

Veritas Storage Foundation[™] Administrator's Guide

Windows Server 2003, Windows Server 2008

5.1. Service Pack 1



Veritas Storage Foundation Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 5.1.SP1.0

Document version: 5.1.SP1.1

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Veritas and Veritas Storage Foundation are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice file accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrades protection
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information

- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan customercare_apac@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America supportsolutions@symantec.com

Contents

Section 1 Configuring

Chapter 1 Overview

About Veritas Storage Foundation for Windows products	21
General features	23
Optional advanced features	25
Veritas FlashSnap option	25
Veritas Dynamic Multi-pathing option	26
Veritas Volume Replicator option	26
Veritas cluster option for Microsoft Clustering	27
Veritas Global Cluster Option	27
Software components	28
Advantages of dynamic volumes	29
SFW's software RAID	30
What is RAID?	30
SFW and Virtual Disk Service (VDS)	30
Choosing RAID levels	32
Hardware and software RAID	35

Chapter 2 Setup and configuration

Setup and configuration summary	38
Function overview	39
Basic and dynamic disks	39
Basic and dynamic volumes	40
Disk groups	41
Dynamic volume components	41
Access Veritas Storage Foundation for Windows	43
Accessing VEA through the Windows start menu	43
Accessing VEA through the Windows computer management window	44
Disabling write caches and HBA caches	45
Disconnecting from a server	46
Understanding the conditions for remote connection	46
Review the Veritas Enterprise Administrator GUI	48
Configure basic disks (Optional)	51

About basic disks	51
Upgrading basic disks to dynamic	51
Create dynamic disk groups	53
Considerations when changing a basic disk to dynamic	53
Steps for creating a dynamic disk group	55
Making storage available after system startup	59
Create dynamic volumes	60
Background information	60
Steps for creating a dynamic volume	61
Dynamic volume types	67
Set up a dynamic boot and system volume (Optional)	70
Configure VCS and program options	73
SFW HA	73
Veritas cluster option for Microsoft Clustering	73
Veritas Dynamic Multi-pathing option (DMP)	74
Veritas FlashSnap option	74
Veritas Volume Replicator option (VVR)	74
Additional SFW HA options	75
Set desired preferences	76
Hot relocation settings	76
Event notification settings	77
S.M.A.R.T. monitoring for a disk	77
Capacity monitoring for volumes	77
Task throttling	78
Configuration task performance tuning	78
Track alignment settings	78
Protecting your SFW configuration with vxcbt	79
Guidelines for running SFW	79

Section 2 Managing

Chapter 3 Using the GUI to manage your storage

Overview of console features	84
Viewing disks and volumes	85
Storage Foundation general preferences	86
The URL bar	87
The Toolbar	88
The Perspective bar	89
Systems perspective	90
The left pane	91
The right pane	95
Right-pane display for disks and volumes	95

Disk view tab	98
Right-pane legends	99
Customizing the table headers	100
The lower pane	102
The disk view	103
Disk view overview	103
Options for graphical views	105
Expanded view	106
Search	111
Conducting a search	111
Using saved queries	114
Creating search reports	116
Assistant perspective	120
Logs perspective	121
Control Panel perspective	122
Log settings	123
Rule Manager	124
Configuration backup	124
Historical statistics	125
SMTP configuration	125
System settings	126
Task settings	133
Track alignment	134

Chapter 4 Working with disks, partitions, and volumes

Adding storage	138
Add a new disk to your system	138
Add a disk signature to a disk	139
Add a disk to a dynamic disk group	141
Create new volumes	143
Disk tasks	144
Remove a disk from a dynamic disk group	144
Remove a disk from the computer	145
Offline a disk	147
Update disk information by using rescan	147
Set disk usage	147
Evacuate disk	148
Replace disk	148
Changing the internal name of a disk	150
Renaming an enclosure	150
Work with removable media	151
Working with disks that support thin provisioning	151
View disk properties	161

General Partition/Volume tasks	164
Delete a volume	164
Delete a partition or logical drive	165
Shredding a volume	165
Refresh drive letter, file system, and partition or volume information	166
Add, change, or remove a drive letter or path	167
Renaming a mirror (plex)	169
Changing the internal name of a volume	169
Mount a volume at an empty folder (Drive path)	170
View all drive paths	172
Format a partition or volume with the file system command	172
Cancel format	173
Change file system options on a partition or volume	173
Set a volume to read only	174
Check partition or volume properties	174
Expand a dynamic volume	177
Expand a partition	180
Shrink a dynamic volume	180
Basic disk and volume tasks	183
What can you do with a basic disk?	183
Converting the partition style of a disk	184
Create primary and extended partitions	184
New logical drives	189
Mark a partition as active	190
Change a basic disk to dynamic	191
Troubleshoot basic disks and volumes	191

Chapter 5 Dealing with disk groups

About disk groups	194
Basic and dynamic disk groups	194
Moving dynamic disk groups between computers	194
Primary and secondary dynamic disk groups	195
Cluster disks and cluster dynamic disk groups	196
Private dynamic disk group protection	196
Delete a dynamic disk group	197
Recommended method for deleting a disk group	197
Alternative method for deleting a disk group	197
Upgrade a dynamic disk group version	199
Importing a dynamic disk group to a cluster disk group	200
Rename a dynamic disk group	201
Detaching and attaching dynamic disks	202
Detaching dynamic disks	202

	Attaching dynamic disks	203
	Importing and deporting dynamic disk groups	205
	Deport a dynamic disk group	205
	Import a dynamic disk group	207
	Partitioned shared storage with	
	private dynamic disk group protection	209
	Create a new dynamic disk group with private dynamic	
	disk group protection	210
	Add private dynamic disk group protection to an	
	existing dynamic disk group	211
	Remove private dynamic disk group protection	
	from a dynamic disk group	212
	Dynamic disk group properties	213
	Troubleshooting problems with dynamic disk groups	216
Chapter 6	iSCSI SAN support	
	About iSCSI SANs	218
	About iSNS servers	218
	Configuring an iSCSI SAN with SFW	220
	Considering prerequisites	220
	Setting up an iSCSI SAN	220
	Using SFW vxdg latestart for iSCSI	221
	Managing an iSCSI SAN with SFW	223
	Managing with the VEA Console	223
Chapter 7	Settings for monitoring objects	
	Event monitoring and notification	234
	Alert log	234
	Severity levels	235
	Log configuration	236
	Event notification	236
	Accessing the Rule Manager utility	237
	Preliminary setup	238
	Steps for creating rules	239
	Accessing the SFW SNMP MIB files	241
	Disk monitoring	242
	Capacity monitoring	244
	Automatic volume growth	246
	Configuring Automatic Volume Growth in a	
	cluster environment	249
	Automatic volume growth script for volume	
	capacity monitoring	249

SMTP configuration for email notification	253
---	-----

Chapter 8 Standard features for adding fault tolerance

Overview	256
Mirroring	257
About mirroring	257
Two methods for creating a mirror	258
Break or remove a mirror	259
Break mirror	260
Remove mirror	261
Set the mirrored volume read policy	262
Mirror a dynamic boot or system volume	264
Reactivate a mirrored volume	264
Repair a mirrored volume	265
RAID-5 and RAID 0+1	266
Hot relocation	268
Hot relocation overview	268
Hot relocation setup summary	269
Hot relocation mode	269
Customize target disks with set disk usage	270
Undo hot relocation	271
Clear hot relocation information	272
Dirty region logging (DRL) and RAID-5 logging	274
Dirty region logging for mirrored volumes	274
RAID-5 logging	274
Add a log	275
Remove a log	276
Dynamic relayout	277
Examples of dynamic relayout	278
Detailed steps for dynamic relayout	279

Chapter 9 Command line interface

SFW commands available from the command line	281
Command line log	283
Conventions for command line syntax	285
vxvol	288
vxvg	302
vxclus	325
vxdisk	329
vxassist	341
Windows-specific vxassist commands	373
vxevac	377

vxunreloc	378
vxsd	379
vxstat	381
vxtask	384
vxedit	385
vxdumpadm	388
vxabr	404
vxsnap	407
vxsnapsql	447
vxfsync	455
vxscrub	456
vxverify	459
vxcache	461
vxprint	464

Chapter 10 Troubleshooting and recovery

Using disk and volume status information	467
Disk status descriptions	468
Volume status descriptions	472
SFW error symbols	476
Resolving common problem situations	477
Bring an offline dynamic disk back to an imported state	477
Bring a basic disk back to an online state	478
Remove a disk from the computer	479
Bring a foreign disk back to an online state	479
Bring a basic volume back to a healthy state	481
Bring a dynamic volume back to a healthy state	481
Repair a volume with degraded data after moving disks between computers	482
Deal with a provider error on startup	483
Commands or procedures used in troubleshooting and recovery	485
Refresh command	485
Rescan command	485
Replace disk command	487
Merge foreign disk command	487
Reactivate disk command	491
Reactivate volume command	492
Repair volume command for dynamic RAID-5 volumes	493
Repair volume command for dynamic mirrored volumes	493
Starting and stopping the Veritas Storage Foundation for Windows Service	494
Accessing the CLI history	495
Additional troubleshooting issues	496

Disk issues	496
Volume issues	498
Disk group issues	500
Connection issues	502
Issues related to boot or reboot	504
Cluster issues	505
Dynamic multi-pathing issues	508
vxsnap issues	509
vxsnapsql issues	511
Other issues	512
Automated System Recovery (ASR)	513
Automated system recovery (ASR) overview	513
SFW's support for ASR	514
ASR recovery process	515
Cluster recovery	516

Section 3 Optimizing

Chapter 11 Performance tuning

About performance tuning	519
Statistics overview	519
Real-time statistics collection and display	522
Online monitoring window features	522
Setup steps for real-time statistics	524
Historical statistics collection and graphing	531
Features of the graphing window	531
Setup steps for historical statistics	533
Subdisk move, split, and join	539
Purpose of the subdisk commands	539
Subdisk context menu	541
Subdisk properties	542
Moving subdisks	544
Splitting subdisks	546
Joining subdisks	547
Command line commands for statistics	548
VxCache	549
Overview	549
Identifying the memory capabilities of your servers	550
Determining the memory to assign to VxCache for a server	551
Determining the volumes to include on the server	553
Enabling VxCache	554
VxCache volume monitoring	558

Monitoring VxCache performance	559
More on the policy file	560
SmartMove	561

Chapter 12

FlashSnap

FlashSnap overview	563
FlashSnap components	566
Summary of the FlashSnap procedure	567
FastResync	570
FR limitations	570
Resynchronization	571
Reconnection	571
Enabling and disabling FR	572
Disk change object (DCO) volume	572
Snapshot commands	577
Using the snapshot procedure	578
Prepare	580
Snap shot	585
Snap back	588
Snap clear	590
Snap abort	591
Using the Snapshot Scheduler wizard	593
Dynamic disk group split and join	597
About dynamic disk group split and join	597
Dynamic disk group split	600
Recovery for the split command	604
Dynamic disk group join	606
Using dynamic disk group split and join with a cluster on shared storage	609
Limitations when using dynamic disk group split and join with VVR	612
DGSJ troubleshooting tips	612
CLI FlashSnap commands	613
Fast file resync	614
Volume Shadow Copy Service (VSS)	617
Overview	617
VSS components	618
Overview of VSS process for SFW snapshots	620
VSS snapshot wizard for Microsoft Exchange, Microsoft SharePoint, and Microsoft SQL	622
Using the VSS snapshot wizards with Microsoft Exchange	624
Using the VSS Snapshot wizard	625
Using the VSS Snapback wizard	627

Using the VSS Snapshot Scheduler wizard	627
Using the VSS Restore wizard	637
Refreshing the snapshot set	641
Supporting replication in Exchange 2007	641
Using the VSS snapshot wizards with Microsoft SharePoint	646
Using the VSS SharePoint Snapshot wizard	646
Using the VSS SharePoint Snapshot Scheduler wizard	649
Using the VSS SharePoint Snapback wizard	652
Using the VSS SharePoint Restore wizard	653
Using the VSS snapshot wizards with Enterprise Vault	656
Using the Enterprise Vault Snapshot wizard	657
Using the Enterprise Vault Snapback wizard	663
Using the VSS Enterprise Vault Snapshot Scheduler wizard	664
Using the Enterprise Vault Restore wizard	669
Using the VSS snapshot wizards with Microsoft SQL	673
Using the VSS Snapshot wizard	674
Using the VSS Snapback wizard	677
Using the VSS Snapshot Scheduler wizard	677
Using the VSS Restore wizard	686
Copy on Write (COW)	693
Overview	693
SFW VSS COW snapshot process	693
Managing Shadow Storage	693
Using the VSS COW Snapshot wizard	695
Using the VSS COW Snapshot Scheduler wizard	695
Using the VSS COW Restore wizard	699
Additional information about COW snapshots	700
Using the VSS COW snapshot wizards with Microsoft Exchange	702
Using the VSS COW Snapshot wizard	702
Using the VSS COW Snapshot Scheduler wizard	704
Using the VSS COW snapshot wizards with Microsoft SQL	709
Using the VSS COW Snapshot wizard	709
Using the VSS COW Snapshot Scheduler wizard	711

Chapter 13 Dynamic multi-pathing software

Dynamic multi-pathing overview	718
About dynamic multi-pathing	718
Major features of dynamic multi-pathing	720
Active/Active and Active/Passive settings	721
DMP DSMs	728
DMP DSMs menus	729
Add and remove paths	735
Specify load balancing settings and the primary path	736

	Specifying control timer settings for an array	745
	View array, disk, and path status	747
Chapter 14	Microsoft Clustering support	
	Overview of support for Microsoft Clustering	754
	How SFW works with Microsoft Clustering	756
	Installing Microsoft Clustering support after SFW is already installed	757
	Create a cluster dynamic disk group	759
	Make the cluster disk- group a cluster resource	761
	Display cluster disk group resource properties	770
	Create a dynamic mirrored quorum resource	773
	Microsoft Clustering quorum arbitration time settings	777
	Additional considerations for SFW Microsoft Clustering support	778
Chapter 15	VCS support in SFW HA	
	Overview	784
	How SFW HA works with VCS	784
	Integration steps	786
	Setting up the cluster hardware	786
	Installing and configuring Windows	786
	Installing SFW HA	786
	Setting up a VCS cluster	787
	Creating cluster dynamic disk groups and volumes	787
	Installing the application on cluster nodes	787
	Configuring cluster disk groups and volumes as VCS resources	788
	Bringing resources online	793
	Testing the cluster	793
	Additional considerations for SFW VCS support	794
Chapter 16	Implementing disaster recovery with VVR	
	Overview of VVR	798
	Summary of the steps for setting up a disaster recovery solution with VVR	801
	VVR terms	803
Glossary		805
Index		817

Configuring

- [Chapter 1, “Overview”](#) on page 21
- [Chapter 2, “Setup and configuration”](#) on page 37

Overview

- [General features](#)
- [Optional advanced features](#)
- [Software components](#)
- [Advantages of dynamic volumes](#)
- [SFW's software RAID](#)

About Veritas Storage Foundation for Windows products

Veritas Storage Foundation™ for Windows includes the following products:

- Veritas Storage Foundation 5.1 for Windows (SFW)
- Veritas Storage Foundation 5.1 for Windows Basic (SFW Basic). “Basic” indicates a limited version of SFW.
- Veritas Storage Foundation HA 5.1 for Windows (SFW HA). “HA” indicates SFW with High Availability.

SFW and SFW Basic have the same functions except SFW Basic is limited in the number of dynamic volumes that it can support and that the Veritas Dynamic Multi-pathing option is included. No other options are available in SFW Basic.

SFW and SFW HA have the same functions except for the feature of clustering support. SFW HA adds Veritas Cluster Server (VCS) support. SFW retains the option of Microsoft Clustering (Microsoft Cluster Service (MSCS) for Windows Server 2003; or the Failover Cluster feature for Windows Server 2008).

The information in this guide applies to SFW, SFW Basic, and SFW HA. Clustering support is covered in the last few chapters of the manual. The rest of the manual focuses on the features common to both products. Additional

information about clustering with VCS can be found in other guides in the Veritas Storage Foundation for Windows document set.

Note: To avoid having to repeat the products' names throughout this manual, the name "Veritas Storage Foundation for Windows" and the acronym "SFW" are used to refer to SFW, SFW Basic, and SFW HA when discussing features that are common to the products. When there is a feature that is available in only one of the products, the distinction is clearly identified for the reader.

General features

Veritas Storage Foundation 5.1 for Windows provides a comprehensive solution to storage management in an integrated graphical view. Through the Veritas Enterprise Administrator console, SFW lets you configure and manage local and remote storage attached to your system while your system remains online.

