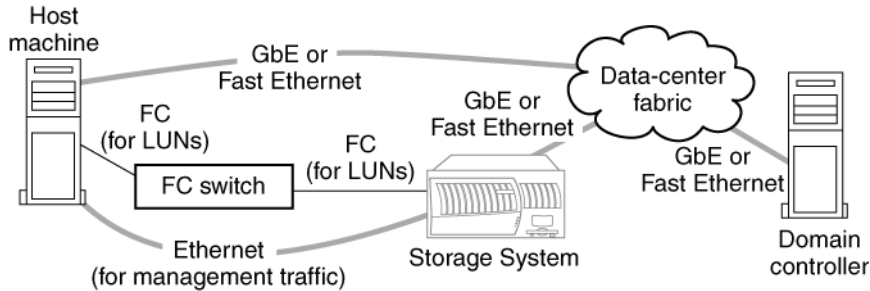
Single host attached to a single storage system through an FC switch

You can configure SnapDrive for Windows to use a dedicated FC switch between the storage system and the host.

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

- 1 HBA to transfer LUN data between storage system and host
- 1 Fast Ethernet (or GbE) NIC to connect to the data-center fabric

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

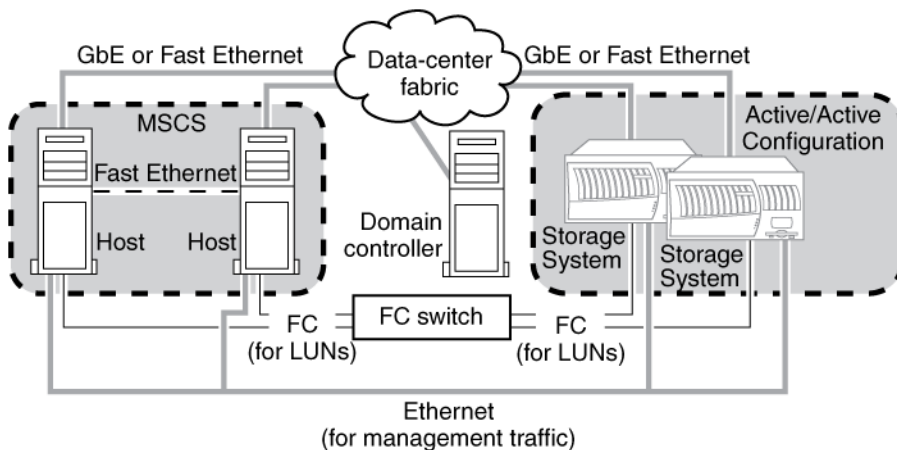


Windows cluster attached to a storage system active/active configuration through an FC switch

You can configure SnapDrive for Windows to use both a Windows cluster and a storage system active/active configuration connected through an FC switch.

The following illustration shows a Windows cluster and a storage system active/active configuration with an optional but recommended dedicated network for internal cluster traffic.

You can also create configurations that connect the Windows cluster to multiple storage systems or storage system active/active configurations.



SnapDrive MPIO configurations

SnapDrive for Windows supports several different MPIO configurations.

If you plan to use MPIO configurations with SnapDrive, you should download Data ONTAP DSM for Windows MPIO from the NOW site at now.netapp.com/. MPIO is not included with the

SnapDrive installation. For more information, see the *Data ONTAP DSM for Windows MPIO Installation and Administration Guide*.

For more information about the latest supported MPIO configurations, see the NOW site at now.netapp.com/.

Next topics

[Single host direct-attached to a single storage system using MPIO](#) on page 192

[Windows cluster attached to a storage system active/active configuration through a GbE switch using MPIO](#) on page 192

[Windows cluster attached to a storage system active/active configuration through an FC switch using MPIO](#) on page 193

Single host direct-attached to a single storage system using MPIO

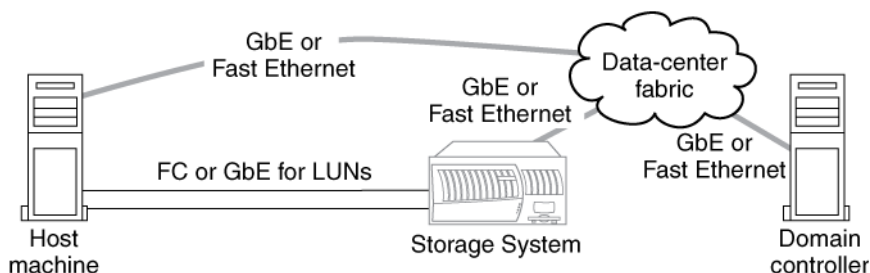
You can configure SnapDrive for Windows to employ FC or iSCSI HBAs to support MPIO between a host and a single direct-attached storage system.

Using FC HBAs, the host and storage system in this configuration each use the following connection hardware:

- 2 FC HBAs to transfer multipathed LUN data between storage system and host
- 1 Fast Ethernet (or GbE) NIC to connect to the data-center fabric

Using iSCSI HBAs or the Microsoft iSCSI Software Initiator, the storage system in this configuration has two GbE adapters, and the host has one or both of the following:

- 2 or more iSCSI HBAs
- The Microsoft iSCSI Software Initiator and 2 GbE NICs



Windows cluster attached to a storage system active/active configuration through a GbE switch using MPIO

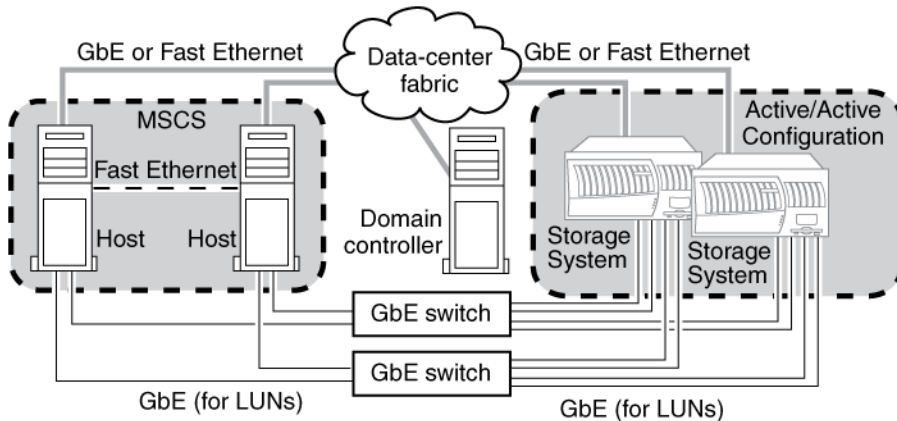
You can configure SnapDrive for Windows to employ both a Windows cluster and a storage system active/active configuration connected through a GbE switch using MPIO.

The following illustration shows a Windows cluster and a storage system active/active configuration with an optional but recommended dedicated network for internal cluster traffic.

Each host in this configuration uses the following connection hardware:

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

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



Windows cluster attached to a storage system active/active configuration through an FC switch using MPIO

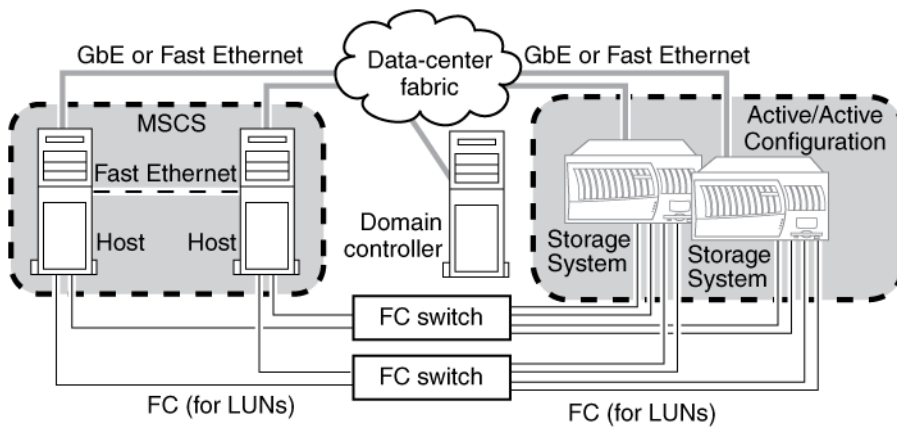
You can configure SnapDrive for Windows to use both a Windows cluster and a storage system active/active configuration connected through an FC switch using MPIO.

The following illustration shows a Windows cluster and a storage system active/active configuration with an optional but recommended dedicated network for internal cluster traffic.

Each host in this configuration uses the following connection hardware:

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

Each storage system configuration requires two dual-port FC adapters and a Fast Ethernet (or GbE) NIC to connect to the data-center fabric. (See your *Data ONTAP Block Access Management Guide for iSCSI and FC* for details.)



Storage system access control reference

Your storage system administrator can use the `AccessControl.xml` file to set a variety of default roles and storage access control operations and descriptions to allow or deny access to resources on a storage system, and use the `ThinProvision.xml` file to enable the creation of thinly provisioned LUNs when using SnapDrive.

Next topics

[Storage system access control operations list](#) on page 195

[Storage system access control roles](#) on page 196

[Storage system access control commands](#) on page 198

[Storage system access control command examples](#) on page 198

Related concepts

[Support for storage system access control](#) on page 42

Storage system access control operations list

You can use these operations in the `AccessControl.xml` file to allow or restrict access to users depending on their assigned roles.

You can use these operations with the default roles provided in the `AccessContol.xml` file, or you can create new roles using one or more of the available operations.

Operation	Descriptions
<code>SD.Config</code>	Allows users to perform all configuration operations.
<code>SD.Config.Read</code>	Allows users to perform only read rights of configuration information on the storage system.
<code>SD.Config.Write:</code>	Allows users to create and modify configuration information on the storage system. For example, a user is allowed to create and modify iGroups, create mappings, and set options on the storage system.
<code>SD.Config.Delete</code>	Allows users to delete any configuration information.
<code>SD.Storage:</code>	Allows users to perform all storage operations.
<code>SD.Storage.Read:</code>	Allows users to list storage system objects. For example, a user can enumerate and read aggregates, volumes, qtrees, LUNs, and files.