With Veritas Storage Foundation 5.1 for Windows, you can do the following:

- Manage domain-wide storage from a single console.
- Create and configure software RAID while systems remain online and available.
- Optimize storage system performance via online capacity monitoring and storage load balancing.
- Run on either Windows Server 2003 or Windows Server 2008

SFW's configuration solutions

Many storage configuration tasks require taking the system offline and restarting the server, which interrupts system and data availability. Veritas Storage Foundation for Windows provides a major improvement for system administrators and their users by allowing online configuration of dynamic volumes without requiring a system reboot. SFW allows you to perform a wide variety of storage administration tasks while your systems remain online and your data remains available.

SFW's configuration solutions offer the following:

- Provides the ability to configure and manage different volume layouts: concatenated, striped, mirrored, mirrored striped, and RAID-5 volumes. Supports up to 32-way mirrors on a mirrored volume.
- Provides automatic detection of failed disks and the ability to repair fault-tolerant volumes on those disks without interrupting applications using the volumes.
- Provides a storage migration path with the ability to upgrade existing partitions to the new "dynamic" volumes (volumes based on Veritas Storage Foundation for Windows technology).
- Supports online extending of all volume types.
- Supports a cluster environment that runs under Microsoft Cluster Service software.
- Supports mounting a volume without requiring the use of a drive letter.

- Supports moving of storage between computers with the Import and Export Dynamic Disk Group functions.
- Provides command line support for administrators who prefer this method over a graphical user interface (GUI).
 - For a Server Core installation of Windows Server 2008, only the SFW command line interface (CLI) is available.

Optimized system performance

Performance degradation occurs when a program or device uses too much disk I/O. By monitoring a system's I/O, you can find the problem areas and eliminate areas of high activity ("hot spots"), thus ensuring smooth operation. SFW's performance monitoring utility allows you to continuously monitor and tune system performance, monitor I/O statistics, perform hot spot detection, and make adjustments.

Veritas Storage Foundation for Windows can help improve overall disk and system performance in several ways, some of which are as follows:

- I/O statistics are used to identify high-traffic areas, known as "hot spots." You can use the Move Subdisk command to resolve these hot spots online.
- Data is assigned to physical drives to evenly balance the I/O load among the disk drives. This is known as storage load balancing.
- Event logging of errors and important information is provided.

Operating system support and Windows storage management availability

Microsoft provides some storage management on Windows Server 2003 and Windows Server 2008. Logical Disk Manager (LDM) is included with Windows Server 2003 and Microsoft Disk Management is included with Windows Server 2008. Veritas Storage Foundation 5.1 for Windows runs on either Windows Server 2003 or Windows Server 2008 and the availability of the Windows storage management is as follows:

- On Windows Server 2008, the installation of SFW 5.1 supports the availability of Microsoft Disk Management. SFW coexists with Microsoft Disk Management.
- On Windows Server 2003, coexistence with Logical Disk Manager (LDM) is not supported. Installing SFW makes LDM unavailable.

Optional advanced features

This section describes the program's licensable options, which are as follows:

- Options available in both SFW and SFW HA
 - [Veritas FlashSnap option](#)
 - [Veritas Dynamic Multi-pathing option](#)
 - [Veritas Volume Replicator option](#)
- Option available in SFW only
 - [Veritas cluster option for Microsoft Clustering](#)
- Option available in SFW HA only
 - [Veritas Global Cluster Option](#)

Note: VxCache also appears on the product installer's Options screen. VxCache is not a licensed option. It is an optional program feature that enables caching on dynamic volumes to improve performance. See "[VxCache](#)" on page 549.

Veritas FlashSnap option

Veritas FlashSnap™ is a multi-step process that allows you to create independently addressable snapshot volumes that are copies or mirrors of the volumes on your server. These snapshot volumes can be used as quick recovery images for recovering applications, such as Microsoft Exchange. They also can be used for backup or application testing. One of the main advantages of using FlashSnap is that the snapshot volumes can be easily moved to another server. Thus, backup or other processing can be performed on another server without affecting the performance of applications on the applications server.

Even when FlashSnap is performed on the same server, its very efficient mirror breakoff and join process is much faster and takes less CPU availability than other mirror breakoff procedures that use ordinary mirroring.

Starting with SFW 4.0, the capability of creating simultaneous, multiple split-mirror snapshots was added. These snapshots can be done either through the GUI or through the `vxsnap` command line interface (CLI) command.

Also starting with SFW 4.0 was support for VSS hot snapshots with Microsoft Exchange 2003. If you are running Microsoft Exchange 2003 with SFW 5.1 and FlashSnap, you can perform snapshots of all volumes of an Exchange database without taking the databases offline. The VSS process allows the databases of an Exchange Server 2003 storage group to be quiesced before the snapshot operation occurs and then reactivated immediately after it. This quiescing,

supported by Exchange Server 2003 at the storage group level, allows for Microsoft supported and guaranteed persistent snapshots of your data.

SFW 5.1 also provides support for snapshots when the Local Continuous Replication (LCR) and Cluster Continuous Replication (CCR) features of Microsoft Exchange 2007 are enabled. LCR and CCR are available on Windows Server 2003 (x64 Editions) and later releases.

In addition, SFW 5.1 provides recovery support for Microsoft Exchange storage groups or individual databases within an Exchange storage group.

Note: FlashSnap requires a separate license. See the licensing section in the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide* for details.

FlashSnap contains several components: FastResync, Snapshot commands, and Disk Group Split and Join.

See “[FlashSnap components](#)” on page 566.

If you install FlashSnap, you also have access to the Fast File Resync feature that allows you to resynchronize one or more files in a snapshotted volume back to the original volume.

See “[Fast file resync](#)” on page 614.

Veritas Dynamic Multi-pathing option

The Veritas Dynamic Multi-pathing™ (DMP) option adds fault tolerance to disk storage by making use of multiple paths between a computer and individual disks in an attached disk storage system. Disk transfers that would have failed because of a path failure are automatically rerouted to an alternate path. With Veritas Dynamic Multi-pathing, the Veritas Enterprise Administrator (VEA) console allows you to configure, manage, and obtain status information about these multiple paths. Veritas Dynamic Multi-pathing also improves performance by allowing load balancing among the paths.

See “[Dynamic multi-pathing overview](#)” on page 718.

Veritas Volume Replicator option

Veritas Storage Foundation 5.1 for Windows enables dynamic volumes to work with Veritas Volume Replicator (VVR).

VVR is a data replication tool designed to contribute to an effective disaster recovery plan by maintaining a consistent copy of application data at a remote site. In the event that the data center is down, the application data is

immediately available at the remote site, and the application can be restarted at the remote site.

See “[Overview of VVR](#)” on page 798.

Veritas cluster option for Microsoft Clustering

Veritas Storage Foundation 5.1 for Windows can support up to eight nodes in a cluster environment set up for Microsoft Clustering (Microsoft Cluster Service (MSCS) on Windows Server 2003; or the Failover Cluster feature of Windows Server 2008).

See “[Overview of support for Microsoft Clustering](#)” on page 754.

Veritas Global Cluster Option

The Global Cluster Option (GCO) allows for the management of multiple clusters and their applications from a single console. GCO is also a disaster recovery tool that facilitates replication support after a site failure. It ensures that applications are failed over as well as data.

Software components

Veritas Storage Foundation for Windows includes the following components:

Client software

The client software includes the console and runs on Windows XP Professional; Windows Vista; Windows Server 2003 Standard Edition, Web Edition, Enterprise Edition, or Datacenter Edition or Windows Server 2008 Standard Edition, Web Edition, Enterprise Edition, or Datacenter Edition. The client enables you to configure and manage storage attached to both local and remote hosts.

Server software

The server software, which runs on a managed server, is the common repository for all storage objects.

Providers

The providers run on a managed server. Providers are similar to drivers. Each provider manages a specific hardware or software storage component. For example, there is a disk provider that manages all disks that Windows Server 2003 sees as disks.

The providers discover the existing physical and logical entities and store that information in the Veritas Storage Foundation for Windows distributed database. Providers update the database whenever there is a change in the physical or logical entities present in the hardware or software.

See “[Providers](#)” on page 813.

Advantages of dynamic volumes

One of the main advantages of dynamic volumes is that they can span across multiple disks. You can get better use of your available disk space by combining areas of unallocated space in volumes that go across multiple disks. Multi-disk volumes also improve disk performance by letting more than one disk drive read and write data. Finally, multi-disk volumes let you use RAID technology to make volumes fault tolerant.

When you upgrade a disk so that it can contain dynamic volumes, Veritas Storage Foundation for Windows writes a small database onto the upgraded disk that contains volume management information about the disk and all other dynamic disks in its disk group. This database gives a dynamic disk additional advantages, which are as follows:

- Users can create dynamic volumes without restarting the system.
- Volumes can be accessed continuously, even across disk reconfiguration events.
- All dynamic volumes with an NTFS file system can be extended online. You can select where to extend the volume, or Veritas Storage Foundation for Windows assigns space optimally on the disks available within the volume's dynamic disk group.
- Disk configuration information is contained on the disk, not in the registry. The disk configuration information is also replicated across all dynamic disks in the disk group so that the failure of one disk does not obstruct access to data on other disks.
- Dynamic disks provide volume migration, which is the ability to move a disk or disks containing a volume or volumes from one system to another system without loss of data.
- Dynamic disks allow you to move portions of volumes (subdisks) between disks on a single computer system to optimize performance.

SFW's software RAID

To make the best use of SFW's dynamic volumes, you need an understanding of the RAID levels available with the program and what uses are appropriate for each RAID level. This section's topics are as follows:

- [What is RAID?](#)
- [SFW and Virtual Disk Service \(VDS\)](#)
- [Choosing RAID levels](#)
- [Hardware and software RAID](#)

What is RAID?

RAID (Redundant Array of Independent Disks) is a collection of specifications that describe a system for ensuring the reliability and stability of data stored on large disk subsystems.

RAID provides the following general benefits:

- Increased storage system reliability
- Improved I/O performance
- Fault tolerance

SFW and Virtual Disk Service (VDS)

Virtual Disk Service (VDS) provides a standard way to manage multi-vendor storage devices through a common storage interface. VDS focuses on the management of logical volumes through both software and hardware RAID. VDS supports the Disk Management user interface (Logical Disk Manager is the built-in default disk and volume manager that comes with Windows Server 2003 and Windows Server 2008) and two scriptable command line interfaces, DISKPART and DISKRAID.

DISKPART implements software RAID procedures. It deals with the creation, extension, and deletion of logical volumes or partitions on both basic disks and dynamic disks. DISKPART is the command line version of Disk Management.

DISKRAID implements hardware RAID procedures. It is used with vendor-specific hardware arrays to configure virtual disks (logical disks that span two or more independent physical disks).

In order for the common storage interface to work, participating hardware and software vendors must prepare their providers for the VDS software. Each hardware or software provider translates VDS standard APIs into instructions specific to the related storage device or software RAID procedures.

Storage administrators can use the scriptable command line utilities to create scripts to automate storage procedures across multi-vendor devices. The administrator creates the scripts using standard commands from the CLI, and therefore does not have to spend extra time to learn the specific management utilities that come with each hardware device or software RAID program. Once the script is set up, it can automate time-consuming procedures that had been done manually, such as adding storage to the network.

Where does Veritas Storage Foundation for Windows fit into this picture? When SFW is installed on a Windows Server 2003 system, it takes the place of Logical Disk Manager (LDM). Therefore, it must provide the functionality that LDM supplies, including a provider interface to VDS. This allows VDS applications, such as DISKPART or VDS-enabled third-party vendor applications, to continue to function. If SFW is uninstalled, LDM is restored as the native disk and volume manager for Windows Server 2003 and resumes its role with the VDS service.

For Windows Server 2008, the native disk and volume manager is Microsoft Disk Management. On a Windows Server 2008 system, SFW does not take the place of Microsoft Disk Management. SFW provides all the functionality as if it were installed on a Windows Server 2003 system with the added benefit that Microsoft Disk Management is still available. Uninstalling SFW does not affect Microsoft Disk Management.

Note: On Windows Server 2008, Microsoft Disk Management does not support objects created by SFW, such as dynamic disks or dynamic volumes.

At this time, the advanced functionality of Veritas Storage Foundation for Windows is not available through the Microsoft CLI VDS interfaces.

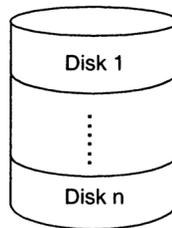
Choosing RAID levels

The following illustrations show how RAID levels (RAID-0, RAID-1, RAID-5, and RAID 0+1) provide various levels of redundancy and performance, compared with a simple volume on a single disk. From these, you can decide what choices are applicable to your particular situation.

Concatenated

Figure 1-1 shows a concatenated volume layout.

Figure 1-1 Concatenated volume layout



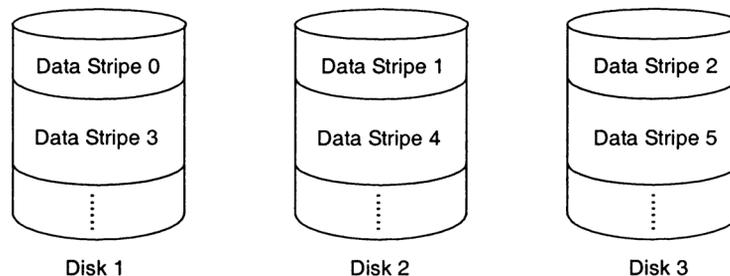
Concatenated volume layout offers the following:

- Concatenates n disks as one large virtual disk with a capacity of n disks.
- Data fills up the first disk before it is written to the second disk.
- Not fault tolerant. When a disk fails, the large virtual disk fails.
- No performance gain.

RAID level 0 (Striping)

Figure 1-2 shows a RAID-0 volume layout.

Figure 1-2 RAID-0 volume layout



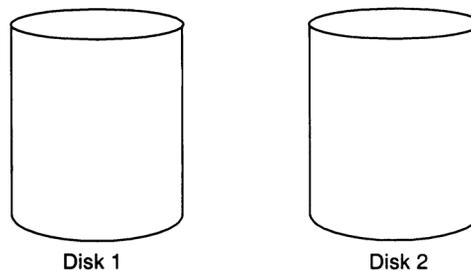
RAID-0 volume layout offers the following:

- Groups n disks as one large virtual disk with a capacity of n disks.
- Data is stored to the disks alternately.
- Not fault tolerant. When a disk fails, the large virtual disk fails.
- Better read and write performance than both simple volumes and all other RAID levels.

RAID level 1 (Mirroring)

Figure 1-3 shows RAID level 1 (mirroring).

Figure 1-3 Mirrored volume



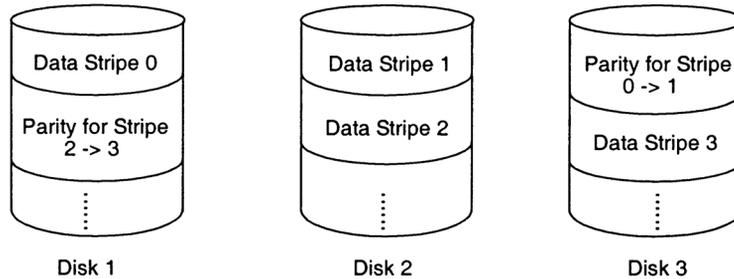
RAID level 1 (mirroring) volume layout offers the following:

- Groups two or more disks as one virtual disk with the capacity of a single disk.
- Data is replicated on each disk, providing data redundancy.
- When a disk fails, the virtual disk still works. The data is read from the surviving disk(s).
- Better read performance, but slightly slower write performance.
- Because data is duplicated on two or more disks, RAID-1 is more “expensive” in terms of disk space.

RAID level 5 (Striping with distributed parity)

Figure 1-4 shows RAID level 5 (striping with distributed parity).

Figure 1-4 RAID-5 volume layout



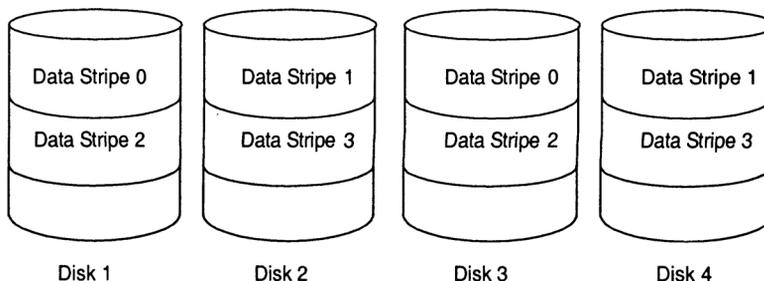
RAID-5 (striping with distributed parity) volume layout offers the following:

- Groups n disks as one large virtual disk with a capacity of $(n-1)$ disks.
- Redundant information (parity) is alternately stored on all disks.
- When a disk fails, the virtual disk still works. The data is reconstructed from the surviving disks and the parity alternately stored on the disks. You need to replace the failed disk to restore fault tolerance.
- Better read performance, but slower write performance.