Operation	Descriptions
SD.Storage.Write:	Allows users to create and modify storage system objects.
SD.Storage.Delete:	Allows users to delete storage objects.
SD.Snapshot:	Allows users to perform all Snapshot copy operations.
SD.Snapshot.Read	Allows users list Snapshot copies, including archived copies, and objects inside the Snapshot copies.
SD.Snapshot.Delete	Allows users to delete Snapshot copies.
SD.Snapshot.Write:	Allows users to create, rename and modify Snapshot copies.
SD.Snapshot.Restore	Allows users to restore from a Snapshot copy.
SD.Snapshot.Clone	Allows users to clone-related operations such as FlexClone volume operations and LUN clone operations.
SD.Access.None	Denies all access to a storage system.

Storage system access control roles

You can assign roles to a user in the AccessControl.xml file to allow or restrict only certain operations to SnapDrive and storage system resources.

You can use these default roles to restrict access or you can create new roles using the available operation types.

Role	Operations	Descriptions
SD.Admin:	All operations	Allows all SnapDrive operations

Role	Operations	Descriptions
SD.Provision:	SD.Storage.Write SD.Storage.Read SD.Config.Read SD.Config.Write	Allows all LUN provisioning and Snapshot copy operations including create, connect, and map, if the operations are set on the storage system Note: If a LUN is disconnected by a user to whom you have assigned the default SD.Provision role, but the volume on which the LUN resides does not have Storage.Read permission, that user cannot reconnect the LUN from SnapDrive MMC using manual igroup management. This is because without the Storage.Read permission on the storage system, no igroups are listed. In this case, reconnect the LUN using automatic igroup management or sdcli.exe.
SD.Discovery:	SD.Config.Read SD.Storage.Read SD.Snapshot.Read	Allows all operations for discovering volumes, qtrees, igroups, and Snapshot copies
SDBackup:	SD.Snapshot.Read SD.Snapshot.Write	Allows create, replicate, and archive backup operations
SDRestore:	SD.Snapshot.Restore	Allows restore operations from a Snapshot copy or archive
SDNoAccess	SD.Access.None	Denies all access Note: When you use this role, the storage access control tool will not allow other roles to exist.

Storage system access control commands

The storage system access control tool provides several commands that enable you to control what actions a user can perform on a storage system.

The following commands are available in the storage system access control tool:

create	Creates the AccessControl.xml file that contains default operations and roles. The storac.exe tool places the AccessControl.xml file in the storage system /etc directory.
delete	Deletes the AccessControl.xml file after user confirmation. Deleting the AccessControl.xml files disables access control on the storage system.
operation	Lists the SnapDrive operations.
roles	Lists, adds, removes, and modifies both default and user-created roles on the storage system.
user	Enables you to perform the following actions: • List users for whom access rights have been set • Add, remove, and modify access rights for users
dfmrbac	Sets the DFM-RBAC value that determines which RBAC method to use: either DFM or file-based.
storage	Lists the storage system resources for which access rights have been configured.
spacereserve	Enables and disables thin provisioning of LUNs using the value <code>true</code> or <code>false</code> . The <code>true</code> value enables fully provisioned LUNs. The <code>false</code> value enables thinly provisioned LUNs.
host	Enables you to list, add, and remove host access to storage system volumes.
hvol	Lists the volumes a host can access.
help	Provides Help on any storac.exe command or operation
exit	Exits storac.exe

Storage system access control command examples

The examples show some of the commands you can run when you use storacle.exe to manage storage access and to determine space reservation status on volumes.

Launch storacle.exe This example launches the storac tool.

	storac1	
Launch storac1.exe and connect to storage system	This example launches the storac1 tool and connects to the storage system called SYSTEM1.	storac1 -stor SYSTEM1
Disable access control on a storage system	This example disables access control to the root user on the storage system called System1.	delete -stor System1 -user root
Create a new role	This example creates a role called TESTROLE with the ability to list storage system objects.	role add -rn TESTROLE -OPN SD.Storage.Read
Add operations to an existing role	This example adds storage write access to the role called TESTROLE:	role add -rn TESTROLE -OPN SD.Storage.Write
Remove operations from an existing role	This example removes storage read access from the role called TESTROLE:	role remove -rn TESTROLE -OPN SD.Storage.Read
Add user access rights	This example adds the access rights defined by the SDProvision and SDBackup role to the domain user usr1 on the volume volTest on storage system System1.	user add -rsn System1:/vol/volTest -rtype vol -un mydomain\usr1 -RN SDProvision SDBackup
Remove roles assigned to a user for a resource	This example removes only the SDBackup role for the domain user usr1 on the volume volTest on the storage system System1.	user remove -rsn System1:/vol/volvpn -rtype vol -un mydomain\usr1 -RN SDBackup
List resources accessible to a user	This example lists the resources that are accessible by the domain user usr1.	user list -un mydomain\user1
List resources accessible to all users	This example lists the resources that are accessible to all users.	user list
Remove all access rights to a user	This example removes all access rights to the domain user usr1.	user remove -un mydomain\usr1

List storage system resources

This example lists all volumes on the storage system.

```
storage list -rtype vol
```

This example lists all aggregates in the storage system.

```
storage list -rtype aggr
```

List volumes accessible to a host

This example lists storage system volumes accessible by HOST1.

```
hvol list -h HOST1
```

Remove volume access from a host

This example makes the volume volTest inaccessible to the host HOST1.

```
hvol remove -h HOST1 -vol volTest
```

Remove a host entry from a storage system

This example removes the entry for HOST1 from the storage system.

```
host remove -h HOST1
```

Check the current LUN space reservation policy

This example checks the current LUN space reservation policy on the volume vol1 on System1 using the root user to log in to the storage system.

```
spacereserve get -vol vol1 -stor System1 -user root
```

When no protocol type is specified, storac1 uses HTTPS as the default. The default HTTPS port is 443. The default HTTP port is 80.

Enable space reservation

This example enables space reservation on the volume vol1 on System1 by logging on to the storage system as the user root.

```
spacereserve set -vol vol1 -val true -stor System1 -user root
```

Disable space reservation

This example disables space reservation on the volume vol1 on the storage system System1.

```
spacereserve set -vol vol1 -val false -stor System1
```

SnapDrive for Windows to DataFabric Manager role mappings

To enable RBAC to work between SnapDrive for Windows and DataFabric Manager server, the DataFabric Manager server must be configured with predefined SnapDrive roles, capabilities and operations.

SnapDrive for Windows operations map to the DataFabric Manager roles as follows:

SnapDrive operation	Role and capability	Description
disk create	SD.Storage.Write	Enables LUN creation when set at the volume or qtree resource
disk expand	SD.Storage.Write	Enables LUN expansion when set at the disk resource
disk delete	SD.Storage.Delete	Enables LUN deletion when set at the disk resource
disk connect disk disconnect disk disconnect -f	SD.Storage.Write	Enables LUN connect, disconnect, and forced disconnect when set at the disk resource
disk list	SD.Storage.Read	Enables the ability to list all disks on a volume when set at the storage system volume resource
snap list	SD.Snapshot.Read	Enables the ability to list all Snapshot copies when set on a storage system volume resource
snap create	SD.Snapshot.Write	Enables Snapshot copy creation when set on a storage system volume resource
snap restore	SD.Snapshot.Restore	Enables Snapshot copy restoration when set on a storage system volume resource
snap delete	SD.Snapshot.Delete	Enables Snapshot copy deletion when set on volume when set at the storage system volume resource

SnapDrive operation	Role and capability	Description
snap rename	SD.Snapshot.Write	Enables Snapshot copy renaming on a volume when set at the storage system volume resource
snapvault archive	SD.Snapshot.Write	Enables SnapVault archiving when set on a secondary SnapVault volume resource
snapvault snapshot_delete	SD.Snapshot.Delete	Enables deletion of SnapVault Snapshot copies when set on a secondary SnapVault volume resource
snapvault snap_list	SD.Snapshot.Read	Enables the ability to list SnapVault Snapshot copies when set on a secondary SnapVault volume resource
Snapvault verify_configuration	SD.Snapshot.Read	Enables SnapVault configuration verification when set on primary and secondary SnapVault volumes resource
snapvault rename	SD.Snapshot.Write	Enables renaming of SnapVault Snapshot copies when set on the secondary SnapVault volume resource
igroup create	SD.Config.Write	Enables initiator group creation when enables on the storage system resource
igroup rename	SD.Config.Write	Enables renaming of initiator groups when set on the storage system resource
igroup delete	SD.Config.Delete	Enables deletion of initiator groups when set on the storage system resource
igroup list	SD.Config.Read	Enables the ability to list initiator groups when set on the storage system resource

SnapDrive operation	Role and capability	Description
snap mount	Set on the volume for LUN clones:SD.Snapshot.Clone Set on the qtree for LUN clones:SD.Snapshot.Clone Set on the storage system for traditional volume clones:SD.Snapshot.Clone Set on the parent volume for flexible volume clones:SD.Snapshot.Clone Set on the parent for flexible volume clones that are split:SD.Snapshot.Clone SD.Storage.Write	Enables Snapshot copy mounting when set on the specified resources
snapshot unmount	For LUN clones in a volume or qtree:SD.Snapshot.Clone on the volume For volume clones:SD.Snapshot.Clone on the parent volume	Enables unmounting of LUN clones or volume clones on the indicated resources
volume create	SD.Storage.Write	Enables volume creation when set on the aggregate resource
volume rename	SD.Storage.Write	Enables renaming of a volume when set on the volume resource
volume delete	SD.Storage.Delete	Enables deletion of a volume when set on the volume resource
volume list	SD.Storage.Read	Enables the ability to list volumes on a storage system aggregate when set on an aggregate resource
aggregate list	SD.Storage.Read	Enables the ability to list aggregates when set on the storage system resource

SnapDrive command-line reference

The SnapDrive command-line utility, `sdcli.exe`, enables you to perform many of the tasks available in the SnapDrive MMC, as well as some that are only available using the command-line.

Next topics

- [About *sdcli* commands](#) on page 205
- [Configuration commands](#) on page 208
- [License commands](#) on page 209
- [Initiator group management commands](#) on page 210
- [Fractional space reservation monitoring commands](#) on page 212
- [SnapManager for Virtual Infrastructure commands](#) on page 214
- [Space reclamation commands](#) on page 215
- [Preferred IP address commands](#) on page 217
- [iSCSI connection commands](#) on page 218
- [iSCSI initiator commands](#) on page 219
- [LUN commands](#) on page 220
- [Snapshot copy commands](#) on page 228
- [SnapVault commands](#) on page 234
- [DataFabric Manager commands](#) on page 237
- [Transport protocol commands](#) on page 238
- [Virtual server commands](#) on page 240

About `sdcli` commands

Use the SnapDrive for Windows `sdcli` command-line utility to execute SnapDrive commands individually or through automation scripts.

Next topics

- [Executing *sdcli* commands](#) on page 206
- [Common command switches](#) on page 207

Executing sdcli commands

The sdcli commands consist of three input parameters, which must be specified in the correct order, followed by one or more command-line switches. You can specify the command-line switches in any order.

Before you begin

When you use the sdcli command-line utility on a Windows 2008 server, keep the following information in mind:

- You must be logged in as Administrator, or as a user with administrative rights.
- If you log in as a user other than the one used to install SnapDrive, you must update the SnapDrive service credentials with the new user information and restart the SnapDrive service.

About this task

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.

Steps

1. Using a host that has SnapDrive installed, select **Start > Run**.
2. Type
cmd
in the dialog box entry field, and then click **OK**.
3. After the Windows command prompt window opens, navigate to the directory on your host where SnapDrive is installed.

Example

C:

cd \Program Files\NetApp\SnapDrive

4. Enter the individual command you want to run. Make sure to include all input parameters in the proper order and to specify both required and desired command-line switches in any order.

Example

sdcli disk disconnect -d R

Alternatively, enter the name and path of the automation script you want to run.

Example

C:\SnapDrive Scripts\disconnect_R_from_host4.bat

Common command switches

Many of the `sdcli` commands share command-line switches.

Common command-line switches are listed in the following table.

Switch	Description
-d	The drive letter, mount point, volume name, or CSV reparse point of the LUN. If <code>sdcli</code> cannot find the drive letter specified through the <code>-d</code> switch, it displays a list of all LUNs connected to the host.
-D	A list of drive letters or mount points separated by spaces.
-dtype	The drive type (shared or dedicated).
-e	The name of an existing MSCS resource group, which is required only if the LUN is shared among MSCS nodes.
-i	The initiator name. - For FC, the initiator name is the WWPN (World Wide Port Name) for the initiator, which takes the form <code>hh:hh:hh:hh:hh:hh:hh:hh</code>. - For iSCSI, the initiator name takes the form <code>iqn.iSCSI</code> qualified name. For more information on iSCSI node names, see the Block Access Management Guide.
-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 (<code>nnn.nnn.nnn.nnn</code>) 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 FC 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.
-IG	The list of node machine names and existing igroup names, in pairs. One pair is required for dedicated disks. Two pairs are required for shared disks (at least one pair for each cluster node).

Switch	Description
-m	The host on which the operation is executed. You can use an IP address or a machine name to identify the host. Note: When you use an IP address to identify a host, you should use only those IP addresses displayed in the output from the <code>ipconfig /all</code> command rather than those displayed in the output from the <code>sdcli sysconfig list</code> command. Note: Do not specify the -m switch when running an <code>sdcli</code> command on the local host.
-n	The name and description of an MSCS cluster resource group to be created as part of the associated command. This switch is required only if you need to create an MSCS cluster resource group to facilitate the sharing of a LUN among MSCS cluster nodes.
-np	The IP address and port of the network portal on the iSCSI connection target.
-p	The storage system path to the location of the LUN on the storage system. This string takes the following form: <code>storagesystemname:/vol/volname/[qtree]/lun</code> for a storage system path.
-z	Specifies the size (in megabytes) of a new LUN—or the number of megabytes by which an existing LUN is to be expanded. The minimum size for MBR partition-style LUNs is 32 MB and the minimum for GPT style LUNs is 64 MB. The maximum sizes vary according to the remaining available space in your volume.

Note: Switches that apply to just one command appear with those commands in the sections that follow.

Configuration commands

The `sdcli` utility provides command-line support for viewing SnapDrive configuration information.

The `sysconfig list` command

The `sysconfig list` command displays the SnapDrive configuration information for your host.

Syntax for this command is:

```
sdcli sysconfig list
```

License commands

The `sdcli` utility provides command-line support for SnapDrive license operations.

Next topics

[The `license set` command](#) on page 209

[The `license list` command](#) on page 209

[The `license remove` command](#) on page 209

The license set command

`license set` sets the license key for the specified module.

Syntax for this command is:

```
sdcli license set -module ModuleName -key LicenseKey
```

Example

```
sdcli license set -module LPSM -key ABCDEFGHIJKLMN
```

The license list command

`license list` displays all SnapDrive licenses installed.

Syntax for this command is:

```
sdcli license list
```

The license remove command

`license remove` removes an existing server license.

Syntax for this command is:

```
sdcli license remove -module ModuleName
```

Example

```
sdcli license remove -module LPSM
```

Initiator group management commands

The `sdcli` utility provides command-line support for initiator group management.

Next topics

[The `igroup list` command](#) on page 210

[The `igroup create` command](#) on page 210

[The `igroup rename` command](#) on page 211

[The `igroup delete` command](#) on page 211

The `igroup list` command

The `igroup list` command displays all igroups on a storage system that have initiators on the local host or, if specified, a remote host.

Syntax for this command is:

`sdcli igroup list [-m MachineName] -f StorageSystem`

`-f` specifies the storage system name or IP address for which the igroups will be listed.

Examples

`sdcli igroup list -f 172.17.167.45`

The preceding example displays the igroup list for the storage system with the IP address 172.17.167.45.

`sdcli igroup list -m server3 -f v34filer`

The preceding example displays the igroup list for the storage system v34filer, which has initiators on the remote host server3.

The `igroup create` command

The `igroup create` command enables you to create a new igroup.

Syntax for this command is:

`sdcli igroup create [-m MachineName] -f StorageSystem -I NodeName InitiatorName -ig groupName`

`-I` lists the machine name and initiator name in pairs.

Note: A new igroup is created for only one machine, so you must specify the same machine name for each pair.

`-ig` specifies the name of the igroup you are creating.

Example

```
sdcli igroup create -f v34filer -I server3 10:00:00:00:c9:48:c9:5d  
server3 10:00:00:00:c9:48:c9:5e -ig v3group1
```

The preceding example creates a new igroup called v3group1 on a storage system called v34filer for two initiators, 10:00:00:00:c9:48:c9:5d and 10:00:00:00:c9:48:c9:5e, on a host called server3.

The igroup rename command

The `igroup rename` command enables you to rename an existing igroup.

Syntax for this command is:

```
sdcli igroup rename [-m MachineName] -f StorageSystem -ig groupName -igNew  
igroupNewName
```

`-ig` specifies the name of the existing igroup you are renaming.

`-igNew` specifies the new name of the igroup.

Example

```
sdcli igroup rename -f 172.17.167.45 -ig v3group1 -igNew v3group1fc
```

The preceding example renames an igroup from v3group1 to v3group1fc on a storage system with the IP address 172.17.167.45.

The igroup delete command

The `igroup delete` command enables you to delete an existing igroup if there is no LUN mapped to it.

Syntax for this command is:

```
sdcli igroup delete [-m MachineName] -f StorageSystem -ig groupName
```

`-ig` specifies the name of the igroup you want to delete.

Example

```
sdcli igroup delete -f 172.17.167.45 -ig v3group1fc
```

The preceding example deletes the igroup named v3group1fc from the storage system with the IP address 172.17.167.45.

Fractional space reservation monitoring commands

The `sdcli` utility provides command-line support for fractional space reservation monitoring.

Next topics

[The `spacemon list` command](#) on page 212

[The `spacemon set` command](#) on page 212

[The `spacemon snap\_delta` command](#) on page 213

[The `spacemon snap\_reclaimable` command](#) on page 213

[The `spacemon vol\_info` command](#) on page 214

[The `spacemon delete` command](#) on page 214

The `spacemon list` command

The `spacemon get` command displays the space reservation monitoring settings for the specified host.

Syntax for this command is:

```
sdcli spacemon list {-m MachineName}
```

MachineName is the machine name on which you want to execute the command. If no machine name is specified, the command is executed on the local machine.

The `spacemon set` command

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

Syntax for this command is:

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

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

Storage System is the name of the storage system on which the LUNs reside.

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

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

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

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

MachineName is the machine name on which you want to execute the command. If no machine name is specified, the command is executed on the local machine.

Example

```
sdcli spacemon set -mi 30 -f controller1 -vn testvol -rap 90 -roc 500mb -ccs true
```

The preceding example shows that fractional space reservations will be monitored every 30 minutes on the volume named testvol on controller1. The threshold for testvol is 90 percent of the reserved available percentage and the threshold for rate of change is 500 MB. SnapDrive will verify storage system and volume names and that space is available for Snapshot copies to be created.

The spacemon snap_delta command

The `spacemon snap_delta` command displays the rate of change between two Snapshot copies or between a Snapshot copy and the active file system of the storage system volume.

Syntax for this command is:

```
sdcli spacemon snap_delta -f Storage System -vn Volume Name -s1 snapshot1 -s2 snapshot2 {-m MachineName}
```

Storage System is the name of the storage system on which the volume exists.

Volume Name is the name of the volume for which you want to display the snap delta.

snapshot1 is the name of the Snapshot copy you want to compare with either a second Snapshot copy or with the active file system.

snapshot2 is name of the second Snapshot copy.

MachineName is the machine name on which you want to execute the command. If no machine name is specified, the command is executed on the local machine.

The spacemon snap_reclaimable command

The `spacemon snap_reclaimable` command displays the space that can be reclaimed by deleting a Snapshot copy.

Syntax for this command is:

```
sdcli spacemon snap_reclaimable -f Storage System -vn Volume Name -s snapshot
```

Storage System is the name of the storage system on which the volume exists.

Volume Name is the name of the volume on which the Snapshot copy resides.

snapshot is the name of the Snapshot copy for which you want to view reclaimable space.

The spacemon vol_info command

The spacemon vol_info command displays information about fractional space reserved volumes.

Syntax for this command is:

```
sdcli spacemon vol_info {-m MachineName}
```

MachineName is the machine on which you want to execute the command. If no machine name is specified, the command is executed on the local machine.

Note: Output for the spacemon vol_info command is displayed in XML format.

The spacemon delete command

The spacemon delete command enables you to delete the fractional space reservation monitor settings for the specified storage system volume.

Syntax for this command is:

```
sdcli spacemon delete -f Storage System -vn Volume Name {-m MachineName}
```

Storage System is the name of the storage system on which the volume exists.