RAID level 0+1 (Mirrored striped volumes)

Figure 1-5 shows RAID level 0+1 (mirrored striped volumes).

Figure 1-5 RAID 0+1 volume layout



RAID level 0+1 (mirrored striped volumes) volume layout offers the following:

- Stripes the data across two disks and mirrors it.
- When a disk fails, the data is read from the surviving mirror.
- Better read performance and write performance than RAID level 1 alone.

- Provides both redundancy (with mirroring) and performance (with striping).

Hardware and software RAID

RAID functions can be implemented with either hardware RAID (a specific RAID controller) or software RAID (software without the specific hardware).

Software RAID can be configured on top of the hardware RAID volumes and provide a powerful variety of features.

Setup and configuration

- [Setup and configuration summary](#)
- [Function overview](#)
- [Access Veritas Storage Foundation for Windows](#)
- [Review the Veritas Enterprise Administrator GUI](#)
- [Configure basic disks \(Optional\)](#)
- [Create dynamic disk groups](#)
- [Create dynamic volumes](#)
- [Set up a dynamic boot and system volume \(Optional\)](#)
- [Configure VCS and program options](#)
- [Set desired preferences](#)
- [Protecting your SFW configuration with vxabr](#)
- [Guidelines for running SFW](#)

Setup and configuration summary

This chapter presents the procedures for doing the initial setup and configuration of the Veritas Storage Foundation for Windows software once the program is installed on the server. It also describes how to work with disk groups that were created with earlier versions of the software, Veritas Volume Manager™ for Windows.

Note: Installation information is covered in the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Veritas Storage Foundation for Windows allows you to optimize your storage through the use of dynamic disk groups and dynamic volumes.

The main configuration tasks that you need to do are as follows:

- Create one or more disk groups
- Create dynamic volumes for each disk group
- Set up a dynamic boot and/or system volume (optional)
- Configure options
- Set preferences

Function overview

Before you can configure Veritas Storage Foundation for Windows, you need an understanding of the main concepts in the program.

This section gives an overview of these concepts and has the following topics:

- [Basic and dynamic disks](#)
- [Basic and dynamic volumes](#)
- [Disk groups](#)
- [Dynamic volume components](#)

Basic and dynamic disks

Physical disks under SFW's control are either basic or dynamic. When you install Veritas Storage Foundation for Windows initially on a new system, all disks on a computer system are defined as basic disks. You can upgrade them to dynamic disks by making the disks part of a dynamic disk group.

Basic and Dynamic disk details are as follows:

Basic Disks	Basic disks adhere to the partition-oriented scheme of Windows NT, Windows 95/98, and MS-DOS. Basic disks can also contain RAID volumes that were created in NT Disk Administrator. In addition, CD-ROMs and other removable media are considered basic disks.
Dynamic Disks	Dynamic disks can contain dynamic volumes created with Veritas Storage Foundation for Windows. The five dynamic volume types are concatenated (includes simple and spanned volumes), mirrored, striped, RAID-5, and mirrored striped (RAID 0+1). On a dynamic disk, space is organized through dynamic volumes rather than partitions.

Because a dynamic disk does not have the partitioning scheme used by Windows NT, Windows 95/98, and MS-DOS, you cannot access dynamic disks through those operating systems. If you have a dual-boot system with both Windows Server 2003 or later release and an earlier Windows operating system or MS-DOS, you need to retain some basic disks for use with the alternate operating system.

Basic and dynamic volumes

A volume is a logical entity that is made up of a portion or portions of one or more physical disks. A volume can be formatted with a file system and can be accessed by a drive letter or a mount path. Like disks, volumes can be basic or dynamic. Volumes are defined as basic or dynamic, depending on whether they reside on a basic or dynamic disk.

Basic and Dynamic volume details are as follows:

Basic Volumes Basic volumes can be primary or extended partitions, simple logical drives that reside on extended partitions, or RAID volumes that were originally created in Windows NT Disk Administrator.

Dynamic Volumes Dynamic volumes are volumes created on dynamic disks by using Veritas Storage Foundation for Windows. You can create any number of dynamic volumes in unallocated space on one or more disks.

The volumes are created online without the need for rebooting (except a boot or system volume). Each volume can have a FAT, FAT32, or NTFS file system.

SFW's volumes are internally organized according to established RAID levels.

See "[SFW's software RAID](#)" on page 30.

You can do online extending of all dynamic volume types, and you can add up to 32 mirrors to any volume type, except RAID-5.

The dynamic volumes created by SFW are accessed by the Windows Server 2003 and Windows Server 2008 operating systems in the same way that physical partitions are accessed. The volumes are identified by a drive letter or mount point.

Although you cannot create new NT Disk Administrator-type volumes on a basic disk, you can upgrade them to dynamic. Then these volumes will have the full capabilities of other SFW dynamic volumes.

About dynamic volumes in SFW basic

As in SFW, dynamic volumes can be created in SFW Basic. However, SFW Basic is limited to a maximum of four dynamic volumes. Upgrading SFW Basic to SFW allows you to create any number of dynamic volumes.

Disk groups

All basic and dynamic volumes are required to be in a disk group. There is only one disk group for basic disks, known as the Basic disk group (or BasicGroup in the GUI). There can be one or more dynamic disk groups. A dynamic disk group contains dynamic disks managed by SFW.

When you move disks between computers, you use the Import and Deport Dynamic Disk Group commands. The disk group for clusters is called a cluster disk group.

See [“Dealing with disk groups”](#) on page 193.

See also [“Microsoft Clustering support”](#) on page 753.

On Windows Server 2008, there are two different types of dynamic disk groups, the Microsoft Disk Management Disk Group and the SFW dynamic disk group. The Microsoft Disk Management Disk Group is a disk group that can be created by Microsoft Disk Management. In the VEA GUI, this type of disk group is distinguished with an icon containing the character “M”. In addition to the SFW disk groups, SFW can also create and manage the Microsoft Disk Management Disk Group.

Dynamic volume components

The components or virtual storage objects involved in a dynamic volume include its disk group, the dynamic disks it is associated with, and its plexes, columns, and subdisks. The terms “dynamic disk” and “dynamic disk group” have been defined in the preceding sections. The definitions for plexes, columns, and subdisks are given below:

Plexes

A plex refers to an instance of the volume. Mirrored volumes have two or more plexes. All other volumes have one plex.

Columns

A column refers to an area on the disk where all or a portion of the volume resides. Striped, RAID-5, and mirrored striped (RAID 0+1) volumes contain multiple columns. Other volume types contain one column.

Subdisks

Subdisks identify the disk location and size of each contiguous disk area in the volume. Subdisks are the basic units in which Veritas Storage Foundation for Windows allocates disk space in a volume. A SFW disk can be divided into one or

more subdisks. Each subdisk represents a specific portion of a volume on a dynamic disk.

An SFW disk may contain multiple subdisks, but subdisks cannot overlap or share the same portions of disk space. Any SFW disk space that is not part of a subdisk is considered to be unallocated space, which can be used to create new volumes or to extend existing volumes.

You can move subdisks to improve disk performance.

See [“Moving subdisks”](#) on page 544.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support operations on subdisks.

Access Veritas Storage Foundation for Windows

To access Veritas Storage Foundation for Windows, you must have installed the program on the servers to be managed and on any client machine that is used to manage the program remotely.

For complete installation instructions, see the Installation Guide.

SFW is accessed through the Veritas Enterprise Administrator (VEA) GUI interface. The VEA GUI is used for multiple Symantec programs.

If SFW has been installed correctly, then the VEA GUI can be accessed through either the **Start** menu or the Computer Management window of the server or the client machine you are using. Once you access the VEA GUI, you then need to connect to one or more servers that you want SFW to manage.

This section describes how to use these two methods to access VEA and to connect to a server.

The section's topics are as follows:

- [Accessing VEA through the Windows start menu](#)
- [Accessing VEA through the Windows computer management window](#)
- [Disabling write caches and HBA caches](#)
- [Disconnecting from a server](#)
- [Understanding the conditions for remote connection](#)

Note: To access and perform operations within Veritas Storage Foundation for Windows, you must have administrator rights on the machine you want to connect to. Not having administrator rights only allows you to view information in Veritas Storage Foundation for Windows.

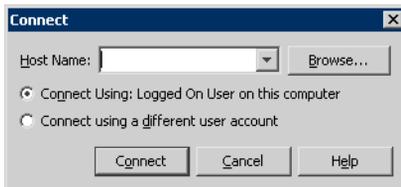
See "[Understanding the conditions for remote connection](#)" on page 46.

Accessing VEA through the Windows start menu

To access VEA through the start menu and connect to a server

- 1 Select **Start>Programs>Symantec>Veritas Storage Foundation>Veritas Enterprise Administrator**.
The Select Profile window appears.
- 2 Select a profile and click **OK** to continue.
The Veritas Enterprise Administrator window appears.
- 3 Click **Connect to a Host or Domain** to connect.
The Connect window appears.

- 4 Select a Host from the drop-down menu, click Browse to find a Host, or enter the Host name of the computer and click **Connect**.



You may also choose to connect using a different user account after selecting a Host. In this case, you will be prompted for another username and password to connect with.

Accessing VEA through the Windows computer management window

To access VEA through the computer management window and connect to a server

- 1 Right-click the **My Computer** icon and select **Manage** from the context menu that appears.
The Computer Management window comes up.
The window's display can represent a local computer or a remote computer.
 - If the window is representing the local computer, "(Local)" appears after the Computer Management node in the tree view.
 - If a remote computer is being represented, the name of the remote computer appears after the Computer Management node.The default setting is for the window to display the local computer as the top node.
- 2 To connect to a different computer, right-click the top node of the Computer Management tree view and select **Connect to another computer** from the context menu. In the Select Computer window that appears, click **Local** or **Another computer**.
For another computer, enter or browse for the name of the appropriate computer. Click **OK** to connect. You may be asked to enter a user name and password.
- 3 In the Computer Management tree view, expand the Storage node and the Volume Management node that appears under it.
If the server is running SFW or a version of Volume Manager for Windows, **Veritas Enterprise Administrator** appears under the Volume Management node.

- 4 Double-click **Veritas Enterprise Administrator**.
The Veritas Enterprise Administrator GUI comes up with the Select Profile window displayed.
- 5 Select a profile and click **OK** to continue.
The Veritas Enterprise Administrator console appears.

Disabling write caches and HBA caches

Write caches

Write caches for disks and disk arrays improves disk performance, but the cached data may be lost in an unplanned disk shutdown. In general, Symantec recommends that write caches be disabled to avoid any possible data loss. However, write caches may be enabled for disks and disk arrays that have an emergency backup power source for their caches.

It may be possible to disable the write cache for a disk by using the Windows Computer Management GUI as shown in the following steps.

- 1 Select Device Manager in the left pane of Windows Computer Management.
- 2 Expand Disk Drives in the right pane to display the disks.
- 3 Right-click the appropriate disk and select Properties from the context menu.
- 4 Click the Disk Properties tab and clear the checkbox for Write cache enabled.
- 5 Click OK to save and close your setting.

Refer to your hardware documentation for additional information about disabling the write cache.

If you choose to have the write cache enabled, the warning message about write cache enabled disks is displayed during startup. This message can be turned off by clearing the checkbox for Show write cache enabled information in the Storage Foundation General tab of the Preferences GUI.

For more information about turning off the message, see [“The disk view”](#) on page 103.

HBA caches

Some storage devices, such as RAID controllers, may have HBA caches. If these storage devices are used in a cluster environment, such as Microsoft Clustering or VCS, the data in the cache of a failed system has the potential of corrupting the data in the cluster. Symantec recommends that the HBA caches be disabled for these devices. Refer to your hardware documentation for information about disabling HBA caches.

Disconnecting from a server

- 1 Right-click the server icon you want to disconnect from, and select **Disconnect** from the computer context menu. Alternatively, you can select **Disconnect** from the **File** menu or click the **Disconnect** tool on the toolbar, the second tool from the left (the small computer with a red checkmark).
- 2 A confirmation dialog appears; click **OK** to end the connection. The computer icon disappears from the tree view. If the connection is lost for any other reason, a message appears that indicates the connection has been terminated. SFW removes the icon for that computer from the tree view. You need to click **OK** to close the message box.

Understanding the conditions for remote connection

This section describes the conditions for connecting to a remote computer. You are able to connect to a remote computer if it is established that your user name and password match those of an account with any of the following:

- Local Administrator rights of the remote server
- Domain Administrator rights of the domain of the remote server and you have logged on from that domain or a trusted domain
- Domain Administrator rights of a trusted domain to the remote server's domain and you have logged on from that domain or the remote server's domain

When you initiate the command to connect to a remote computer, Veritas Storage Foundation for Windows checks to see whether you have already met one of the three conditions above when you logged on initially to the local client computer. If you have, then you will be connected directly to the remote computer without being asked to supply a user name and password.

You will not be connected automatically if you have logged onto the local computer with an account that does not have administrator privileges on the remote machine you want to connect to. However, with the **Connect** command in the VEA GUI, you are always given the opportunity to enter a user name and password. Click the **More** button in the Connection dialog box to expand the dialog box and display the Authentication section. If you then enter a user name and password for an administrator account on the remote machine, you will be connected to the remote computer.

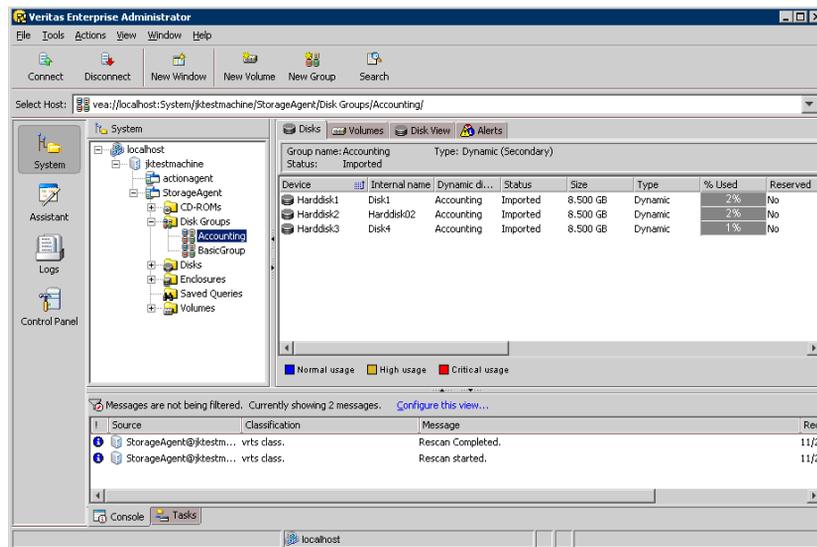
Note: The first time you enter a user name and password, you can click the **Remember password** checkbox, so that you do not have to enter the password every time.

Review the Veritas Enterprise Administrator GUI

Once you have connected to one or more servers, you are able to use the VEA GUI to view and manage the connected servers. This section gives a brief overview of the VEA GUI so that you may understand how to use the GUI to accomplish the tasks needed to set up and configure the Veritas Storage Foundation for Windows program on the server.

If you look in the right pane of the VEA GUI window, you should see an icon representing the server or servers that you are connected to. There are additional icons for all of the storage components associated with the server. By viewing these icons, you are able to see at a glance how the different storage components on the server are organized and whether they are functioning normally.

Figure 2-1 VEA GUI window



The key points about the VEA GUI are as follows:

- The tree view in the left pane provides an efficient overall view of the storage.
In the GUI, the different components of the storage being managed by Veritas Storage Foundation for Windows are represented as icons. The top level of the tree is the management console icon. Under it are the servers being managed by SFW. Under each server are the storage components associated with it—CD-ROMs, disk groups, disks, and volumes. By clicking

on the + or - sign in front of an icon, you can display or hide subordinate icons under that icon. The Control Panel icon for each server gives access to further settings that can be applied to the storage objects. The Logs icon brings up an Event Log and a Task Log relating to the storage objects.

- If there is a problem with one of the storage components, a small error symbol is superimposed on the icon. A yellow caution symbol indicates there is a potential problem. A red circle with an x on it indicates that a serious storage failure has occurred, such as a disk failure. See “[SFW error symbols](#)” on page 476.
- Selecting a storage object in the tree view brings up further information relating to that object in the right pane of the GUI window. For example, if you expand the Disks icon in the tree view and click a particular disk, the right-pane view displays the volumes on that disk. That right-pane view for the disks has two other tabs, **Disk Regions** and **Disk View**. Disk Regions shows you subdisks (that is, parts of volumes that reside on the disk) and free space. The Disk View represents the same disk regions in a diagram and provides additional information. The tabs in the right pane change, depending on what storage object is selected in the tree view.
- Right-clicking a storage object in the tree view or right-pane view brings up a context-sensitive menu with the commands that are appropriate to that storage object. For example, two tasks that are necessary in setting up storage under Veritas Storage Foundation for Windows are to create disk groups and volumes. You can right-click the **Disk Group** icon or a disk icon and a menu will come up that includes the command **New Dynamic Disk Group**. Likewise, once a dynamic disk group is created, you can click the **Disk Group** icon or an icon of a disk that is included in a dynamic disk group and a menu comes up that includes the command **New Volume**.
- You can also select commands from the menu bar and the toolbar. Again, the commands on each menu can vary, depending on what storage object you have selected.
- The lower pane of the GUI is used to display recent alerts relating to the storage objects, or it can also show the progress of storage tasks, such as formatting of a volume. To toggle back and forth between the two purposes, click the **Console** or **Tasks** tab at the lower left corner of the pane. See also “[Using the GUI to manage your storage](#)” on page 83.

Note: If you are installing on a new system with new disks or you have added new disks to the system, such disks show up in the tree view with the words “No Signature” after them. Right-click each disk and select **Write Signature** from the context menu.

See “[Add a disk signature to a disk](#)” on page 139.

Configure basic disks (Optional)

The Veritas Storage Foundation for Windows program defines disks as being either basic or dynamic. Basic disks are disks other than the ones that have been defined through SFW as dynamic. In most cases, it is not necessary to configure basic disks for your initial setup and configuration of SFW.

This section provides information about basic disks and describes the situations where you might want to use the commands provided within SFW to configure basic disks.

Topics are as follows:

- [About basic disks](#)
- [Upgrading basic disks to dynamic](#)

About basic disks

Basic disks are disks that have the standard partitioning scheme used by Windows NT, Windows 95/98, and MS-DOS. When you install Veritas Storage Foundation for Windows on a new system, all physical disks on your system are defined as basic, even though they may not all have partitions on them. If the Windows operating system is installed, you will have your system and boot partition already set up as a basic disk partition. This partition is created as a part of the Windows install process. Once Veritas Storage Foundation for Windows is running, you do not need to create any more basic disk partitions. You can then set up dynamic disk groups and volumes with your remaining storage to make them into dynamic disks. It is not necessary to place partitions on a new disk for it to be made into a dynamic disk through Veritas Storage Foundation for Windows.

Upgrading basic disks to dynamic

All basic disks can be upgraded to dynamic disks through Veritas Storage Foundation for Windows. To upgrade a basic disk to a dynamic disk, you need to create a dynamic disk group and include the disk in the group.

See [“Create dynamic disk groups”](#) on page 53

The basic disk does not have to include a partition on it; but if it does, a primary partition becomes a simple dynamic volume and any logical drives within an extended partition also become simple volumes. The extended partition will no longer exist.

The process of upgrading a basic partition to a dynamic volume is called “encapsulation,” because it encapsulates the partition information within the dynamic volume structure.

You can also upgrade your system and boot partition to a dynamic disk and then mirror it.

See [“Set up a dynamic boot and system volume \(Optional\)”](#) on page 70.

Create dynamic disk groups

When you create a dynamic disk group and add disks to it, those disks become dynamic—that is, they can now have Veritas Storage Foundation for Windows dynamic volumes created on them. Thus, a basic disk is said to be “upgraded to a dynamic disk” through its addition to a dynamic disk group. You can change multiple basic disks to dynamic at one time when you use either the **New Dynamic Disk Group** command or the **Add Disk to Dynamic Disk Group** command.

This section on creating dynamic disk groups has the following topics:

- [Considerations when changing a basic disk to dynamic](#)
- [Steps for creating a dynamic disk group](#)
- [Making storage available after system startup](#)

In this setup and configuration chapter, only the command for creating a dynamic disk group is included.

For information on adding a disk to a disk group, see the following topic:

- [Add a disk to a dynamic disk group.](#)

Considerations when changing a basic disk to dynamic

You need to consider the following:

- Once you change a basic disk to a dynamic disk, the volumes on the disk cannot be accessed by MS-DOS, Windows 95/98, or Windows NT.
- After you upgrade a basic disk to a dynamic disk and create dynamic volumes on it, you cannot change the dynamic volumes back to partitions or basic volumes. You can revert a dynamic disk to basic, but you must delete all dynamic volumes on the disk and then use the **Remove Disk from Dynamic Disk Group** command.
- In Windows Server 2008, you can upgrade a basic disk to a dynamic disk that can be contained in a Microsoft Disk Management Disk Group or in an SFW dynamic disk group.
 - If you upgrade a basic disk to a dynamic disk in a Microsoft Disk Management Disk Group, you can add it to an existing Microsoft Disk Management Disk Group or use it to create the Microsoft Disk Management Disk Group. You are not able to have more than one Microsoft Disk Management Disk Group.
 - If you upgrade a basic disk to a dynamic disk in an SFW dynamic disk group, you can add it to an existing SFW dynamic disk group or use it to

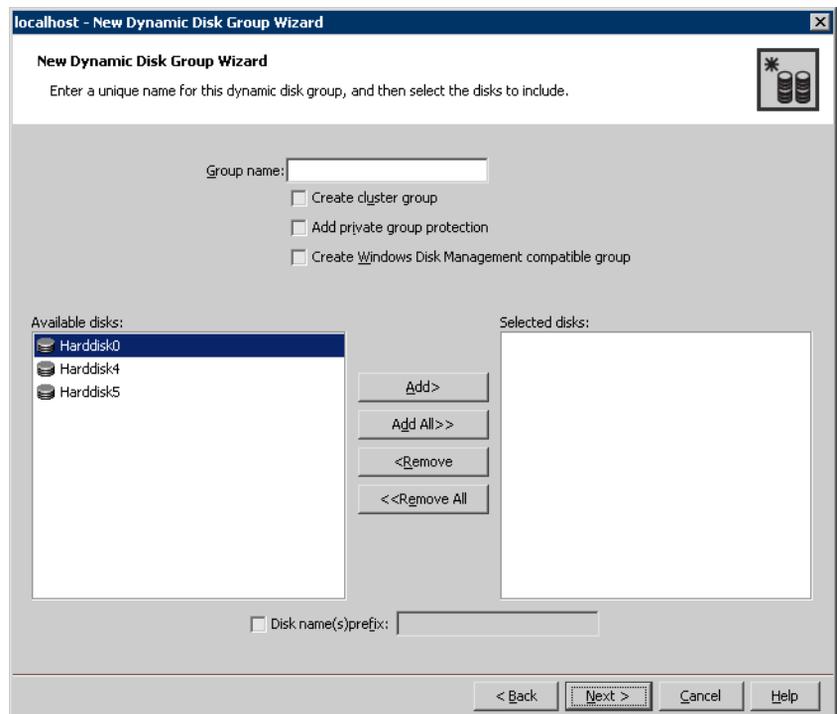
create an SFW dynamic disk group. You are able to have multiple SFW dynamic disk groups.

- To create a bootable dynamic disk that can be mirrored, you must upgrade a basic disk that contains the system partition to a dynamic disk. See “[Set up a dynamic boot and system volume \(Optional\)](#)” on page 70.

Steps for creating a dynamic disk group

To create a new dynamic disk group

- 1 Right-click the **Disk Groups** folder or right-click a disk.
- 2 Select **New Dynamic Disk Group** from the context menu that comes up. The New Dynamic Disk Group Wizard screen appears. The wizard can also be reached by clicking the **New Dynamic Disk Group** button on the Storage Foundation Assistant.
- 3 Click **Next** to continue. A screen comes up for naming the disk group and for selecting its disks and type.



- 4 Enter a name for the dynamic disk group, and indicate which disks you want to include in the group. Also consider whether you want the disks to be part of a regular disk group or one of the optional disk group types, which are defined in the table below. If you click none of the optional disk group type checkboxes, you will create a regular dynamic disk group.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support cluster disk groups.

If you already have disk groups on your Windows Server 2003 system that were created in Windows 2000 Disk Management or in Volume Manager 2.7 or earlier, you might want to consider the Disk Management compatible dynamic disk group type.

Make sure only the disks you want to include are listed in the right pane of the window (**Selected disks**), and click **Next**.

Check the **Disk names prefix checkbox** and enter a disk name prefix to give the disks in the disk group a specific identifier. The identifier precedes a system-generated numeric ID that SFW uses to distinguish the disks in the disk group. For example, entering TestGroup as the prefix for a disk group that contains three disks creates TestGroup1, TestGroup2, and TestGroup3 as internal names for the disks in the disk group.

Note: A dynamic disk group name is limited to 18 ASCII characters. It cannot contain spaces or forward or backward slashes. Also, a period cannot be the first character in the name.

Table 2-1 Optional Disk Group Types

Disk Group Type	Description
Cluster Dynamic Disk Group	Creates a cluster dynamic disk group that can be used with VCS or Microsoft Clustering.
Private Dynamic Disk Group Protection	The feature of private dynamic disk group protection makes it possible to partition shared storage with a regular dynamic disk group. See “Partitioned shared storage with private dynamic disk group protection” on page 209.

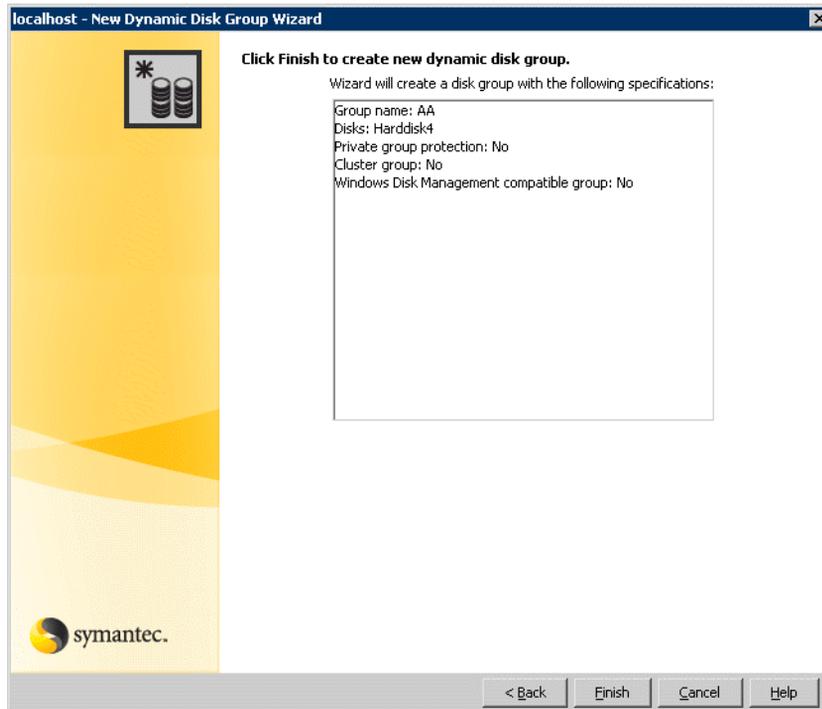
Table 2-1 Optional Disk Group Types

Disk Group Type	Description
Windows Disk Management Compatible Dynamic Disk Group	For Windows Server 2003, this creates a disk group that is compatible with the disk groups created with Windows Disk Management and with earlier versions of Volume Manager for Windows products. Starting in Volume Manager 3.0 (and later Volume Manager releases) and all SFW releases, disk groups have enhanced capabilities and are not compatible with these earlier disk groups. You can upgrade the earlier-style disk groups by using the Upgrade Dynamic Disk Group Version command.
Windows Disk Management Disk Group	For Windows Server 2008, this creates a Windows Disk Management disk group. This is the type of disk group that is created by Microsoft Disk Management. See “Upgrade a dynamic disk group version” on page 199.

- 5 The next screen confirms the disks you have selected. Choose **Next** to continue if you are satisfied with the disk selection. If you are not satisfied, you can click the **Back** button to go back to the previous screen in order to modify your disk choices.

For each disk, information is provided on whether it contains volumes and whether it will be updated. If it is not going to be updated, you will want to modify the selection.

Normally, you would add all the disks you want in the group at this point. You can always add more disks later with the **Add Disk to Dynamic Disk Group** command.



- 6 Click **Finish** in the final screen.
The next step in the process is to create dynamic volumes.

Making storage available after system startup

Generally, dynamic (non-cluster) disk groups are available during system startup. However, some types of storage are not available until the service that controls the storage has been started. SFW provides the Veritas DG Delayed Import Service (VxDgDI) to accommodate this type of storage. VxDgDI and the `vxdg latestart` command allow SFW to access the storage when it becomes available.

See “[vxdg latestart](#)” on page 322.

Create dynamic volumes

This section on creating dynamic volumes has some useful background information, as well as the detailed steps for carrying out the procedure.

Background information

Dynamic volume layouts or types

There are five dynamic volume layouts or types—concatenated (simple or spanned), mirrored, striped, RAID-5, and mirrored striped (RAID 0+1).

See “[Dynamic volume types](#)” on page 67.

Volume size in the new volume wizard

It is important to understand that the total volume size you indicate for the volume in the New Volume wizard is the *usable* size for storing the data. Depending on the layout type, the volume can take more space on the disk. The size shown in the wizard for simple, striped, and spanned volumes is the actual volume size on the disk. A RAID-5 volume requires additional space for parity information, and a mirrored volume is a multiple of the space taken by the original plex of the volume.

The wizard provides a **Max Size** button to determine the size of the volume. Again, this is the usable size of the volume rather than the actual size taken by the volume on the disk.

Preselecting disks

You can preselect one or more disks before invoking the **New Volume** command. For example, you can click a specific disk in the tree view or select several disks in the right pane and then invoke the command from the context menu. If you have a disk or several disks selected, the program assumes that only the selected disks will be used for the volume and the manual selection radio button will be indicated in the New Volume wizard. If you find that you want to use more disks than those originally selected, you can adjust the disk selection from within the wizard.

Thin Provisioned disks

Volumes can be created with disks that are enabled to support thin provisioning and storage reclamation. Using thin provisioned disks for a volume allows for efficient allocation of storage for the volume. A disk that supports thin provisioning is represented with a disk icon that includes a red colored

sector. A disk that supports thin provisioning and storage reclamation is represented with a disk icon that includes a green colored sector with an asterisk (*).

Note: The operation to reclaim storage from thin provisioned disks is not supported for RAID-5, DCO, or VVR DCM volumes.

Note: The operation to reclaim storage is supported only for NTFS volumes.

About dynamic volumes in SFW basic

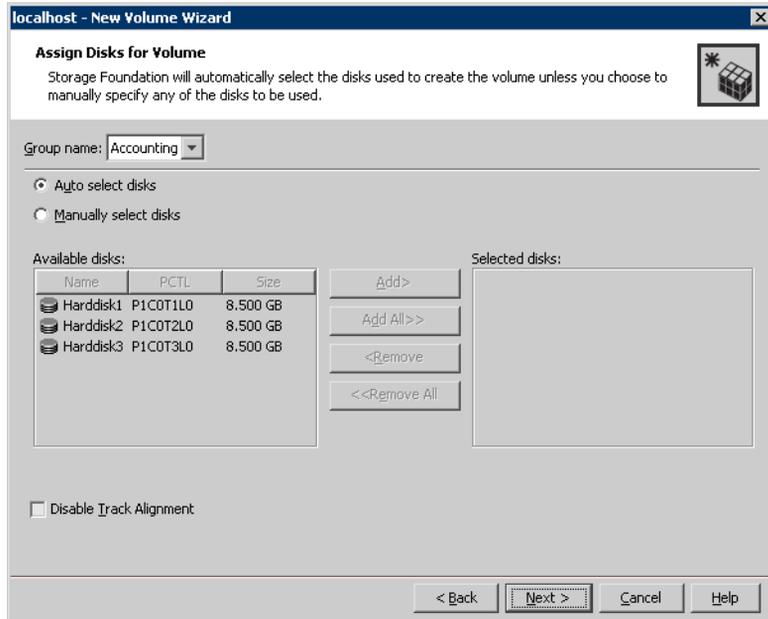
As in SFW, dynamic volumes can be created in SFW Basic. However, SFW Basic is limited to a maximum of four dynamic volumes. Upgrading SFW Basic to SFW allows you to create any number of dynamic volumes.

Steps for creating a dynamic volume

To create a new volume

- 1 Right-click a dynamic disk in the tree view, the right pane, or the **Disk View** tab, and select **New Volume** from the context menu that comes up.
You can also select the command from the **Actions** menu or click the **New Volume** tool on the toolbar.
- 2 The New Volume wizard appears.
Click **Next** to continue.

The Assign Disks for Volume screen appears.