Volume Name is the name of the volume from which you want to delete fractional space reservation settings.

SnapManager for Virtual Infrastructure commands

The sdcli utility provides command-line support for managing communication between SnapDrive for Windows and SnapManager for Virtual Infrastructure.

Next topics

[The smvi_config list command](#) on page 214

[The smvi_config set command](#) on page 215

[The smvi_config delete command](#) on page 215

The smvi_config list command

The smvi_config list command displays the

Syntax for this command is:

```
sdcli smvi_config list
```

Enter an example to illustrate your reference here (optional).

The **smvi_config set** command

The **smvi_config set** command to set the SnapManager for Virtual Interfaces server IP address and port.

Syntax for this command is:

```
sdcli smvi_config set -host host [-smviport SMVI port number] [-port SnapDrive port] [-m MachineName]
```

-host specifies the SMVI server name or IP address

-smviport specifies the SMVI service port number you use to communicate with SMVI. The default port is 8043.

-port specifies the Web service port number you use to communicate with SnapDrive. The default port is 808.

The **smvi_config delete** command

The **smvi_config delete** command deletes the specified SMVI server entry.

Syntax for this command is:

```
sdcli smvi_config delete [-m MachineName] [-port SnapDrive port]
```

-port specifies the Web service port number you use to communicate with SnapDrive. The default port is 808.

Enter an example to illustrate your reference here (optional).

Space reclamation commands

The **sdcli** utility provides command-line support for space reclamation operations.

Next topics

[*The spacereclaimer start command*](#) on page 215

[*The spacereclaimer stop command*](#) on page 216

[*The spacereclaimer analyze command*](#) on page 216

[*The spacereclaimer status command*](#) on page 217

The **spacereclaimer start** command

The **spacereclaimer start** command starts the SnapDrive space reclamation process.

Syntax for this command is:

```
sdcli spacereclaim start [-m MachineName] -d MountPoint [-t TimetoRun]
```

-d *MountPoint* specifies the LUN mount point, volume name, or CSV reparse point on which you want to start Space Reclaimer.

-t *TimetoRun* specifies the amount of time Space Reclaimer will run on the specified LUN. Specify a time from 1 to 10080 minutes (7 days).

Note: Space Reclaimer will run even if the analyzer determined there is no space to reclaim.

Example

```
sdcli spacereclaim start -d C:\ClusterStorage\Volume8
```

The preceding example starts the space reclamation process by specifying the CSV reparse point of a CSV disk.

The spacereclaim stop command

The `sdcli spacereclaim stop` command stops the space reclamation process.

Syntax for this command is:

```
sdcli spacereclaim stop [-m MachineName] -d MountPoint
```

-d *MountPoint* specifies the LUN mount point, volume name, or CSV reparse point on which you want to stop Space Reclaimer.

Example

```
sdcli spacereclaim stop -d \\?\Volume{0944ca87-be05-45ad-8606-ba13ee7388a0}\
```

The preceding example stops the space reclamation process on a CVS volume.

The spacereclaim analyze command

The `sdcli spacereclaim analyze` command checks whether space reclamation is needed for the LUN specified.

Syntax for this command is:

```
sdcli spacereclaim analyze [-m MachineName] -d MountPoint
```

-d *MountPoint* specifies the LUN mount point, volume name, or CSV reparse point on which you want to analyze.

The spacereclaimer status command

The `spacereclaimer status` command displays the space reclamation status for the LUN specified.

If you specified a time to run when you started Space Reclaimer, the status displays the number of minutes remaining. If no time was specified, the status displays the percentage of space remaining for space reclamation.

Syntax for this command is:

`sdcli spacereclaimer status [-m MachineName] [-D MountPointList]`

-DMountPointList specifies a list of LUN mount points. This list is optional. If no mount points are specified, SnapDrive displays the status for all Space Reclaimer operations.

Preferred IP address commands

The `sdcli` utility provides command-line support for managing preferred storage system IP addresses.

Next topics

[The preferredIP set command](#) on page 217

[The preferredIP list command](#) on page 217

[The preferredIP delete command](#) on page 218

The preferredIP set command

The `preferredIP set` command sets the SnapDrive preferred IP address for the specified storage system.

Syntax for this command is:

`sdcli preferredIP set -f Storage System -IP PreferredIPAddress`

Example

`sdcli preferredIP set -f Storage1 -IP 172.18.53.94`

The preceding example sets the SnapDrive preferred IP address for the storage system named Storage1 to 172.28.53.94.

The preferredIP list command

The `preferredIP list` command displays the storage system names and IP addresses that you set as the preferred IP addresses for SnapDrive to use for management traffic.

Syntax for this command is:

```
sdcli preferredIP list
```

The preferredIP delete command

The `preferredIP delete` command deletes the preferred IP address for the specified storage system.

Syntax for this command is:

```
sdcli preferredIP delete -f Storage System
```

iSCSI connection commands

The `sdcli` utility provides command-line support for managing connections to iSCSI targets.

Next topics

[The `iscsi\_target disconnect` command](#) on page 218

[The `iscsi\_target list` command](#) on page 218

The iscsi_target disconnect command

The `iscsi_target disconnect` command disconnects the specified iSCSI initiator from the specified iSCSI target on all portals.

Syntax for this command is:

```
sdcli iscsi_target disconnect -t TargetName
```

Example

```
sdcli iscsi_target disconnect -t iqn.1992.08.com.netapp:sn.33604307
```

The preceding example disconnects the specified iSCSI target.

The iscsi_target list command

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

Syntax for this command is:

```
sdcli iscsi_target list {-f Storage System | -i InitiatorPortName}
```

`-f` displays all targets on the specified storage system.

Example

```
sdcli iscsi_target list -f Storage2
```

The preceding example lists all the iSCSI targets on the Storage2 storage system, as well as all portals those targets are available through or connected to.

iSCSI initiator commands

The `sdcli` utility provides command-line support for managing iSCSI initiators.

Next topics

[The `iscsi\_initiator list` command](#) on page 219

[The `iscsi\_initiator establish\_session` command](#) on page 219

[The `iscsi\_initiator terminate\_session` command](#) on page 220

The `iscsi_initiator list` command

The `iscsi_initiator list` command displays a list of all iSCSI sessions on the specified machine.

Syntax for this command is:

```
sdcli iscsi_initiator list {-m MachineName} -s
```

MachineName is the machine name on which you want to execute the command. If no machine name is specified, the command is executed on the local machine.

-s enumerates the iSCSI sessions.

The `iscsi_initiator establish_session` command

The `iscsi_initiator establish_session` command establishes a session with a target using the specified HBA.

Syntax for this command is:

```
sdcli iscsi_initiator establish_session {-m MachineName} {-h HBA_ID} {-hp  
HBA Portal ID} -t TargetName -np IPAddress IPPort {-c CHAPName  
CHAPPassword}
```

-h*HBA_ID* is used to establish the iSCSI session. The HBA ID can be obtained by using the `sdcli sysconfig list` command.

-hp*HBA Portal ID* is used to specify the portal on the iSCSI HBA to be used to establish the iSCSI session. The HBA Portal ID can be obtained by using the `sdcli sysconfig list` command.

-t *TargetName* is the name of the iSCSI target.

-np*IP Address* *IPPort* specify the IP address and IP port of the network portal on the target. The IP Port can be obtained by using the `sdcli iscsi_initiator list` command.

Example

```
sdcli iscsi_initiator establish_session -h 0 -t iqn.1992-8.com.netapp:maya -np 172.18.53.94 3260
```

The preceding example establishes an iSCSI session with the specified target using the specified HBA ID.

The iscsi_initiator terminate_session command

The `iscsi_initiator terminate_session` command terminates the session.

Syntax for this command is:

```
sdcli iscsi_initiator terminate_session {-m MachineName} -s Session_ID
```

MachineName is the machine name on which you want to execute the command. If no machine name is specified, the command is executed on the local machine.

-sSession_ID is the session ID of the session you want to terminate.

Example

```
sdcli iscsi_initiator terminate_session -s 0xffffffff868589cc-0x4000013700000006
```

The preceding example terminates the specified iSCSI session on the local machine.

LUN commands

The `sdcli` utility provides command-line support for managing LUNs in SnapDrive.

Next topics

[The disk create command](#) on page 221

[The disk connect command](#) on page 222

[The disk delete command](#) on page 223

[The disk disconnect command](#) on page 223

[The disk resize command](#) on page 224

[The disk expand command](#) on page 224

[The disk add_initiator command](#) on page 225

[The disk remove_initiator command](#) on page 225

[The disk list command](#) on page 226

[The disk add_mount command](#) on page 227

[The disk remove_mount command](#) on page 227

The disk create command

The `disk create` command creates a new LUN.

Syntax for this command is:

```
sdcli disk create [-m MachineName] -d MountPoint -p LUNpath -z DriveSize [-rs Reserve Snapshot Space y | n] [-I NodeMachineName InitiatorName +] | [-IG NodeMachineName GroupName +] -dtype {shared | dedicated} [-ds "datastore name" {[-e "ResourceGroupName" ] | [-n "ResourceGroupName" "ResourceGroupDesc"]} | [-csv ]] -port "PortNumber" -passthrough
```

-rs enables you to limit the maximum disk space of the LUN you are creating to allow for at least one Snapshot copy on the volume.

-ds enables you to specify the name of a VMFS datastore on which to store the VMDK file if you are creating a LUN on an ESX server guest OS. When the -ds option is not specified, the VMDK file is stored by default on the same VMFS datastore as the virtual machine. If the virtual machine resides on an NFS datastore, you must specify a VMFS datastore for the VMDK file.

-e enables you to specify the name of an existing resource group.

-n enables you to specify the name of a new resource group.

-csv enables you to add a shared disk to a cluster shared volume.

-passthrough enables you to dynamically add a pass-through disk. This option is only applicable when a Hyper-V virtual machine is present.