- 3 Make your selections in the Assign Disks for Volume screen.
 - A default dynamic disk group will appear in the **Group name** box. If you wish to create the volume in a different dynamic disk group, select it from the pull-down list.
 - Automatically selecting disks is the default setting. To manually select the disks, click the **Manually select disks** radio button. The disks that you select should be in the right pane when you click **Next**.
If you had one or more disks selected when you invoked the **New Volume** command, the disk selection method will be set to manual. You may view disks that are only enabled for thin provisioning, by checking the checkbox for Thin Provisioned Disks. Using this checkbox allows you to manually select only thin provisioned disks to create the volume.
 - You may also check **Disable Track Alignment** to disable track alignment for the volume.
Disabling Track Alignment means that the volume does not store blocks of data in alignment with the boundaries of the physical track of the disk.
For more information about Track Alignment, see “[Track alignment](#)” on page 134.

Click **Next** to continue. The screen for selecting volume attributes appears.

- 4 Select the attributes listed below for the volume, and click **Next** to continue.

localhost - New Volume Wizard

New Volume Wizard
Select the attributes for this volume.

Volume name: AcctVolume

Size: 300 MB Max Size

Layout

Concatenated Columns: 2

Striped Stripe unit size (Sectors): 128

RAID-5 Stripe across: Port

Mirror Info

Mirrored

Total mirrors: 2

Mirror across: Port

Enable logging

Striped: A volume with a single copy of data across multiple disks.

< Back Next > Cancel Help

If you find the volume layout that you want is grayed out, it is most likely because not enough disks have been selected. Choose the **Back** button and return to the previous screen to select more disks.

- The volume name is the internal Veritas Storage Foundation for Windows-specific name that is used in some SFW commands. Enter a name in the **Volume name** text box.

A volume name is limited to 18 ASCII characters. It cannot contain spaces or forward or backward slashes. Also, a period cannot be the first character in the name.

If you enter a volume name, SFW will automatically assign the file system volume label the same name. If you later change the file system volume label through the **File System** command, the Veritas Storage Foundation for Windows volume name and the file system volume label will be different. However, it will make little difference because the GUI identifies the volume by the file system label name except for the one entry that is listed as “Volume Name.” If you use the command line interface to create a volume, the file system name is not automatically set to the name of the volume.

- Select one of the following volume layout types:

- Concatenated
- Striped
- RAID-5
- Mirrored
- Mirrored Striped (RAID 0+1) – choose **Striped** and the **Mirrored** checkbox

For a detailed description of the volume layout types, see “[Dynamic volume types](#)” on page 67.

If you are creating striped or RAID-5 volumes, the **Columns** and **Stripe unit size** must be specified. The stripe unit size is expressed as a number of sectors. Default values are provided.

In addition, you may specify to have the stripe across disks done by Port, Target, Enclosure, or Channel.

For a concatenated or striped volume, you may also specify a mirror volume with the following optional attributes:

- Number of mirrors
- Enable logging
- Mirror across disks by Port, Target, Enclosure, or Channel

Note that the operation to create a new dynamic volume fails if the appropriate resources are not available to support the selected attributes to mirror across disks.

- Provide a size for the volume. You can use the pull-down list to the right of the **Size** entry box to select Sectors, KB, MB, GB, or TB for indicating the volume size.

If you click the **Max Size** button, a size appears in the **Size** box that represents the maximum possible volume size for that layout in the dynamic disk group. For a given dynamic disk group, the maximum volume size will depend on the type of layout selected.

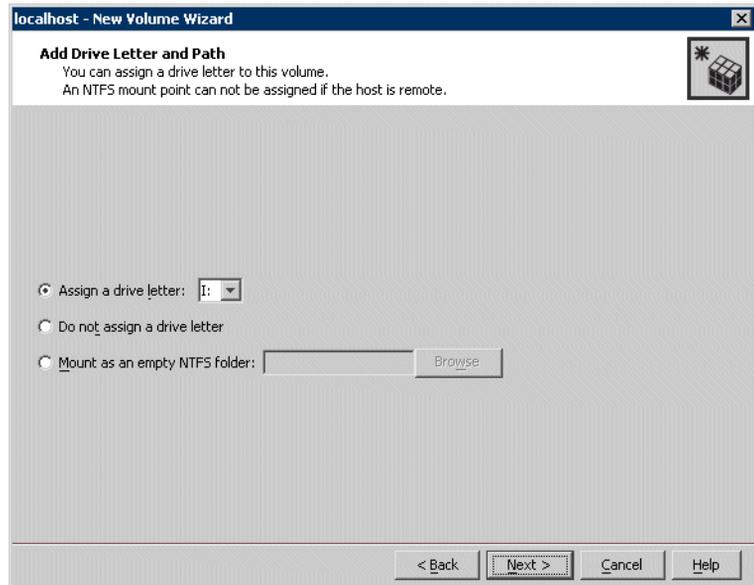
Click **Next** to continue.

- 5 In the Add Drive Letter and Path screen, select one of the three choices described below, and click **Next**.

The options are as follows:

- Accept the drive letter assignment indicated or assign a drive letter by using the pull-down list.
- Do not assign a drive letter. You may prefer to do this task later.
- Mount as an empty NTFS folder by clicking the option and then typing in a folder name or browsing to select the folder name. Veritas Storage

Foundation for Windows will create a new folder for you if you click the **New Folder** button in the Browse for Drive Path dialog box.

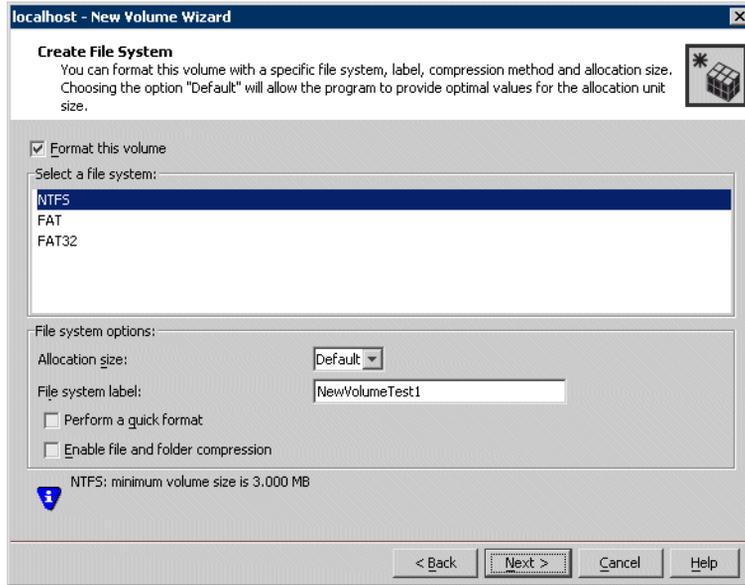


- 6 In the Create File System screen that appears next, indicate your choices for the file system selections that are described below, and click **Next**.

The options are as follows:

- Make sure that the **Format this volume** checkbox is checked if you want to format the volume using NTFS, FAT, or FAT32. You can uncheck the box if you want to format later.
- Make sure the file system type that you want is highlighted if you want to format the volume now.
- If desired, change the allocation size. The default size is recommended.
- If desired, type a file system label. If you do not enter a label, no default label will be provided. You can enter a label for the file system later.
- Decide if you want to perform a quick format. If the **Perform a quick format** box is not checked, the volume will be formatted with normal formatting.

- If desired, check the **Enable file and folder compression** checkbox. This option is available only if the volume is being formatted with NTFS.



If you want to format the volume, create a file system label, or change any of the settings shown in the screen above after the volume is created, right-click the volume and select **File System** and the subcommand **New File System** from the volume context menu. You will be able to make your choices from a screen that has the same selections as the one above.

- 7 Check your selections in the final screen. When you are satisfied with your choices, click **Finish**.

By clicking the **Back** button, you can go back and make changes before you click **Finish**.

If you chose to format the volume, Veritas Storage Foundation for Windows will begin the formatting process. Click the **Tasks** tab in the bottom left corner of the lower pane to see a text entry indicating the status and progress of the formatting process.

By default, the dynamic volume is created as a read/write volume. To make the dynamic volume a read only volume, right-click the volume and check **Read only** in the Properties for the volume.

Dynamic volume types

This section provides a detailed description on the five types of dynamic volumes it is possible to create and use in Veritas Storage Foundation for Windows.

The types are as follows:

- [Concatenated \(Simple and spanned\) volumes](#)
- [Striped volumes](#)
- [Mirrored volumes](#)
- [RAID-5 volumes](#)
- [Mirrored striped volumes \(RAID 0+1\)](#)

Note: In the Veritas Storage Foundation for Windows **New Volume** command, simple and spanned volume types are both referred to as concatenated and considered one type.

Concatenated (Simple and spanned) volumes

The concatenated volume type includes both simple and spanned dynamic volumes.

Simple volumes

A dynamic simple volume consists of a single contiguous region (or subdisk) on a single physical disk. Dynamic simple volumes can be extended or mirrored. When you extend a simple volume to a noncontiguous region within the same disk or onto additional disks, it becomes a spanned volume.

Spanned volumes

A dynamic spanned volume consists of two or more subdisks (single contiguous regions) on one or more disks. With a spanned dynamic volume, you can combine sections of unallocated space from multiple dynamic disks into one large volume. The areas of unallocated space used to create spanned volumes can be different sizes. Spanned volumes are organized sequentially—that is, Veritas Storage Foundation for Windows sequentially allocates space on each disk until that disk is full and then continues with the next disk until the volume size is reached. Up to 256 disks can be included in a spanned volume.

Existing spanned volumes can be extended by the amount of unallocated space on all the disks in the dynamic disk group. However, after a spanned volume is extended, no portion of it can be deleted without deleting the entire spanned volume.

The advantage of a spanned volume is that it allows you to create a large volume consisting of smaller pieces of disk space from several disks, thereby making more efficient use of the disk space than would be possible if you had to limit the volume to a single disk. The disadvantage of a spanned volume is that it is not fault tolerant. If one of the disks containing a spanned volume fails, the entire volume fails. However, a spanned volume can be mirrored.

Striped volumes

Striped volumes are created by combining areas of free space on two or more disks into one logical volume. Data is divided into blocks and spread in a fixed order among all the disks in the volume. With a striped volume, data is written to multiple disks, similar to spanned volumes. However, striping writes files across all disks so that data is added to all disks at the same rate. Up to 256 disks can be used in a striped volume.

Striped volumes offer the best performance of all the disk management strategies. However, as with spanned volumes, striped volumes do not provide fault tolerance. If a disk in a striped volume fails, the data in the entire volume is lost. However, a striped volume can be mirrored to provide data redundancy. In addition, Veritas Storage Foundation for Windows allows you to extend a striped volume, either with or without a mirror.

Mirrored volumes

A mirrored volume is a fault-tolerant volume that duplicates your data on two or more physical disks. A mirror provides redundancy by simultaneously writing the same data onto two or more separate mirrors (or plexes) that reside on different disks. If one of the disks fails, data continues to be written to and read from the unaffected disk or disks.

Mirrored volumes protect the data on the disk from media failure. Mirroring reduces the chance of an unrecoverable error by providing duplicate sets of data, but it also multiplies the number of disks required for data storage and the input/output (I/O) operations when writing to the disk. However, some performance gains are achieved for reading data because of I/O load balancing of requests between the plexes. A mirrored volume is about the same as a RAID-5 volume in read operations but faster in write operations.

You can create a mirrored volume with the Create Volume wizard, or you can add a mirror to an existing volume with the Add Mirror wizard. To create a mirrored volume on two or more disks, each mirror or plex of the original volume requires space that is at least the same size as the original volume. When you create a mirror, the same drive letter is used for all plexes of the volume. If you have sufficient disks available, you can create multiple mirrors

for extra redundancy (up to the limit of 32 mirrors). Then, you can break off a mirror to use for backup, data analysis, or testing without losing redundancy.

Note: Adding a mirror to a volume involves a certain amount of time for mirror resynchronization. The SmartMove feature can help reduce mirror resynchronization time. See “[SmartMove](#)” on page 130.

Breaking off a plex of the mirrored volume does not delete the information, but it does mean that the plex that is broken off will no longer mirror information from the other plex or plexes in the mirrored volume. The broken-off plex will be assigned a different drive letter than that of the original mirrored volume. It is no longer part of the mirrored volume, but it retains its other volume layout characteristics. For example, if you had a mirrored striped volume, the broken-off plex would become a striped volume.

In the case of an unrecoverable error on a plex within a mirrored volume, you need to remove the plex that is damaged with the **Remove Mirror** command. You then can use the **Add Mirror** command to create a new plex on another disk to take the place of the damaged plex.

When you want to use the space in a mirrored volume for other purposes, you can remove a plex and return the space it used to unallocated space.

Veritas Storage Foundation for Windows lets you add a mirror to any kind of dynamic volume, except RAID-5. You can extend any mirrored volume.

RAID-5 volumes

A RAID-5 volume is a fault-tolerant volume with data and parity striped alternately across three or more physical disks. If one of the physical disks fails, data that was on the failed disk is recreated from the remaining data and parity on the other disks. RAID-5 volumes are a good solution for data redundancy in a computer environment in which most activity consists of reading data.

You need a minimum of three disks for a RAID-5 volume. Veritas Storage Foundation for Windows can accommodate up to 256 disks in a RAID-5 volume. You can extend a RAID-5 volume, but it cannot be mirrored.

Mirrored striped volumes (RAID 0+1)

RAID 0+1 volumes are mirrors of striped volumes. For example, a two-disk striped volume can be mirrored to two additional disks. This RAID type provides the advantages of both speed (from striping) and fault tolerance (from mirroring). You can add more mirrors to a mirrored striped volume, and you can extend this type of volume onto additional dynamic disks within the dynamic disk group.

Set up a dynamic boot and system volume (Optional)

You may want to make the Windows boot and system partition into a dynamic volume and mirror that volume. Then, if the disk containing the boot and system volume fails, you can start the computer from the disk containing the mirrors of the volume.

To make a boot and system partition dynamic, you include the disk that contains the basic active boot and system partition in a dynamic disk group. When you do that, the boot and system partition is automatically upgraded to a dynamic simple volume that is active—that is, the system will boot from that volume.

For an optimal setup, it is recommended that you have a separate disk for the dynamic system and boot volume and mirror it with one or two disks. Thus, you will have a boot dynamic disk group with two or three disks. You then need to have an additional disk or disks for the data. The data disks would be in another dynamic disk group.

In Windows documentation, the boot volume is the partition that contains the operating system and the system volume is the partition that the computer starts from. The boot and system volumes can be in the same partition or different partitions for MBR style partitions. For GPT style partitions, the boot and system volumes must be in different partitions.

This following procedure is written for an MBR style partition with the boot and system volumes in the same partition. If the boot and system volumes are in different partitions, then these steps can be used as a guide to apply to each volume separately.

For GPT style partitions, the following procedure can also be used as a guide to apply to each volume separately. However, use the Microsoft bootcfg.exe utility instead of editing the boot.ini as described in the procedure.

Note: A dynamic system volume on an Itanium (IA64) system with a GPT style partition is not supported by SFW. Therefore creating a mirror of a dynamic system volume on an IA64 system with this configuration is not supported. Refer to the SFW Release Notes for more information about creating and booting from a mirror on a system with this configuration.

Note: On Windows Server 2008, although you can create and manage the dynamic boot and system volume using the SFW VEA console, the native Windows driver handles the input/output operations for that volume. Therefore, ensure that you comply with Windows Server 2008 information on best practices and restrictions on the use of a dynamic boot and system volume.

Setting up a dynamic boot and system volume for MBR style partitions:

- 1 Make sure that the server has a basic system and boot partition that is active.
If you installed Windows Server 2003, the boot and system partition are set up as a part of the operating system installation.
- 2 As a precaution, create a boot floppy of the system partition.
If something goes wrong with the original system and boot volume or its mirror, you can boot your system from the floppy. Test the boot floppy while your system is in a known good state.
- 3 Make sure that there are sufficient disks attached to the server so that there will be a separate disk for the boot and system volume plus one or two more for mirroring the system disks and then additional disks for the data.
- 4 Create a dynamic disk group that has the disk with the existing boot and system partition plus one or two other disks to be used for mirroring purposes.
See [“Create dynamic disk groups”](#) on page 53.
When you designate a disk as part of a dynamic disk group, the entire disk becomes a dynamic disk—that is, a disk capable of having dynamic volumes. Any basic partitions on that disk become dynamic volumes. Thus, the boot and system partition automatically becomes a dynamic simple volume. You do not have to mark it as the active volume, because it is automatically made active.
There is no command in Veritas Storage Foundation for Windows for making an existing dynamic volume active—that is, to make it the volume that the computer starts from. The only way to make a dynamic volume active through SFW is to upgrade the existing active basic system partition by including the disk that contains the partition as a member of a dynamic disk group. You can make a basic partition active through the command **Mark Partition Active**.
- 5 If you have not done so already, create one or more additional disk groups for your data and then create the necessary volumes for the data.
See [“Create dynamic disk groups”](#) on page 53.
See [“Create dynamic volumes”](#) on page 60.

- 6 Create one or more mirrors on the dynamic system and boot volume.
See “[Add a mirror to a volume](#)” on page 258.
The troubleshooting section covers difficulties that can occur.
See “[An attempt to mirror a boot or system volume fails or has an error message](#)” on page 499.
- 7 If the dynamic boot or system volume fails, you must make the change to the server’s **boot.ini** file to make one of the mirrored boot or system volumes the active volume for your computer and then reboot.
If a break-mirror operation is performed on a mirrored boot volume, the resulting new volume—the broken-off mirror—will not be usable as a boot volume.

Configure VCS and program options

If you installed SFW HA or any of the various Veritas Storage Foundation for Windows options—Microsoft Clustering (MSCS) Support, DMP, FlashSnap, and VVR Support—you need to do additional configuration steps. This section contains a high-level summary and refers you to other sections of the documentation for details.

SFW HA

SFW HA installs VCS on specified machines. The installation does the initial setup of the VCS cluster. However, there are additional steps you need to do to complete to cluster configuration.

See “[VCS support in SFW HA](#)” on page 783.

Also, the VCS documentation set is included with the SFW HA product.

In addition, see the step-by-step examples in the *Veritas Storage Foundation and High Availability Solutions Solutions Guide*. If you are planning to use VCS with Microsoft Exchange Server or Microsoft SQL Server, you need to have selected the Veritas Cluster Server Enterprise Agent for Exchange or the Veritas Cluster Server Enterprise Agent for SQL. The *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange* and the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft SQL* have step-by-step examples of what needs to be done for SFW, VCS, and Exchange and SQL Server applications to function together. In addition, a VCS documentation set is included with the program.

Veritas cluster option for Microsoft Clustering

After Veritas Storage Foundation for Windows and Microsoft Clustering are installed, you create one or more SFW disk groups and their volumes. Then you use Microsoft Clustering to make each disk group a resource in the cluster program. You might want to mirror the SFW cluster volumes for redundancy.

See “[Microsoft Clustering support](#)” on page 753.

If you are installing Microsoft Clustering with DMP, see the information on this topic in the Installation Guide. The *Veritas Storage Foundation and High Availability Solutions Solutions Guide* has step-by-step examples of different configurations with SFW and Microsoft Clustering. A DMP configuration is also covered.

Veritas Dynamic Multi-pathing option (DMP)

The Veritas Dynamic Multi-pathing (DMP) option adds fault tolerance to disk storage by making use of multiple paths (each with its own host adapter and cabling) between a computer and the disks in a storage array.

See [“Dynamic multi-pathing software”](#) on page 717.

See the Installation Guide for general information about installing DMP either by itself or with Microsoft Clustering.

Veritas FlashSnap option

Veritas FlashSnap is a multi-step process that allows you to create independently addressable snapshot volumes that are copies or mirrors of the volumes on your server. These snapshot volumes can be used as quick recovery images for recovering applications, such as Microsoft Exchange. They also can be used for backup or application testing. One of the main advantages of using FlashSnap is that the snapshot volumes can be easily moved to another server. Thus, backup or other processing can be performed on another server without affecting the performance of applications on the applications server.

The only configuration step for FlashSnap that you might need to do is to upgrade your disk groups if you have installed the program on a server that has disk groups that were created in Volume Manager 3.1 or earlier.

See [“Upgrade a dynamic disk group version”](#) on page 199.

FlashSnap is a SFW option that must be purchased separately.

For full information on FlashSnap, see [“FlashSnap”](#) on page 563.

Veritas Volume Replicator option (VVR)

Veritas Volume Replicator also requires configuration steps in order to work properly.

See [“Summary of the steps for setting up a disaster recovery solution with VVR”](#) on page 801.

See also the SFW Solutions Guides and the VVR documentation set for further information.

Additional SFW HA options

If you are installing SFW HA, there are additional options that are agents for working with VCS: the Veritas Cluster Server Agent for Microsoft Exchange Server, the Veritas Cluster Server Agent for Microsoft SQL Server, and the Veritas Cluster Server Agent for EMC SRDF. If you are using any of these products, you will want to license and install these agents.

Set desired preferences

This section describes some of the main settings in the SFW program that are useful to know about and that you might want to change from the default values or that require input from you before they can be implemented.

The settings described in this section are as follows:

- [Hot relocation settings](#)
- [Event notification settings](#)
- [S.M.A.R.T. monitoring for a disk](#)
- [Capacity monitoring for volumes](#)
- [Task throttling](#)
- [Configuration task performance tuning](#)
- [Track alignment settings](#)

Hot relocation settings

Hot relocation is an automatic process that relocates subdisks from a disk that has I/O errors. If there are I/O errors on a subdisk containing a redundant volume (RAID-5 or mirrored), the redundant volume's subdisks are moved from the failed subdisk to a hot spare disk. If there is not enough free space on designated hot spare disks, then free space on any available disk will be used.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support Hot Relocation.

The **Undo Hot Relocation** command can be used to move the subdisks back to their original location after the failed disk has been repaired or replaced.

For more information on how hot relocation works, see “[Hot relocation](#)” on page 268.

The default for Veritas Storage Foundation for Windows is to have automatic hot relocation mode inactive. This means that if an I/O error occurs in a redundant subdisk, the subdisk is not automatically relocated to another disk. Use the **Set Disk Usage** command to designate preferred disks as targets for hot relocation.

The option to disable the hot relocation mode is available from the Control Panel.

See “[Hot relocation mode](#)” on page 269.

Event notification settings

SFW provides event notification by SMTP email, by pager, and through SNMP traps that can be displayed in HP OpenView, CA Unicenter, and IBM Tivoli. You can configure the notification service to send messages to specific individuals, to groups, or to a management console in the case of SNMP traps. The event notification service is implemented through SFW's Rule Management utility. If you want to set up event notification, you must use the Rule Management utility to set up rules that will send out notifications after certain events occur. You access the Rule Management utility through SFW's Control Panel.

See "[Event notification](#)" on page 236.

The details of defining the rules for events are in the online help in the module "Optional Rules for Handling Events." To invoke the online help, choose **Contents** from the **Help** menu in SFW. In the tree view that comes up in the left pane, you will see the help module "Optional Rules for Handling Events."

S.M.A.R.T. monitoring for a disk

Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) is available on many new SCSI disks. S.M.A.R.T. provides a way for disks to self-check certain physical conditions that are useful predictors of disk failure and send an alert to the SFW Event Log when conditions indicate that a failure may occur soon. This allows the system administrator to take preventive action to protect the data on the disk.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support S.M.A.R.T. monitoring.

In order to receive alerts in the SFW Event Log, S.M.A.R.T. monitoring must be enabled for the global configuration and also on each disk you want checked. The default is to have S.M.A.R.T. monitoring disabled.

See "[Disk monitoring](#)" on page 242.

Capacity monitoring for volumes

Capacity monitoring is a feature that monitors the capacity of SFW dynamic volumes so that when used space on any volume reaches certain size thresholds, you are notified with an alert message. The purpose of capacity monitoring is to provide you with a warning when any dynamic volume has nearly reached full capacity. You can set up capacity monitoring for individual volumes or all volumes. Capacity monitoring is turned off by default. You can set individual volumes to grow automatically when a certain threshold is met.

See “[Capacity monitoring](#)” on page 244.

Task throttling

This feature allows you to control how the system allocates CPU time between I/O and other tasks that must also be performed.

See “[Task throttling](#)” on page 133.

Configuration task performance tuning

Configuration task performance tuning allows you to set the number of I/O threads to perform certain mirror-related operations, such as creating a mirror or adding a mirror.

See “[Configuration task performance tuning](#)” on page 134.

Track alignment settings

This feature allows you to set dynamic volumes to always store blocks of data in alignment with the boundaries of the physical track of the disk. Aligning data so that it does not straddle a track boundary helps optimize I/O performance.

You can specify track alignment through the VEA GUI.

See “[Track alignment](#)” on page 134.

You can also specify track alignment through the CLI.

See “[vxdisk](#)” on page 329.

Protecting your SFW configuration with vxcb

To protect your SFW configuration (that is, the disk group and volume layouts), it is highly recommended that you perform periodic backups of the configuration, using the `vxcb` utility.

See “[Configuration backup](#)” on page 124 and “[vxcb](#)” on page 404.

Guidelines for running SFW

Once SFW is installed, the SFW service (`vxvm`) always runs in the background. The client can be stopped and started when needed. To exit the client software, select **Exit** from the **File** menu or click the **Close** box.

If there are a lot of processes running on the server, you may want to close the SFW GUI to improve system performance. When you do so, the SFW service continues to run.

For troubleshooting purposes only, occasionally you may need to stop and restart the SFW service.

See “[Starting and stopping the Veritas Storage Foundation for Windows Service](#)” on page 494.

Managing

- [Chapter 3, “Using the GUI to manage your storage”](#) on page 83
- [Chapter 4, “Working with disks, partitions, and volumes”](#) on page 137
- [Chapter 5, “Dealing with disk groups”](#) on page 193
- [Chapter 6, “iSCSI SAN support”](#) on page 217
- [Chapter 7, “Settings for monitoring objects”](#) on page 233
- [Chapter 8, “Standard features for adding fault tolerance”](#) on page 255
- [Chapter 9, “Command line interface”](#) on page 281
- [Chapter 10, “Troubleshooting and recovery”](#) on page 467

Using the GUI to manage your storage

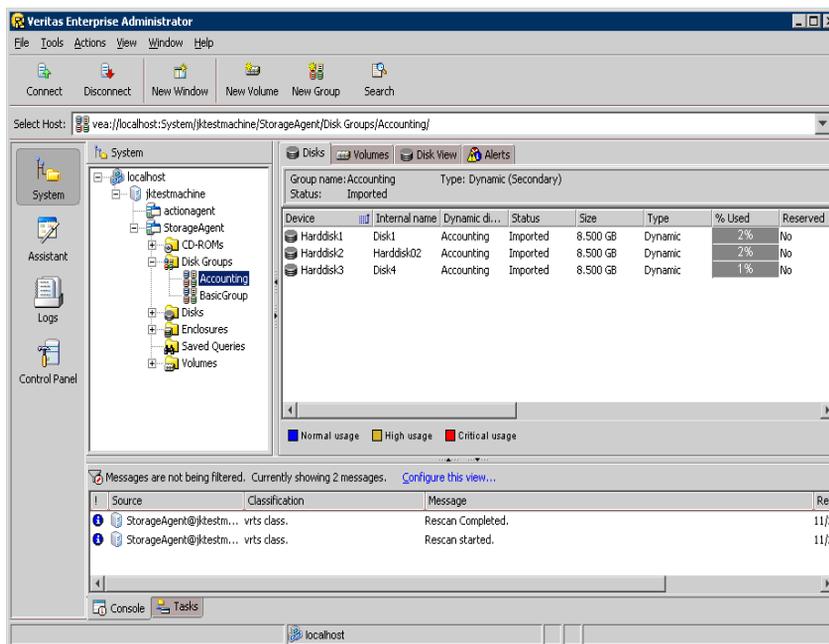
- Overview of console features
 - Viewing disks and volumes
 - Storage Foundation general preferences
 - The URL bar
 - The Toolbar
 - The Perspective bar
- Systems perspective
 - The left pane
 - The right pane
 - The lower pane
 - The disk view
 - Search
- Assistant perspective
- Logs perspective
- Control Panel perspective

Overview of console features

The GUI for Veritas Storage Foundation for Windows is the Veritas Enterprise Administrator (VEA) console.

The VEA GUI console window provides a graphical way to view and manipulate all the storage objects in your system. The VEA console display for Veritas Storage Foundation for Windows storage objects is shown in the sample screen that follows.

Figure 3-1 VEA GUI window



The VEA console display has the following features:

- Perspectives of the system
- A tree view displaying the storage objects in the left pane of the window
- Tabbed views in the right pane of the window containing additional information on the storage objects
- A menu bar, toolbar, and URL bar
- A lower pane containing information on processes initiated by the program or a listing of alert messages

Viewing disks and volumes

The VEA console is used to view disks and volumes and their relationship with each other.

Viewing all disks associated with a volume

To view all disks associated with a volume

- 1 In the left pane, click the desired volume icon.
If the volume icon is not displayed because the tree view is not fully expanded, click the plus sign in front of the nodes starting at the top of the tree. The Volumes icon appears under the StorageAgent node.
- 2 If necessary, in the right pane of the console window, select the **Disks** tab. The **Disks** tab view displays the disk or disks associated with a particular volume.

Viewing all volumes associated with a disk

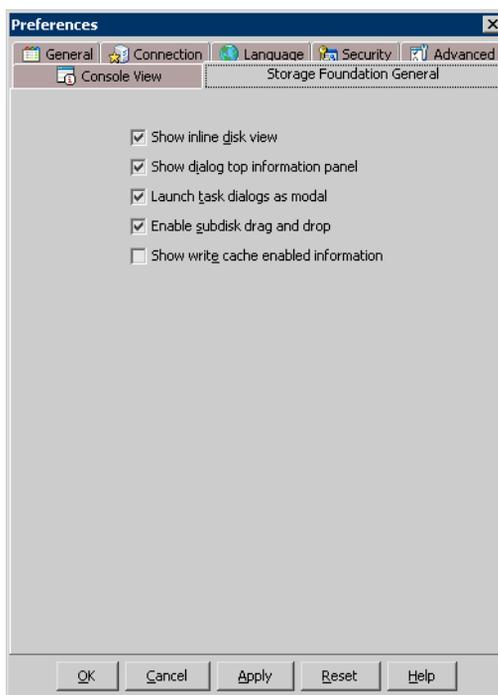
To view all volumes associated with a disk

- 1 In the left pane, click the desired disk.
If the disk icon is not displayed because the tree view is not fully expanded, click the plus sign in front of the nodes starting at the top of the tree. The Disks icon appears under the StorageAgent node.
- 2 If necessary, in the right pane of the console window, select the **Volumes** tab. The **Volumes** tab view displays all the volumes that are on that disk.

Storage Foundation general preferences

Storage Foundation General preferences are settings for displaying GUI features relating to SFW. To access these settings select **Preferences** from the VEA **Tools** menu. In the dialog box that appears, select the **Storage Foundation General** tab, as shown in the screen below.

Figure 3-2 Storage Foundation General tab



Check the settings desired and click **Apply** to enable the settings in the GUI. Click **OK** to exit the dialog box. To make your selected settings appear in the GUI, you may need to refresh the right pane. Click an object in the left pane to refresh the right pane.

The available settings are as follows:

- **Show inline disk view**
Allows the Disk View to be accessed as a tab in the right panel of the GUI.
- **Show dialog top information panel**
Enables the display of helpful information at the top of certain dialogs.

- **Launch task dialogs as modal**
Task dialogs will be launched so that the task dialog is the only active window on the desktop.
- **Enable subdisk drag and drop**
Allows the drag and drop of subdisks to a different location on the same disk or to a different disk in the Disk View.
- **Show write cache enabled information**
If SFW determines there is a write cache enabled disk, then this setting will enable the display of a message reminding the user about write cache enabled disks every time SFW is launched.

The URL bar

The URL bar, located above the tabs of the right pane, displays the selected object's location in the tree in a URL style. If you are connected to more than one host, you can click on the drop-down to select a different host.

The Toolbar

The Toolbar provides quick access to the program's most common tasks.

Figure 3-3 Toolbar



Table 3-1 Description of Toolbar Icons

Icon	Name	Description
	Connect	Brings up the Connection dialog box.
	Disconnect	Disconnects from selected machine.
	New Window	Opens a new window that displays the console.
	New Volume	Brings up the New Volume wizard.
	New Group	Brings up the New Dynamic Disk Group wizard.
	Search	Searches by specific criteria for volumes, disks, or disk groups.

The Perspective bar

The Perspective bar located at the far left of the console, provides quick access to different perspectives (views) of the system that you are connected to. Clicking a perspective displays certain operations and objects of the system.

The perspectives are as follows:

- **System**
Displays the objects, details of the objects, and status of the system.
- **Assistant**
Provides shortcuts to perform common tasks on the objects of the system. This provides a task based approach to operations that can be performed on the system.
- **Logs**
Displays the system's task and alert logs in the right pane. Clicking the Alert Log tab or the Task Log tab in the right pane displays the corresponding log entries.
 - The Task Log is a listing of tasks, such as formatting a volume or resynchronization of a volume. In SFW, the Task Log is not implemented.
 - The Alert Log lists events and alerts pertaining to the Veritas Storage Foundation for Windows program.
See "[Alert log](#)" on page 234.
- **Control Panel**
Displays the tasks related to configuring the system. The Control Panel allows you to access settings for Logs, Rule Management, Configuration Backup, Historical Statistics, SMTP Configuration, Task Settings, and Track Alignment.
See "[Control Panel perspective](#)" on page 122.