Examples

```
sdcli disk create -dtype dedicated -z 1024 -p storage2:/vol/  
sd_vds_only/mktng.lun -d R -I host3 10:00:00:00:C9:2B:FD:12
```

The preceding example creates a dedicated, 1-GB LUN named `mktng.lun` in the `storage2` volume named `sd_vds_only`. Next, it connects this LUN to the host as drive `R`.

```
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
```

The preceding example creates a shared, 4-GB LUN on `host4` (the local machine running the `sdcli` command) and maps it to drive `R`, using a pair of initiators.

```
sdcli disk create -d T -p rlabf6:/vol/vol1_nfs/a -z 65MB -IG vmware229  
igroup_fcp -dtype dedicated -ds "big guy"
```

The preceding example creates a 65-MB RDM LUN in the NFS volume named `vol1_nfs`, and maps the LUN to drive `T`. The VMFS datastore named "big guy" is specified to store the VMDK file.

The disk connect command

The `disk connect` command connects a LUN to a host by mapping the LUN to a Windows drive letter.

Syntax for this command is:

```
sdcli disk connect [-m MachineName] -p LUNpath -d MountPoint [-I NodeMachineName InitiatorName ...] | [-IG NodeMachineName GroupName ...] -  
dtype {shared | dedicated} -ds "datastore name" {[-e "ResourceGroupName"] |  
[-n "ResourceGroupName" "ResourceGroupDesc"] | [-csv]} [-c "ClusterName"] -  
port PortName -passthrough
```

-ds enables you to specify the name of a VMFS datastore on which to store the VMDK file if you are creating a LUN on an ESX server guest OS. When the -ds option is not specified, the VMDK file is stored by default on the same VMFS datastore as the virtual machine. If the virtual machine resides on an NFS datastore, you must specify a VMFS datastore for the VMDK file.

-csv enables you to add a shared disk to a cluster shared volume.

-passthrough enables you to dynamically connect a pass-through disk. This option is only applicable when a Hyper-V virtual machine is present.

Examples

```
sdcli disk connect -d s -dtype shared -p storage2:/vol/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 in the storage2 volume `sd_vds_only` and named `mktng.lun`, which belongs to the MSCS cluster resource group `tech_mktng` on the `mktng` cluster.

```
sdcli disk connect -d T -p rlabf6:/vol/vol1_nfs/a -z 65MB -IG  
vmware229 igroup_fcp -dtype dedicated -ds "big guy"
```

The preceding example connects an RDM LUN on the NFS volume named `vol1_nfs`. The VMFS datastore named "big guy" is specified to store the VMDK file.

```
sdcli disk connect -p ab-270-2:/vol/sdw_vol1/csvLun12 -I CLAB-A9-8  
iqn.1991-05.com.microsoft:clab-a9-8.sddev.netapp.com CLAB-A9-7 iqn.  
1991-05.com.microsoft:clab-a9-7.sddev.netapp.com -dtype shared -csv
```

The preceding example connects a CSV LUN called `csvLun12` as a shared disk to the cluster.

The disk delete command

The `disk delete` command deletes a LUN. The LUN must be connected (mapped to a Windows drive letter or mount point) for the command to succeed.

Syntax for this command is:

```
sdcli disk delete [-m MachineName] {-p LUNpath | -d MountPoint}
```

Example

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

The preceding example deletes the LUN `mktng.lun` from the `sd_vds_only` volume on the storage system identified by the IP address `133.25.61.62`.

```
sdcli disk delete -d \\?\Volume{f1816466-f1d8-4b96-b547-2ce12415aee4}\
```

The preceding example specifies the CSV volume name to delete a CSV disk.

```
sdcli disk delete -d C:\ClusterStorage\Volume8
```

The preceding example specifies the CSV repare point to delete a CSV disk.

The disk disconnect command

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

Note: You must make sure that the LUN you are disconnecting is not monitored with the Windows Performance Monitor (`perfmon`).

Syntax for this command is:

```
sdcli disk disconnect [-m MachineName] {-p LUNpath | -d MountPoint} [-f]
```

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

Example

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

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

```
sdcli disk disconnect -p \\storage2\sd_vds_only\mktng.lun -f
```

The preceding example forces disconnection of the LUN `mktng.lun`, which is in the `sd_vds_only` volume on `storage2`. Because the `-f` switch is being used, all open files in the LUN might be lost or corrupted.

The disk resize command

The `disk resize` command increases or decreases the disk by a user-specified size, as long as that figure falls within the SnapDrive-specified minimum and maximum values.

Syntax for this command is:

```
sdcli disk resize [-m MachineName] {-p LUNpath | -d MountPoint} -z DriveSizeIncrement
```

DriveSizeIncrement is the amount by which you want to increase or decrease the size of the disk. When decreasing the size of the disk, use a dash (-) before the amount to indicate a negative value. You can specify a postfix of MB, GB, or TB. If no postfix is specified, the default is MB.

Examples

```
sdcli disk resize -d G: -z -500
```

The preceding example shrinks the size of the disk mapped to "G" by 500 megabytes.

```
sdcli disk resize -d P: -z 1GB
```

The preceding example increases the LUN 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.)

```
sdcli disk resize -d \\?\Volume{f1816466-f1d8-4b96-b547-2ce12415aee4}\ -z +100
```

The preceding example increases a CSV disk by 100 MB using the CSV volume name.

The disk expand command

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

Syntax for this command is:

```
sdcli disk expand [-m MachineName] {-p LUNpath | -d MountPoint} -z DriveSizeIncrement [-rs Reserve Snapshot copy space {y|n}]
```

-z *DriveSizeIncrement* is the amount by which you want to expand the disk. You can specify a postfix of MB, GB, or TB. If no postfix is specified, the default is MB.

-rs enables you to limit the maximum disk space for the disk you are expanding to allow for at least one Snapshot copy on the volume. This option is recommended.

Example

```
sdcli disk expand -d p -z 1GB
```

The preceding example increases the LUN 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.)

```
sdcli disk expand -d C:\ClusterStorage\Volume8 -z 100
```

The preceding example expands a CSV disk by 100 MB on the CSV reparse point C:\ClusterStorage\Volume8.

The disk add_initiator command

The disk add_initiator adds a new initiator to a LUN.

Syntax for this command is: **sdcli disk add_initiator [-m**

MachineName] {-p LUNpath | -d MountPoint} -i InitiatorPortName

Examples

```
sdcli disk add_initiator -d E -i 21:00:00:e0:8b:85:19:ba
```

The preceding example adds an initiator to a LUN mapped to drive E: on the SnapDrive host from which the sdcli command was executed.

```
sdcli disk add_initiator -p \\sdwatf2\sdwatf2_vol1\sdwath2_EEE.lun -i 21:00:00:e0:8b:85:19:ba
```

The preceding example adds an initiator to a LUN located at the path \sdwatf2\sdwatf2_vol1\sdwath2_EEE.lun on the SnapDrive host from which the sdcli command was executed.

```
sdcli disk add_initiator -d C:\ClusterStorage\Volume4 -i 50:0a:09:80:85:f4:69:37
```

The preceding example specifies the CSV reparse point C:\ClusterStorage\Volume4 to add an initiator to a CSV disk.

The disk remove_initiator command

The disk remove_initiator command removes an initiator from the specified LUN.

Syntax for this command is:

```
sdcli disk remove_initiator [-m MachineName] {-p LUNpath | -d MountPoint} -i InitiatorPortName
```

Examples

```
sdcli disk remove_initiator -d E -i 21:00:00:e0:8b:85:19:ba
```

The preceding example removes an initiator from a LUN mounted on drive letter “E:” on the SnapDrive host running the sdcli command.

```
sdcli disk remove_initiator -p \\sdwatf2\sdwatf2_vol1\sdwath2_EEE.lun  
-i 21:00:00:e0:8b:85:19:ba
```

The preceding example removes an initiator on a LUN located at the path \sdwatf2\sdwatf2_vol1\sdwath2_EEE.lun on the SnapDrive host from which the sdcli command was executed.

```
sdcli disk remove_initiator -d \\?\Volume{24cd94c5-  
d201-4474-9246-2ad491b155ea}\ -i 50:0a:09:80:85:f4:69:37
```

The preceding example specifies the CSV volume name \\?\Volume{24cd94c5-d201-4474-9246-2ad491b155ea}\ to remove an initiator from a CSV disk.

The disk list command

The disk list command displays a list of all the LUNs connected to the host.

Syntax for this command is:

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

Example

```
sdcli disk list
```

The preceding example lists all the SnapDrive LUNs mapped to drive letters on the local host. The disk list command also provides the following information for each LUN:

- LUN path (storage system name, sharename, virtualdiskfilename, and might also include qtree name)
- Storage System
- Storage System Path (storage system-side path, which includes volume name and LUN name)
- Hyper-V VHD present (a Hyper-V VHD exists)
- Hyper-V VM name
- Type
- Disk serial number
- Backed by Snapshot copy (if this is a LUN in a Snapshot copy, this displays the storage system-side path to the Snapshot copy)
- Shared (whether the disk is dedicated or shared)
- CSV disk
- BootOrSystem Disk
- SCSI port
- Bus
- Target
- LUN
- Readonly

- Disk size (in megabytes)
- SnapMirror source
- SnapVault primary
- Disk Partition Style (either MBR or GPT)
- Clone Split Restore status
- Disk ID
- Volume name
- Mount points (the drive letter and path to which the LUN is mapped on the host)
- CSV reparse point
- IP Addresses (IP addresses on the target storage system)
- Initiator name

Note: If you are using ESX 3.5, the initiator name field might be blank for RDM LUNs.

The disk add_mount command

The disk add_mount command adds a volume mount point.

Syntax for this command is:

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

Volume Name is the name of the volume that you are trying to add or move. The volume name can be located in the output from the disk list command.

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

-create_folder indicates that a folder should be created for the new mount point if one does not already exist.

Example

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

The disk remove_mount command

The disk remove_mount command removes a volume mount point or drive letter.

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

Syntax for this command is:

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

Snapshot copy commands

The sdcli utility provides command-line support for managing Snapshot copies of SnapDrive LUNs.

Next topics

[The snap create command](#) on page 228

[The snap delete command](#) on page 229

[The snap list command](#) on page 229

[The snap mirror_list command](#) on page 230

[The snap mount command](#) on page 230

[The snap rename command](#) on page 231

[The snap restore command](#) on page 231

[The snap unmount command](#) on page 232

[The snap update_mirror command](#) on page 233

[The snap restore_volume_check command](#) on page 233

[The snap restore_volume command](#) on page 234

The snap create command

The snap create command creates a new Snapshot copy of the specified LUNs on the SnapDrive system.

Syntax for this command is:

```
sdcli snap create [-m MachineName] -s SnapshotName -D MountPointList  
[. . .] [-x]
```

-x causes data to be flushed and consistent Snapshot copies to be created only for the drives and mount points specified by the -D switch. Otherwise, SnapDrive flushes data and creates consistent Snapshot copies for all LUNs connected to the host and residing on storage system volumes.

Note: Snapshot copies are created at the volume level. When a Snapshot copy is created using -x with the -D switch, Snapshot copies are also created for any additional disks mapped to the host that reside on the same volumes as the disks specified. Snapshot copies for the unspecified disks are dimmed in the SnapDrive MMC because they are inconsistent.

Example

```
sdcli snap create -s Jun_13_03 -D j k l
```

The preceding example creates a Snapshot copy named Jun_13_03 for each volume containing one or more of the LUNs mapped to the specified drives (that is, J:, K:, and L:). The Snapshot copies created are consistent for all LUNs contained by those volumes.