Systems perspective

The Systems perspective displays the SFW console and is made up of the following:

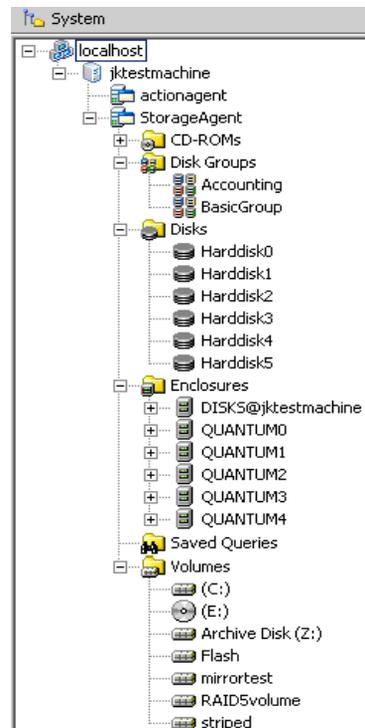
- [The left pane](#)
- [The right pane](#)
- [The lower pane](#)

The contents of these panes are described in the following sections.

The left pane

In the System perspective, the left pane shows a tree view of the system and storage objects detected by the Veritas Storage Foundation for Windows software. The tree view displays the hierarchical relationships of the objects. The node at the top of the tree represents the Veritas Storage Foundation for Windows client that you are connected to. In the screen below, the client is connected to “localhost.” The objects under this node are the managed servers that the client is connected to and managing. In the screen below, there is only one managed server node, a server named “jktestmachine.”

Figure 3-4 Tree view of objects in left pane of VEA GUI



Below each managed server icon are the following default object categories:

- [CD-ROMs](#)
- [Disk groups](#)
- [Disks](#)

- [Enclosures](#)
- [Saved Queries](#)
- [Volumes](#)

For systems configured for support of Microsoft multipath input/output (Microsoft MPIO) solution, the tree view also displays the following:

- [DMP DSMs](#)

For systems running Microsoft Exchange or other VSS-aware applications, the tree view also displays the following:

- [Applications \(VSS writers\)](#)

The tree view can be expanded by clicking on a plus sign (+) in front of an object icon. When the tree view is fully expanded, all the objects have a minus (-) sign in front of them. By clicking on a minus sign at any level, you can collapse an object down to that level. The fully collapsed tree shows only the top-level object.

Right-clicking on an object in the tree view brings up a context menu that is appropriate to that object.

The topics below give additional information on the storage object categories under each managed server node.

CD-ROMs

Any CD-ROM drives recognized by Veritas Storage Foundation for Windows as existing on the computer you are managing.

Disk groups

A disk group is a grouping of disks within Veritas Storage Foundation for Windows. The two types of disk groups are basic and dynamic.

See “[About disk groups](#)” on page 194.

Disks

Disks are physical disks or logical disks recognized by the Windows operating system.

Depending on the type of disk, a disk may be enabled to support thin provisioning and storage reclamation. Thin provisioning is a technology to efficiently allocate storage for a disk. Thin provisioning allocates physical storage only when actual data is written to the disk. Some disks that are enabled for thin provisioning also provide storage reclamation. Storage reclamation is the operation that decreases the physical storage allocation once data is deleted from the disk. A disk that supports thin provisioning is represented with a disk

icon that includes a red colored sector. A disk that supports thin provisioning and storage reclamation is represented with a disk icon that includes a green colored sector with an asterisk (*).

Enclosures

Enclosures are physical objects that contain one or more physical disks. For example, the disks may be contained in arrays or JBODs. Also the disks may be internal to your server.

Saved Queries

Saved Queries refers to queries that were saved with the Search feature of SFW. If you saved queries with the Search feature, then this node would display the results of the saved query.

See [“Search”](#) on page 111.

Volumes

A volume is a logical entity that is made up of portions of one or more physical disks. A volume can be formatted with a file system and can be accessed by a drive letter or a mount point. Veritas Storage Foundation for Windows works with basic and dynamic volumes.

A volume may be either read only or read/write. The icons for read only volumes include a picture of a padlock to differentiate them from read/write volumes. Not all commands available in Veritas Storage Foundation for Windows for read/write volumes are enabled for read only volumes because specific commands require write access to the volume. Check the access mode of a particular volume if a command is not available.

DMP DSMs

On servers that are configured for support of Microsoft multipath input/output (Microsoft MPIO) solution, a node for DMP DSMs appears.

Completely expanding the DMP DSMs node displays DSM nodes being used, nodes of arrays being controlled by the DSM, and the disks contained in the array. These nodes allow you to manage the settings for the arrays and disks configured for Microsoft MPIO.

See [“Dynamic multi-pathing overview”](#) on page 718.

Applications (VSS writers)

On systems running Enterprise Vault, Microsoft SharePoint, Microsoft Exchange,

or other VSS-aware applications, a node for Applications(VSS Writers) appears. SFW provides an option of taking snapshots with Volume Shadow Copy Service (VSS). The VSS snapshot method allows you to take snapshots of VSS-aware applications, such as Microsoft Exchange, while the application files are open. When VSS-aware applications do not exist, the snapshot is taken with the SFW FlashSnap method (VM method).

See “[Volume Shadow Copy Service \(VSS\)](#)” on page 617.

iSCSI

On servers that are connected to an iSCSI SAN, the following nodes may appear:

- iSCSI Initiators
This node displays information about the initiators and targets of the iSCSI SAN.
- iSCSI Arrays
This node displays information about the Microsoft iSCSI Target subsystems of the iSCSI SAN.
- iSNS
This node displays information about the iSNS Server of the iSCSI SAN.

See “[About iSCSI SANs](#)” on page 218.

The right pane

In the System perspective, the right pane provides information on the various storage objects. The tabs available in this pane are determined by the object you have selected in the tree view in the left pane. In each tab view, you can right-click to get a context menu of commands available in that view. In every view, you can widen or narrow columns by placing the mouse pointer on the border between two columns in the header row and moving the mouse to the left or right while holding down the mouse button.

This section focuses on how information about disks and volumes managed by Veritas Storage Foundation for Windows displays in the right pane.

It contains the following topics:

- [Right-pane display for disks and volumes](#)
- [Disk view tab](#)
- [Right-pane legends](#)
- [Customizing the table headers](#)

Right-pane display for disks and volumes

This section describes how the tabbed views change, depending on the disk and volume storage objects you select.

Note: Disks that support thin provisioning are represented with a disk icon that includes a red colored sector.

Note: Disks that support thin provisioning and storage reclamation are represented with a disk icon that includes a green colored sector with an asterisk (*).

Note: Information about thin provisioned disks is not automatically updated in the VEA GUI. The information about thin provisioned disks can be updated by performing a Refresh operation.

Selecting all disks

In the tree view in the left pane of the VEA console, if you select all disks by clicking the Disks folder, the right-pane view displays tabbed views for **Disks** and **Disk View**. The **Disks** tab shows information about the disks available on the

selected server, as shown in the sample screen below. The **Disk View** tab uses a graphical format to show information about the volumes contained on each disk. The **Alerts** tab displays information about alerts.

Figure 3-5 Right-pane information when all disks are selected

Device	Internal name	Dynamic di...	Status	Size	Type	% Used	Reserved
Harddisk0	-	-	Online	8,500 GB	Basic	99%	No
Harddisk1	Disk1	Accounting	Imported	8,500 GB	Dynamic	2%	No
Harddisk2	Disk2	Accounting	Imported	8,500 GB	Dynamic	13%	No
Harddisk3	Disk4	Accounting	Imported	8,500 GB	Dynamic	14%	No
Harddisk4	-	-	Online	8,500 GB	Basic	0%	No
Harddisk5	-	-	Online	17,000 GB	Basic	99%	No

Selecting an individual disk

If you select an individual disk in the tree view, you will see a display similar to the sample screen below. Notice that the tabs have now changed to **Volumes**, **Disk Regions**, **Disk View**, and **Alerts**. The **Volumes** tab gives information about the volumes on the selected disk.

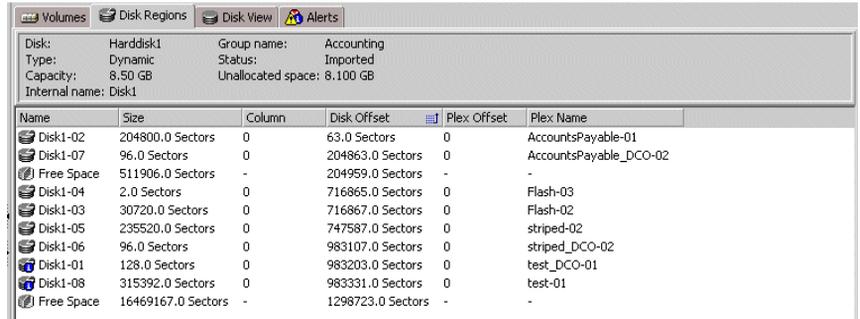
Figure 3-6 Right-pane information for a selected disk

Name	Group name	Status	Size	Free Space	Layout	File Syst...	Volume name	# Copies	Log
test (F:)	Accounting	Healthy	154,000 MB	151,500 MB	Mirrored Co...	NTFS	test	2	FastResync
Flash (H:)	Accounting	Healthy	15,000 MB	12,500 MB	Mirrored Co...	NTFS	Flash	2	DRL
striped (J:)	Accounting	Healthy	115,000 MB	112,500 MB	Concatenated	NTFS	SnapVolume01	1	FastResync
AccountsPayable...	Accounting	Healthy	100,000 MB	97,500 MB	Concatenated	NTFS	SnapVolume02	1	FastResync

Viewing subdisks

If you click the **Disk Regions** tab, you will see all the subdisks or parts of a volume that reside on the disk, as well as any free regions on that disk. In the screen below, there are eight subdisks.

Figure 3-7 Right-pane information for subdisks on a selected disk



Every volume has at least one subdisk. A striped volume has a minimum of two subdisks. A RAID-5 volume has a minimum of three subdisks. A mirrored volume has as many subdisks as there are mirrors, which are also called “plexes.”

Note: There are no subdisk storage objects in the left-pane tree view. You must access the subdisks through the right pane. You will have to click an individual disk in the left pane to gain access to the **Disk Regions** tab.

Selecting volumes

If you select all volumes by highlighting the Volumes folder in the tree view, the right pane displays the tabs: **Volumes**, **Disk View**, and **Alerts**. When you select an individual dynamic volume in the tree view, you will see a right-pane view similar to the screen below. Notice how selecting an individual volume makes available many more tabbed views.

Figure 3-8 Right-pane information for a selected volume



A dynamic volume has the following tabbed views:

Table 3-2 Table of Volume Tabbed Views

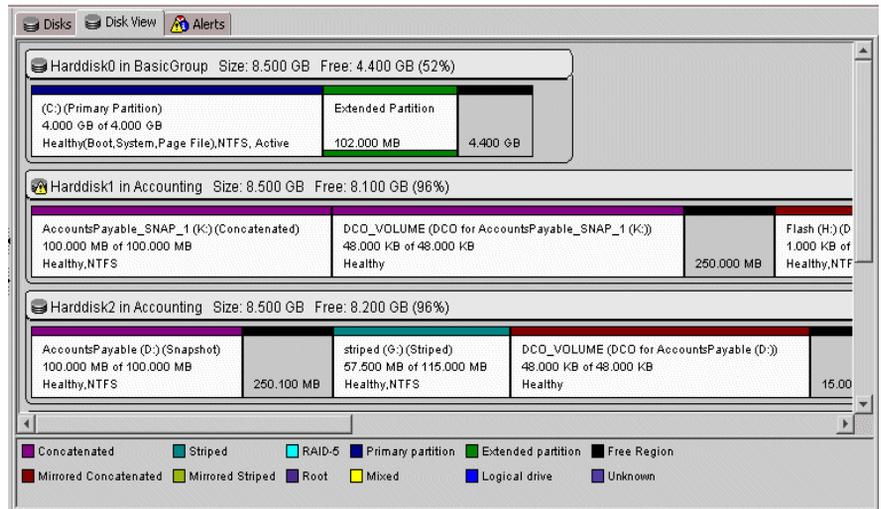
Tab	Description
Disks	Displays information about the disks in the volume.
Mirrors	Details the mirrors in the volume. See “ Mirroring ” on page 257.
Logs	Shows any logs that are added to a volume to increase the speed of resynchronizing mirrored or RAID-5 volumes after disk failures. See “ Dirty region logging (DRL) and RAID-5 logging ” on page 274.
Subdisks	Lists the subdisks associated with the volume. Subdisks are the basic units in which SFW allocates disk space in a volume. Each subdisk represents a specific portion of a volume on a dynamic disk. For example, a mirrored volume with two mirrors (plexes) has two subdisks.
Snapshot Volumes	Gives information on snapshots, which are mirrored volumes that have been broken off from their original volume for backup or other purposes. This tab appears only when you have created snapshot volumes. See “ Snapshot commands ” on page 577.
DCO	Provides information on the Disk Change Object (DCO) volumes that are used with FastResync and also with FlashSnap. See “ Disk change object (DCO) volume ” on page 572.
Disk View	A detailed view of the disks associated with the volume. See “ Disk view tab ” on page 98.
Alerts	Displays information about alerts. This tab appears only when an event has occurred that generates an alert.

A volume that is not dynamic, such as a partition on your C drive, will display only the **Disks**, **Disk View**, and **Alert** tabs.

Disk view tab

The **Disk View** tab displays a graphical layout of the disks on your system, including removable media. As with the tree view, right-clicking on an object or portion of the window relating to an object brings up a context menu that has commands related to the object.

Figure 3-9 Disk view tab



The Disk View is also available as a separate window.
 See “[The disk view](#)” on page 103.

Right-pane legends

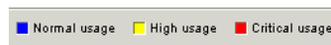
This section describes the two legends in the right pane, the disk usage legend and the Disk View legend.

Disk usage legend

The disk usage legend, located at the bottom of the right pane, is context sensitive and will change depending on the tab selected in the right pane. The legend shows either disk usage or the volume type.

When the **Disks**, **Subdisks**, or **Disk Regions** tab is selected, the disk usage legend shows how to interpret symbols showing the level of I/O activity (Normal, High, or Critical) in each area.

Figure 3-10 Disk usage legend



Disk view legend

The legend shown in the Disk View or with the **Disk View** tab selected shows the volume or partition type. The colors represent the following layout

characteristics: concatenated, striped, RAID-5, primary partition, extended partition, free region, mirrored concatenated, mirrored striped, root, mixed, logical drive, and unknown.

The mixed type refers to a volume that has both concatenated and striped plexes because it has been modified by using the Dynamic Relayout feature.

See “[Dynamic relayout](#)” on page 277.

Figure 3-11 Disk view legend

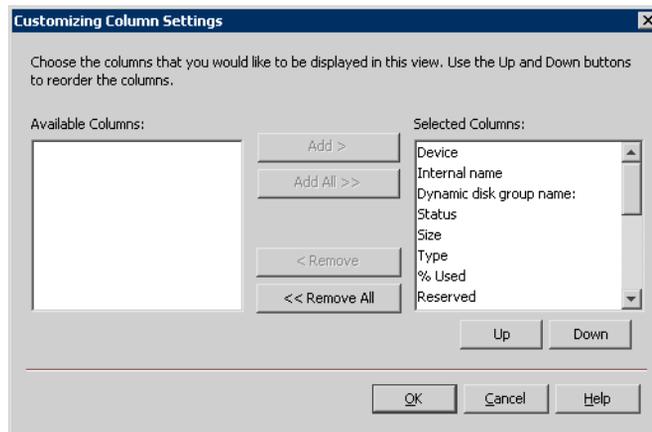


Customizing the table headers

The Customize Columns window allows you to customize the table headers by changing which columns are shown and in what order.

To customize the table headers

- 1 Right-click the column header.
- 2 Select **Customize Table Header**. The Customizing Column Settings window appears.



Headers of columns shown in the right pane of the console are shown on the right side of the dialog. The available headers are shown on the left side.

- 3 Make the desired changes to the column headers.
The options are as follows:
 - To add a column header, select it in the **Available Columns** pane and click the **Add** button.

- To remove a column header, select it in the **Selected Columns** pane and click the **Remove** button.
 - To rearrange the sequence of the headers, select the header you wish to move in the **Selected Columns** pane and use the **Up** and **Down** buttons to move it within the list.
- 4 Click the **OK** button to apply the settings. The column headers displayed in the console are in the order you selected in the **Selected Columns** pane.

The lower pane

In this section of the System perspective, you can toggle the display by clicking on either the **Console** tab or the **Tasks** tab at the bottom left corner. The default **Console** tab display shows Veritas Storage Foundation for Windows alerts. The **Tasks** tab shows progress on Veritas Storage Foundation for Windows tasks, such as formatting a volume. The name of the selected managed server is displayed in the bottom center. This is helpful if you have connected to multiple servers with SFW.