```
sdcli snap create -s csvLun11_051109 -D C:\ClusterStorage\Volume8
```

The preceding example creates a Snapshot copy named csvLUN11_051109 on the CSV reparse point C:\ClusterStorage\Volume8.

The snap delete command

The `snap delete` command deletes an existing Snapshot copy.

Note: You must make sure that the LUN whose Snapshot copy you are deleting is not being monitored with the Windows Performance Monitor (perfmon)

Syntax for this command is:

```
sdcli snap delete [-m MachineName] -D MountPointList [. . .] -s  
SnapshotName
```

Example

```
sdcli snap delete -D k -s Jun_14_09
```

The preceding example deletes the Snapshot copy named Jun_14_09 that is associated with the LUN mapped to K: on the local host.

```
sdcli snap delete -d \\?\Volume{239889f5-3a36-4993-b957-0a85f56cab45}\  
-s csvLun11_051109_new
```

The preceding example deletes the Snapshot copy named csvLun11_051109_new from the CSV volume \\?\Volume{239889f5-3a36-4993-b957-0a85f56cab45}.

The snap list command

The `snap list` command lists all the Snapshot copies that exist for the specified LUN.

Syntax for this command is:

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

MountPoint is a drive letter, mount point path, volume name, or CSV reparse point for the LUN.

Example

```
sdcli snap list -d j
```

The preceding example displays all the Snapshot copies that exist for the volume containing the LUN mapped to “J:” on the local host.

The snap mirror_list command

The `snap mirror_list` command displays the SnapMirror relationships associated with the SnapMirror source volume, including the SnapMirror source storage system, volume, and Snapshot copy; the destination storage system and volume; the current state of the SnapMirror relationship; and whether FlexClone volumes can be created on the destination to allow mirror verification without breaking the mirror.

Syntax for this command is:

```
sdcli snap mirror_list -d MountPoint
```

MountPoint is a drive letter, mount point path, volume name, or CSV reparse point of the SnapMirror source drive.

Example

```
C:\Program Files\NetApp\SnapDrive>sdcli snap mirror_list -d e  
  
1 SnapMirror destination(s) Source: andes-1:s Snapshot:  
andes-2(0084186538)_d.27 Destination: andes-2:d Snapmirrored  
[FlexClone Success]
```

The operation completed successfully.

The preceding example displays the SnapMirror relationship between source drive E: on the storage system volume andes-1 and the destination storage system volume andes-2. The source has one Snapshot copy named andes-2(0084186538)_d.27. FlexClone volumes are enabled on the destination.

The snap mount command

The `snap mount` command mounts a Snapshot copy of a LUN. Snapshots are always mounted in read/write mode.

Syntax for this command is:

```
sdcli snap mount [-m MachineName] [-r LiveMachineName] -k LiveMountPoint -s  
SnapshotName -d MountPoint
```

LiveMachineName refers to the name of the host connected to the LUN in the active file system. When left unspecified, `-r` defaults to the local host.

Note: When using this option to mount a Snapshot copy on a remote host, both the local and remote hosts must be running the same version of SnapDrive.

LiveMountPoint refers to the drive letter, mount point, volume name, or CSV reparse point assigned to the LUN in the active file system.

Example

```
sdcli snap mount -r host3 -k j -s Jun_14_09 -d t
```

The preceding example maps the Snapshot copy named Jun_14_09 to drive T: on the local host. This Snapshot copy represents a point-in-time image of the LUN mapped to J: on host3.

The snap rename command

The `snap rename` command enables you to change the name of an existing Snapshot copy.

Syntax for this command is:

```
sdcli snap rename [-m MachineName] -d MountPoint -o OldSnapshotName -n NewSnapshotName
```

MountPoint is a drive letter, mount point path, volume name, or CSV reparse point.

Example

```
sdcli snap rename -d j -o Jun_14_09 -n last_known_good
```

The preceding example changes the name of the June_14_09 Snapshot copy associated with the J: drive to last_known_good.

```
sdcli snap rename -d C:\ClusterStorage\Volume8 -o csvLun11_051109 -n csvLun11_051109_new
```

The preceding example changes the name of the csvLun11_051109 Snapshot copy associated with CSV reparse point C:\ClusterStorage\Volume8 to csvLun11_051109_new.

The snap restore command

The `snap restore` command replaces the current LUN image in the active file system with the point-in-time image captured by the specified Snapshot copy.

Note: You must make sure that the LUN you are disconnecting is not being monitored with the Windows Performance Monitor (perfmon).

Syntax for this command is:

```
sdcli snap restore [-m MachineName] -d MountPoint -flr [-copy] -s SnapshotName -files filepath[...]
```

MountPoint is a drive letter, mount point path, volume name, or CSV reparse point.

`-flr` specifies that you are performing a file level restore.

`-copy` is an optional setting that forces a copy-restore operation if other restore options fail.

`-files` enables you to specify the path to the files you want to restore.

filepath is the list of files you want to restore, including the path and drive letter or volume mount point to those files.

Use a hyphen (-) at the end of the file path when you want to restore an entire directory, as well as all subdirectories within that directory, recursively.

Use an asterisk (*) at the end of the specified file when you want to restore all files in that directory only. Subdirectories in that directory will not be recursively restored.

Note: File-level wildcard entries are not supported; therefore, the hyphen and asterisk cannot be combined with a filename at the end of the path you want to restore.

Examples

```
sdcli snap restore -d l -s Jun_14_09
```

The preceding example restores the LUN mapped to L: on the local host to its state when the Snapshot copy named Jun_14_09 was taken.

```
sdcli snap restore -flr -s st_10_18_2009 -files c:\mnt1\vm1\vm1_d.vhd f:\vm1\vm1.vhd "f:\vm1\Virtual Machines\" -"
```

The preceding example restores a single file called vm1_d.vhd in the volume mount point c:\mnt1\, a single file called vm1.vhd from the volume mount point f:\vm1, and restores recursively the folder "Virtual Machines" from the Snapshot copy st_10_18_2009.

The snap unmount command

The `snap unmount` command disconnects a Snapshot copy of a LUN that is mounted as a LUN.

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

Attention: If you unmount a LUN on a FlexClone volume that SnapDrive for Windows created and it is the last LUN connected on the volume, SnapDrive deletes that volume resulting in the deletion of all LUNs in the FlexClone volume.

To avoid automatic deletion of the FlexClone volume, rename the volume before unmounting the last LUN. When you rename the volume, be sure to change more than just the last integers in the name. For instance, if the FlexClone volume is named `sdw_cl_myvol_0`, rename it to `new_sdwvol_0`, and not to `sdw_cl_myvol_20`. If you rename only the last integers in the volume name, SnapDrive still recognizes that it created that volume and it will delete the volume when you disconnect the last LUN.

Syntax for this command is:

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

Attention: The -f argument forcibly unmounts the LUN, 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.

Example

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

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

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

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

The snap update_mirror command

The `snap update_mirror` command updates the LUN to a SnapMirror destination volume residing on the same or a different storage system.

Syntax for this command is:

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

Example

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

The preceding example updates the SnapMirror destination for the LUN mapped to the L: drive on the local host. You do not need to specify the location of the SnapMirror destination because that information was entered when mirroring was set up for the LUN.

The snap restore_volume_check command

The `snap restore_volume_check` command verifies whether a restore operation can be performed on a volume.

Syntax for this command is:

```
sdcli snap restore_volume_check [-f StorageSystemName] -volume  
StorageSystemVolumeName -s SnapshotCopyName [-m MachineName]
```

`-f StorageSystemName` is the name of the storage system on which the volume resides.

`-volume StorageSystemVolumeName` indicates the name of the volume on which the restore operation will be performed.

`-s SnapshotCopyName` indicates the name of the Snapshot copy from which the volume will be restored.

Example

```
sdcli snap restore_volume_check -f clpubs-storage1 -volume vol3 -s  
my_snap
```

The preceding example checks whether a volume restoration from the Snapshot copy named `my_snap` can be performed on a volume called `vol3` that resides on a storage system called `clpubs-storage1`.

The `snap restore_volume` command

The `snap restore_volume` command restores a storage system volume from the specified Snapshot copy.

Syntax for this command is:

```
sdcli snap restore_volume [-f StorageSystemName] -volume  
StorageSystemVolumeName -s SnapshotCopyName [-force] [-m MachineName]
```

`-f StorageSystemName` is the name of the storage system on which the volume resides.

`-volume StorageSystemVolumeName` indicates name of the volume on which the restore operation will be performed.

`-s SnapshotCopyName` indicates the name of the Snapshot copy from which the volume will be restored.

`-force` is an optional switch that you use to ensure the volume restoration is performed even when non-LUN files or newer Snapshot copies are found on the volume.

Example

```
sdcli snap restore_volume -f clpubs-storage1 -volume vol3 -s my_snap
```

The preceding example restores a volume from the Snapshot copy named `my_snap` on a volume called `vol3` that resides on a storage system called `clpubs-storage1`.

SnapVault commands

The `sdcli` utility provides command-line support for SnapVault management using SnapDrive.

Next topics

[*The snapvault verify_configuration command*](#) on page 235

[*The snapvault snapshot_rename command*](#) on page 235

[*The snapvault snapshot_delete command*](#) on page 235

[*The snapvault archive command*](#) on page 236

[*The snapvault relationship_status command*](#) on page 236

[*The snapvault snap_list command*](#) on page 236

The snapvault verify_configuration command

The `snapvault verify_configuration` command enables you to check the SnapVault configuration to ensure that it configured correctly.

Syntax for this command is:

```
sdcli snapvault verify_configuration [-m MachineName] {-D MountPoint | -G guidlist}
```

- m specifies the name of the remote system on which you want to execute the command. If no machine name is specified, the command is executed on the local system.
- D specifies a list of mount points of disks on the primary system.
- G specifies a list of GUIDs of disks on the primary system.

The snapvault snapshot_rename command

The `snapvault snapshot_rename` command enables you to rename an existing Snapshot copy on a secondary system.

Syntax for this command is:

```
sdcli snapvault snapshot_rename [-m MachineName] -o OldName -n NewName {-d MountPoint | -G guidlist}
```

- o *OldName* specifies the name of the existing Snapshot copy that you want to change on the secondary system.
- n *NewName* specifies the new name of the Snapshot copy on the secondary system. The new name must not yet exist.
- d *MountPoint* specifies the mount point that identifies the disk on the primary system.
- G *guidlist* specifies a list of GUIDs of disks on the primary system.

The snapvault snapshot_delete command

The `snapvault snapshot_delete` command deletes an existing Snapshot copy on a SnapVault secondary system.

Syntax for this command is:

```
sdcli snapvault snapshot_delete [-m MachineName] {-D MountPoint | -G guidlist} -a ArchivalSnapshotName
```

- D *MountPoint* specifies a list of mount points of disks on the primary system.
- G *guidlist* specifies a list of GUIDs of disks on the primary system.
- a *ArchivalSnapshotName* specifies the name of the Snapshot copy that you want to delete.

The snapvault archive command

The `snapvault archive` command archives a backup set to a secondary system.

Syntax for this command is:

```
sdcli snapvault archive [-m MachineName] [-force] -a ArchivalSnapshotName -DS MountPointandSnapshotList [...]
```

-force forces the secondary Snapshot copy to be made, regardless of the possible failure of some qtree updates.

-a *ArchivalSnapshotName* specifies the name of the Snapshot copy on the secondary system. This Snapshot copy name must not already exist.

-DS *MountPointandSnapshotList* specifies a list of mount points and Snapshot copies to be archived.

The snapvault relationship_status command

The `snapvault relationship_status` command displays the relationship status of the primary system for the disk specified.

Syntax for this command is:

```
sdcli snapvault relationship_status [-m MachineName] {-D MountPoint | -G guidlist}
```

-D *MountPoint* specifies a list of mount points of disks on the primary system.

-G *guidlist* specifies a list of GUIDs of disks on the primary system.

The snapvault snap_list command

The `snapvault snap_list` command displays the Snapshot copies on the volume specified by the mount point or GUID on the SnapVault secondary system.

Syntax for this command is:

```
sdcli snapvault snap_list [-m MachineName] {-D MountPoint | -G guidlist}
```

-D *MountPoint* specifies a list of mount points of disks on the primary system.

-G *guidlist* specifies a list of GUIDs of disks on the primary system.

DataFabric Manager commands

The `sdcli` utility provides command-line support for managing DataFabric Manager credentials after SnapDrive has been installed.

Next topics

[The `dfm\_config list` command](#) on page 237

[The `dfm\_config set` command](#) on page 237

[The `dfm\_config delete` command](#) on page 237

[The `dfm\_config rbaccache` command](#) on page 238

The `dfm_config list` command

The `dfm_config list` command displays a list of already configured DFM servers.

Syntax for this command is:

```
sdcli dfm_config list
```

The `dfm_config set` command

The `dfm_config set` command enables you to set DataFabric Manager server credentials.

Syntax for this command is:

```
sdcli dfm_config set -host Host -user Username -pwd Password[-port Port]
```

-host specifies the hostname or IP address of the host running a DFM server.

-user specifies the username for the DFM server.

-pwd specifies the password to be used for the DFM server.

-port specifies a new TCP port. The default port is 8088 if a new port is not specified.

The `dfm_config delete` command

The `dfm_config delete` command enables you to remove a DFM server from the SnapDrive DFM server list.

Syntax for this command is:

```
sdcli dfm_config delete -host Host
```

-host specifies the hostname or IP address of the host running the DFM server you want to remove from the list.

The dfm_config rbaccache command

The `dfm_config rbaccache` command enables SnapDrive to cache RBAC operations for use when the DataFabric Manager server is down and unavailable for less than 24 hours.

Syntax for this command is:

```
sdcli dfm_config rbaccache [-m MachineName] -rc Enable| Disable
```

Use `-rc Enable` or `-rc Disable` to either enable or disable DataFabric Manager RBAC caching.

Note: The frequency of RBAC cache updates cannot be customized. When `dfm_config rbaccache` is enabled, updates to the RBAC cache occur automatically whenever RBAC information changes on the storage system. If the DataFabric Manager server is unavailable for more than 24 hours, SnapDrive no longer operates.

Transport protocol commands

The `sdcli` utility provides command-line support for managing transport protocols used by SnapDrive.

Next topics

[The transport_protocol list command](#) on page 238

[The transport_protocol set command](#) on page 239

[The transport_protocol delete command](#) on page 239

The transport_protocol list command

The `transport_protocol list` command displays the transport protocol configuration settings SnapDrive uses on the storage system.

Syntax for this command is:

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

Example

```
sdcli transport_protocol list
Default protocol: HTTP
User Name: root
Port: 80
Storage System: Storage1
Other IP address(es)/Name: 172.17.176.44
Protocol: HTTP
Username: root
Port: 80
The operation completed successfully.
```

The preceding example indicates that HTTP is the default transport protocol setting on the local SnapDrive system.

The transport_protocol set command

The `transport_protocol set` command sets or modifies the transport protocol on the storage system.

Syntax for this command is:

```
sdcli transport_protocol set [-m MachineName] -f StorageSystem | -default -type HTTP| HTTPS |RPC [ -port port] [ -user UserName] [-pwd password]
```

`-f StorageSystem` specifies the storage system name or IP address.

`-default` default protocol.

`-type` specifies the protocol type that will be used. Protocol type is either HTTP, HTTPS, or RPC.

`-port port` specifies the port number the protocol will use. The default port for HTTPS is 443. The default port for HTTP is 80.

`-user UserName` specifies the user with permission on the storage system. A username is required if protocol the type is HTTP/HTTPS.

`-pwd password` is the password for the user. A password is required if the protocol type is HTTP/HTTPS. You are prompted for a password if it is not specified.

Example

```
C:\sdcli transport_protocol set -f atlas-1 -type HTTPS -user admin  
Type password for the user:  
New transport protocol has been set.
```

The preceding example sets the transport protocol to HTTPS on the storage system called atlas-1 using the user name "admin." A password is required but was not specified, so the command prompts the user to enter a password.

The transport_protocol delete command

The `transport_protocol delete` command deletes a transport protocol from a storage system.

Syntax for this command is:

```
sdcli transport_protocol delete [-m MachineName] -f StorageSystem | -default
```

`-f StorageSystem` specifies the storage system name or IP address.

`-default` indicates that the protocol will be the default on the specified storage system.

Virtual server commands

The `sdcli` utility provides command-line support for managing virtual server configurations on a VMware Guest OS with SnapDrive on either an ESX server or from the Virtual Center.

Next topics

[The `vsconfig list` command](#) on page 240

[The `vsconfig set` command](#) on page 240

[The `vsconfig dslist` command](#) on page 240

[The `vsconfig delete` command](#) on page 241

The `vsconfig list` command

The `vsconfig list` command displays the virtual server configuration settings.

Syntax for this command is:

```
sdcli vsconfig list
```

The `vsconfig set` command

The `vsconfig set` command enables you to set the virtual server configuration.

Syntax for this command is:

```
sdcli vsconfig set -ip IP Address -user User Name -pwd Password
```

-ip specifies the IP address of the virtual server.

-user specifies the virtual machine user name.

-pwd specifies the password for the virtual machine.

Note: You can change the IP address of a virtual server that you have previously configured during SnapDrive installation without re-entering the username and password. A valid IP address, username, and password must already exist in the Windows registry; otherwise, an error message is displayed indicating that the user credentials are not set.

The `vsconfig dslist` command

The `vsconfig dslist` command displays datastores available on ESX servers.

Syntax for this command is:

```
sdcli vsconfig dslist -m MachineName -port "Port Number"
```

-port specifies the Web service port number you use to communicate with SnapDrive. The default port is 808.

The vsconfig delete command

The `vsconfig delete` command disables ESX server and VirtualCenter settings.

Syntax for this command is:

`sdcli vsconfig delete`

Note: When you disable VirtualCenter or ESX settings, SnapDrive cannot display WWPNs for FC HBAs on the ESX server.

Note: You cannot disable VirtualCenter or ESX settings when FC RDM LUNs are present.

Index

A

- access
 - configuring 66
 - pass-through authentication 67
- adding HTTP user storage system capabilities 46
- aggregates
 - overview 26
- application datasets, definition of 157
- assigning roles using RBAC 93
- authentication
 - HTTP and HTTPS 66
 - pass-through 66, 67
 - RPC 66

B

- backups
 - typical process using VSS 160
 - using SnapVault with SnapDrive 155

C

- CHAP authentication
 - about using with SnapDrive 97
- CIFS
 - limited functionality supplied with FC and iSCSI licenses 64
- cluster
 - support 50
- cluster shared volume
 - about 51
- command line installation
 - examples 185, 186
 - switches 178
 - syntax 177
- communication
 - configuring Windows Firewall 80
- components
 - determining if controller components are installed 64
 - HBA (Host Bus Adapter) 64
 - MPIO 64
 - SnapDrive 23
- configurations
 - choosing 59

- considerations for determining 59
 - FC, single host, dedicated switch 190
 - FC, single host, direct-attached 190
 - FC, Windows cluster 191
 - iSCSI, single host, dedicated switch 188
 - iSCSI, single host, direct-attached 187
 - iSCSI, single host, GbE switch 188
 - iSCSI, Windows cluster 189
 - MPIO, single host, direct-attached 192
 - MPIO, Windows cluster, FC switch 193
 - MPIO, Windows cluster, GbE switch 192
- configuring
 - access 66
 - failover cluster witness disk 113
 - pass-through authentication 67
 - RBAC on SnapDrive 91
 - space reservation monitoring 137
- Connect Disk wizard 122
- connecting
 - a disk 122
 - a LUN 122
 - LUNs, about 121
- creating
 - LUNs 102
 - RDM LUNs 114
- creating roles using RBAC 92
- credentials required 66

D

- Data ONTAP
 - required version 64
- datasets
 - general concepts 157
- dedicated LUN
 - creating 102
- Delete Disk 130
- deleting
 - a LUN 130
 - folder within volume mount point 131
 - volume mount point 127
- disconnecting
 - a LUN 129
 - forced (of LUN) 129
 - iSCSI session 98
 - iSCSI target 97

- disk
 - hot spare 26
- disk allocation
 - planning 25
- documentation
 - obtaining 58
 - recommended to read before installing SnapDrive 58
- drivers
 - obtaining 60, 61

E

- enabling ESX or vCenter logon from SnapDrive MMC 48
- enabling RBAC on the storage system 91
- ESX iSCSI initiator
 - limitations 44
 - support 43
- ESX logon
 - enabling and disabling from SnapDrive MMC 48
- ESX Server
 - requirements 62
- examples
 - command line installation 185, 186
 - storage system access control commands 198
 - unattended installation 185, 186
- expanding
 - a LUN 132
 - a quorum disk 133
 - LUNs, about 131

F

- failover cluster witness disk
 - configuring 113
- FC
 - configurations 190
 - determining components installed 64
 - documentation 58
 - installing 71
 - license requirement on storage system 64
 - obtaining firmware and drivers 60, 61
 - upgrading 71
- FC RDM LUN
 - support with Microsoft clusters 52
- features
 - new 35
 - supported 37
- file-level restore operation

- described 41
- support for 41
- firmware
 - obtaining 60, 61
- FlexClone
 - license requirement on storage system 64
- FlexClone volumes
 - about using in SnapDrive 146
 - prerequisites for using with SnapDrive 147
- forced disconnect (of LUN) 129
- fractional reserve
 - about 29
- fractional space reservation monitoring
 - about 137

G

- GPT partition
 - support 50
- guidelines
 - for choosing SnapDrive configuration 59
 - for preparing a SnapDrive volume 66

H

- high availability
 - virtual machine 118
- hosts
 - hardware requirements 60, 61
 - operating system requirements 60, 61
 - preparing 59
 - software requirements 60, 61
- hot spare disk 26
- hot spares
 - best practices 26
- HTTP and HTTPS
 - authentication 66
 - transport protocol support 45
- Hyper-V pass-through disk
 - limitations 41
 - support for dynamically adding and removing 40

I

- icons
 - SnapDrive for Windows 31
- installing
 - documents to read before 58
 - FC components 71

- iSCSI components 71
- iSCSI Software Initiator 72
- overview 55
- SnapDrive components 73
- SnapDrive on Windows Server Core 79
- unattended 80
- IP address
 - setting preferred 85
- iSCSI
 - configurations 187
 - determining components installed 64
 - disconnecting target from Windows host 97
 - documentation 58
 - establishing a session to a target 96
 - examining session details 99
 - installing 71
 - license requirement on storage system 64
 - obtaining Microsoft iSCSI Software Initiator 60, 61
 - upgrading 71
- iSCSI session
 - disconnecting from target 98
- iSCSI Software Initiator
 - node naming standards 95
 - installing 72
 - upgrading 72

J

- joining Windows Server Core to a domain 77

L

- licenses
 - checking on storage systems 65
 - managing 83
 - requirements 64
- limitations
 - VMDK with SnapDrive 38
- LUN
 - protocols 25
- LUN clone split feature
 - about 150
- LUN restore
 - checking status 151
- LUNs
 - about connecting 121
 - about disconnecting in FlexClone volume 128
 - about disconnecting or deleting 128
 - about expanding 131

- adding, removing, or changing a drive letter or path
 - 127
- connecting to 122
- creating 102
- creating shared 106
- deleting 130
- disconnecting 129
- documentation about protocols 58
- expanding 132
- expanding a quorum disk 133
- forced disconnect 129
- managing 121
- managing non-SnapDrive LUNs 133
- moving a mount point 128
- preparing a volume to hold LUNs 66
- rules for creating 101

M

- managing LUNs 121
- managing space 137
- Microsoft cluster with ESX
 - related documentation 51
- Microsoft iSCSI Software Initiator
 - obtaining 60, 61
- monitoring
 - space reservation 137
- MPIO
 - configurations 191
 - upgrading with 69
- MultiStore
 - license requirement on storage system 64
 - support 45

N

- new features in SnapDrive for Windows 35
- non-SnapDrive LUNs
 - managing 133
 - preparing for SnapDrive 133
- notification settings
 - enabling 84

O

- obtaining
 - firmware and drivers 60, 61
 - Microsoft iSCSI Software Initiator 60, 61
- options

- storage system 27
- volume 27

P

- pass-through authentication
 - configuring 67
 - reasons to use 67
- pass-through disk
 - described 40
- password
 - SnapDrive service account 66
- planning
 - disk allocation 25
- preferred IP address
 - setting 85
- preparing
 - for SnapDrive upgrade 69
 - SnapDrive hosts 59
 - storage system volume 65
 - storage systems for use with SnapDrive 64
 - to install or upgrade SnapDrive 57
- Protection Manager integration with SnapDrive 157
- protection policies
 - overview 157
- protocols
 - for accessing LUNs 25
- provisioning policies
 - overview 157

Q

- quorum disk
 - creating on a Windows 2003 cluster 110
 - expanding 133

R

- rapid LUN restore
 - about 150
- RBAC (role-based access control)
 - assigning roles 93
 - configuring SnapDrive to use 91
 - creating roles 92
 - enabling on storage system 91
 - support for 89
- RDM 128
- RDM LUN
 - FC support 52
- RDM LUNs
 - creating 114

- remote administration
 - enabling on Windows Server Core 77
 - of SnapDrive 87
- remote SnapDrive server
 - adding 87
 - removing 88
- removing stale RDMs 128
- renaming the Server Core system 77
- requirements
 - credentials 66
 - Data ONTAP version 64
 - drivers 60, 61
 - firmware 60, 61
 - licenses 64
 - SnapDrive hosts 60, 61
 - SnapDrive service account 66
 - SnapDrive user account 68
 - storage systems 64
 - VMware 62
- role mappings
 - SnapDrive to DataFabric Manager server 201
- roles
 - storage system access control 196
- RPC
 - authentication 66

S

- SAN booting
 - SnapDrive support for 165
 - support 50
- service account
 - requirements 66
- setting
 - preferred IP address 85
 - space reservation 138
- shared LUNs
 - creating 106
- SnapDrive
 - access configuration 66
 - capabilities 21
 - choosing configuration 59
 - components 23
 - configurations 187
 - documents to read before installing 58
 - installing components 73
 - installing overview 55
 - integration with Protection Manager 157
 - preparing to install or upgrade 57
 - preparing to upgrade 69

- recommendations for using 22
- service
 - stopping and starting 85
- service account 66
- transport protocol 66
- unattended installation 80
- upgrading overview 55
- user account 68
- SnapDrive Administrators group 68
- SnapDrive GUI icons, described 31
- SnapDrive to DataFabric Manager server role mappings 201
- SnapMirror
 - license requirement on storage system 64
 - requirements for using with SnapDrive 169
- SnapRestore
 - license requirement on storage system 64
- Snapshot copies
 - creating 144
 - deleting 152
 - reasons for creating 143
 - scheduling 145
- SnapVault
 - about 155
 - initiating backups 155
 - license requirement on storage system 64
 - support 47
- space
 - managing 137
- Space Reclaimer
 - about 139
 - guidelines 139
 - reasons for SnapDrive to automatically stop 141
 - starting 140
 - stopping 141
 - support with VMDK 38
- space reservation monitoring 137
- space reservation settings
 - managing with storage access control tool 138
- space reservations
 - about 28
- starting
 - SnapDrive service 85
 - Space Reclaimer 140
- stopping
 - SnapDrive service 85
 - Space Reclaimer 141
- storage services
 - overview 157
- storage system access control

- command examples 198
- described 42
- operations, described 195
- roles, described 196
- storage system access control (storac)
- commands 198
- storage system access control tool (storac.exe)
 - using 42
- storage system capabilities
 - adding for HTTP users 46
- storage systems
 - checking licenses 65
 - considerations for preparing a SnapDrive volume 66
 - guidelines for creating a volume 66
 - HBA and NIC requirements 64
 - license requirements 64
 - operating system requirements 64
 - options set by SnapDrive 27
 - preparing a volume for SnapDrive 65
 - preparing for use with SnapDrive 64
- surprise removal (of LUN) 129
- switches
 - command line installation 178
 - unattended installation 178
- syntax
 - command line installation 177
 - unattended installation 177

T

- thinly provisioned LUNs
 - enabling 138
- transport protocol
 - configuring 66
 - default 66
 - support of HTTP and HTTPS 45
- troubleshooting
 - VSS Hardware Provider 161

U

- unattended installation
 - examples 185, 186
 - performing 80
 - switches 178
 - syntax 177
- upgrading
 - FC components 71
 - iSCSI components 71

- iSCSI Software Initiator 72
 - overview 55
 - preparing for 69
 - SnapDrive components 73
 - with MPIO 69
- user account
 - requirements 68
- using the storage system access control tool (storacl.exe)
 - 42

V

- vCenter logon
 - enabling and disabling from SnapDrive MMC 48
- vCenter permissions
 - minimum required 49
- virtual machine
 - creating highly available 118
- VMDK
 - limitations with SnapDrive 38
 - Space Reclaimer support 38
 - support by SnapDrive 37
- VMotion
 - requirements 49
 - support 49
- VMware
 - limitations 48
 - requirements 62
 - support 47
- volume
 - considerations for preparing 66
 - guidelines for creating 66
 - preparing on storage system 65
- volume mount points

- about 102
- adding 127
- changing 127
- deleting folder within 131
- limitations 102
- moving 128
- removing 127
- volume options set by SnapDrive 27
- volume-based Snapshot copy restoration
 - about 152

VSS

- about 159
- troubleshooting 161
- typical backup process 160
- verifying configuration 162
- verifying provider used 162
- viewing installed providers 161

W

- Windows Firewall
 - configuring to enable SnapDrive communication
 - 80
- Windows Server 2008 failover cluster
 - support 113
- Windows Server Core
 - enabling remote administration 77
 - installing SnapDrive 79
 - joining a domain 77
 - limitations 39
 - renaming 77
 - requirements for using with SnapDrive 40
 - SnapDrive support in 39