The disk view

This section describes the Disk View.

The section's topics are as follows:

- [Disk view overview](#)
- [Refresh view](#)
- [Print](#)
- [Show legend](#)
- [Options for graphical views](#)
- [Expanded view](#)
- [Vol details view](#)
- [Full volume display](#)
- [Projection](#)
- [Context menu available from disk view](#)

Disk view overview

The Disk View can be accessed in two ways, which are as follows:

- Select the **Disk View** tab in the right pane.
- Right-click an object (disk group, disk, or volume) in the tree view pane, and select **Disk View** from the context menu that appears.

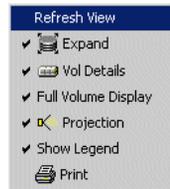
The same commands are available in both views. The Disk View available from the tree view context menu opens a separate window that can remain open as you continue to work in Veritas Storage Foundation for Windows.

Additionally, you can use the Ctrl key to select only the specific objects (disks, volumes, or disk groups) you wish to include in the separate disk view. This feature is helpful if you have a very large number of disks or volumes.

The commands in Disk View include **Refresh View**, **Print**, **Show Legend**, and four options for different views of the selected disks: **Expand**, **Vol Details**, **Full Volume Display**, and **Projection**. These commands are available from several different places.

From the **Disk View** tab in the right pane, right-click in an empty space (right-click any area of the pane where there is not a graphical representation of a disk), and a context menu containing the commands will appear, as shown in the screen that follows.

Figure 3-12 Disk view menu



If you have created a separate window by selecting Disk View from the context menu, these commands can be accessed by right-clicking in an empty space (right-clicking on any area of the pane where there is not a graphical representation of a disk), by clicking the **Options** or **File** menu on the menu bar, or by clicking on icons on the toolbar.

Refresh view

The **Refresh View** command found in the **Disk View** menu will update the Disk View only and ensure that any recent changes are represented accurately.

Show legend

The legend is located at the bottom of the Disk View. The **Show Legend** command toggles the Disk View legend on and off. If you are working with a large number of disks, you may wish to turn the legend off to gain additional space in the window. Each volume type or partition type is assigned a color. The legend shows the color-coding scheme. When the **Vol Details** command is selected, there is a colored bar across the top of each subdisk that indicates its volume type.

Figure 3-13 Disk view legend



Print

The **Print** command sends your current Disk View display to a selected printer. It may be convenient to have a hard copy of your disk configuration, especially if you are working with a large number of disks.

The remaining items on the **Disk View** context menu: **Expand**, **Vol Details**, **Full Volume Display**, and **Projection** are discussed in the sections that follow.

Options for graphical views

There are four options for different views of the selected disks: **Expand**, **Vol Details**, **Projection**, and **Full Volume Display**. The table below shows the buttons available for these commands and for the print function. The toolbar containing these buttons is displayed only in the separate Disk View window and not in the Disk View in the right pane. However, in both versions of the Disk View, you can right-click an empty space (an area of the pane where there is not a graphical representation of a disk) to bring up a context menu with these options.

Table 3-3 Disk View Options

Icon	Meaning	Tasks
	Represents the Expand function in the Disk View.	Allows you to view detailed information about disks and the organization of the data on the disks. If this icon is not checked, the view will be contracted to show less detail.
	Represents the Vol Details function in the Disk View.	Displays subdisks as partial volumes.
	Represents the Projection function in the Disk View.	Highlights objects associated with the selected subdisk or volume.
	Represents the Print function in the Disk View.	Allows you to print the contents of the current view.

Note: The **Full Volume Display** view, which displays more detailed information about subdisks, is not represented by an icon.

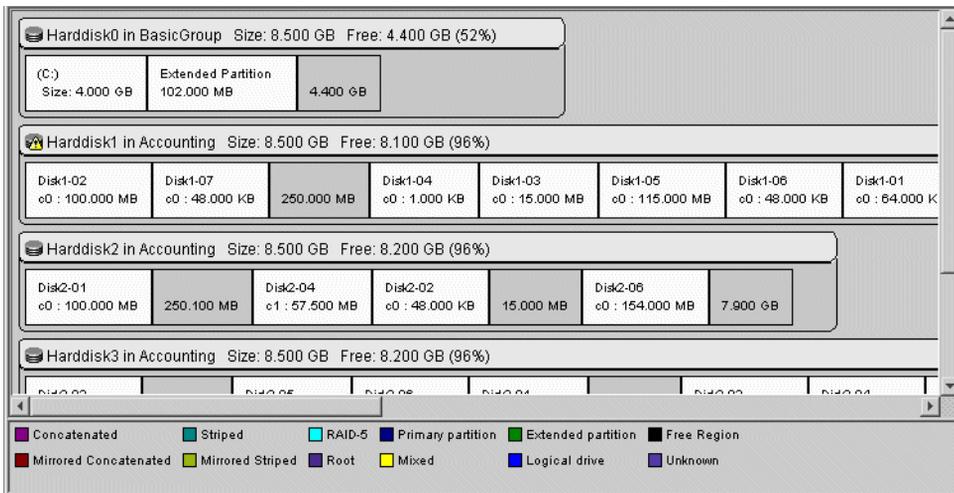
Expanded view

The subdisks can be viewed in either the expanded view or nonexpanded view. Each view gives different information. When **Expand** is checked in the **Disk View** menu, the expanded view is in effect. When it is not checked, the nonexpanded view displays.

Expanded view

The expanded view, shown below, shows the subdisk names and sizes, as well as the amount of free space remaining on the disk.

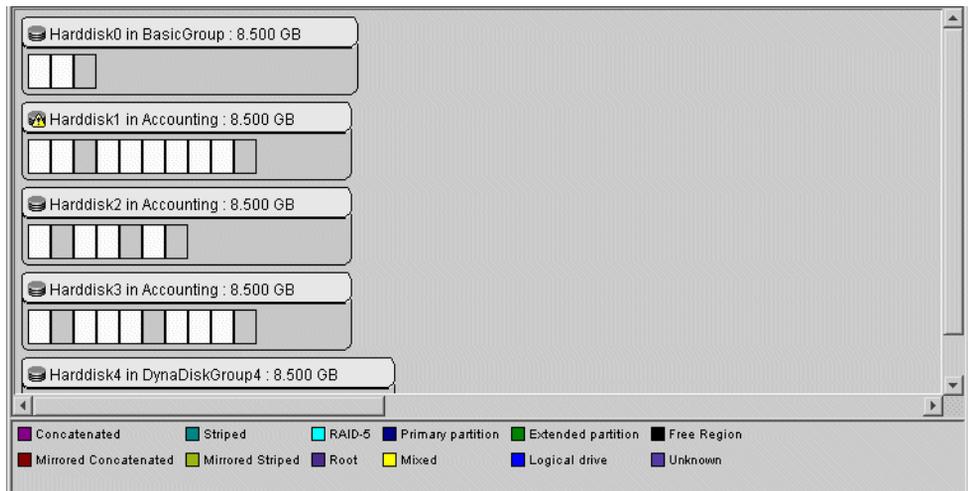
Figure 3-14 Expanded view



Nonexpanded view

If the expanded view is not selected, a contracted disk view is shown. This nonexpanded view, shown below, allows you to easily see the number of subdisks on each disk.

Figure 3-15 Nonexpanded view



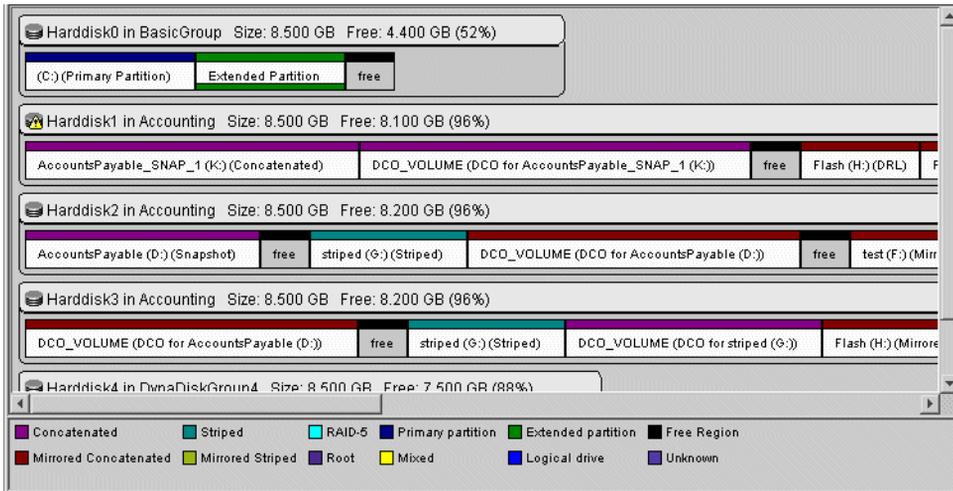
Vol details view

The **Vol Details** view adds information to either the expanded or nonexpanded view. This view is useful if you are looking at a large number of disks, because each disk takes less space than in the full volume display, so more disks can be displayed on the screen at once.

In the nonexpanded view, Vol Details shows a colored bar at the top of each subdisk that indicates its volume type. The legend at the bottom of the pane shows the color-coding scheme. The legend can be toggled on and off with the **Show Legend** command.

Additionally, in the expanded view, as shown below, Vol Details shows the volume name and drive letter associated with each subdisk.

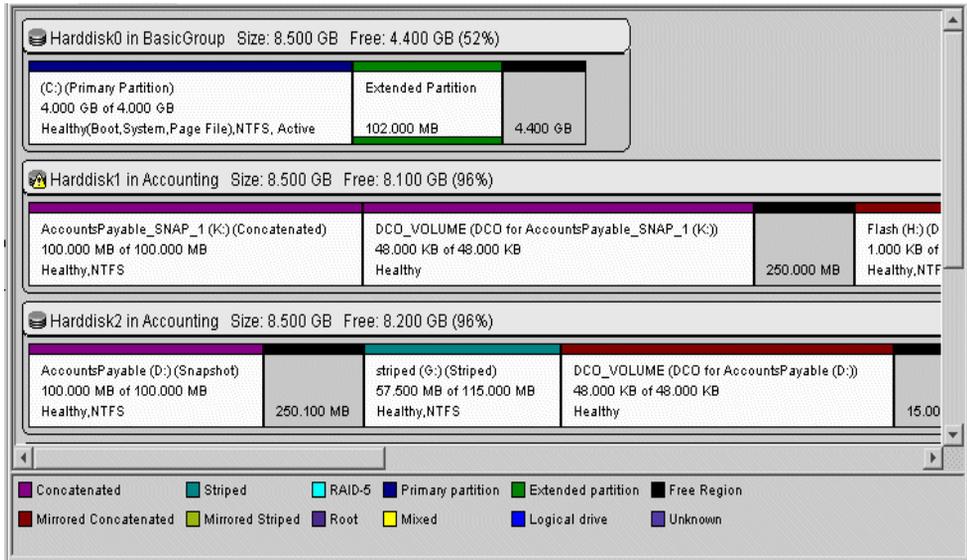
Figure 3-16 Volume details view



Full volume display

As shown below, **Full Volume Display** provides even more information about the subdisks. It is available only in the expanded view and only when the Vol Details option is selected. In addition to the volume name and type, Full Volume Display shows the volume size and status.

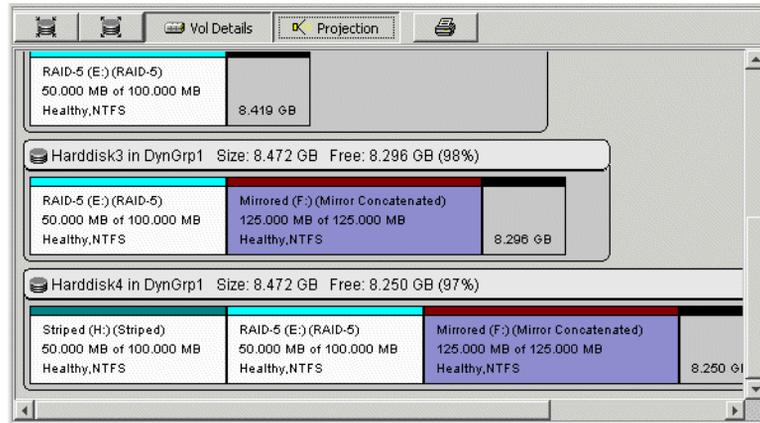
Figure 3-17 Full volume display view



Projection

Projection highlights all the subdisks associated with a selected volume. After the **Projection** command is selected, click a subdisk. The selected subdisk becomes dark purple, and the other subdisks in that volume become a lighter purple. In the example below, the projection feature was turned on, and the subdisk named “Mirrored (F:)” on Harddisk3 was selected. That subdisk became dark purple, and the other mirror that is part of the volume “Mirrored (F:)” (located on Harddisk4) became a lighter purple. This feature can be useful for viewing a volume that is spread across several disks.

Figure 3-18 Projection feature



Context menu available from disk view

The context-sensitive menu of commands that is available by right-clicking on a volume or disk in the tree view is also available by right-clicking a subdisk or disk in the Disk View. Additionally, in the separate Disk View window, the context-sensitive commands are available on the **Action** menu.

Also, in Disk View you can drag and drop subdisks instead of using the **Subdisk Move** command (if drag and drop is enabled in the general preferences).

Search

The Search feature allows you to find specific volumes, disks, or disk groups on a large system or to find a list of volumes, disks, or disk groups meeting specified criteria.

This section has the following topics:

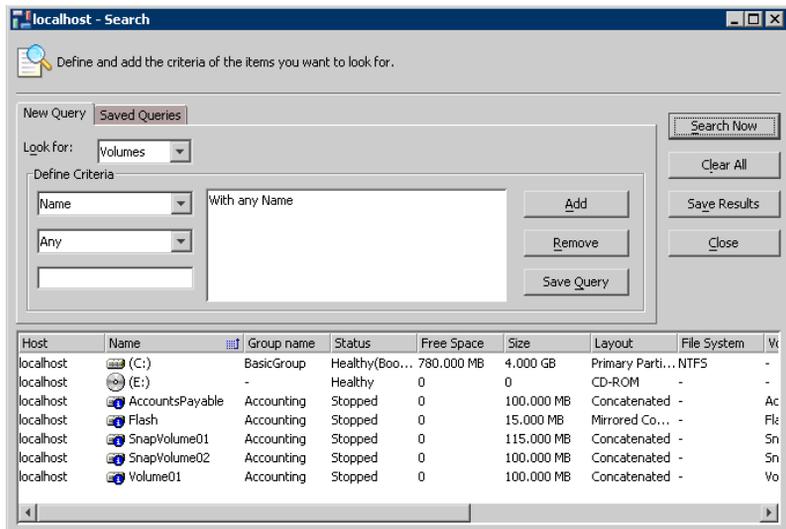
- [Conducting a search](#)
- [Using saved queries](#)
- [Creating search reports](#)

Note: Searches are case sensitive.

Conducting a search

To conduct a search

- 1 Click the **Search** button on the VEA console toolbar or select **Tools>Search** from the menu bar to open the Search window.



- 2 Click the **New Query** tab to display the available search criteria.
- 3 Select the object type from the drop-down list to the right of the words "Look for:" (near the top left corner of the window). The choices are Volumes, Disks, or Disk Groups.

- Select the attribute you want to search for. The available attributes depend on the object type.

Table 3-4 Attributes Available for Each Object Type

Attributes for Volume	Attributes for Disk	Attributes for Disk Group
Name	Name	Name
Volume Name	Disk Group Name	Imported
Disk Group Name	Status	Size
Status	Size	Free Space
Device	Free Space	
FS Capacity		
FS Label		
FS Free Space		

Note: "FS" means "File System."

- Define the limiter you want to use.
Searches may be limited by the following options:

- Any** Finds all instances of the selected attribute.
It is not necessary to enter more criteria in the text box below the limiter box. For example, searching Disk Groups for any Free Space will return all disk groups with free space available.
- Contains** Finds any of the selected attributes that contain the string that is entered in the text box below the limiter box.
Contains acts as a wildcard (*) and will search for the string anywhere within a longer string. For example, searching Volumes for a name that contains "Stripe" will return all volumes that have the string "Stripe" anywhere in the volume name, including "Striped (H:)" and "JKStriped (J:)." Because searches are case sensitive, "Stripe" will not find "Astripedvolume (L:)."
- Is** Finds only an exact match with the string entered in the text box below the limiter box.
It is useful for finding a specific volume, disk, or disk group on a very large system. For example, searching Disks for "Name is Harddisk1" will return Harddisk1. You must enter the exact information, including the drive letter or location for volumes.

Is not Excludes the specific information entered in the text box below the limiter box.
For example, searching Volumes for “FS Type is not FAT32” will return all volumes that are not formatted as FAT32.

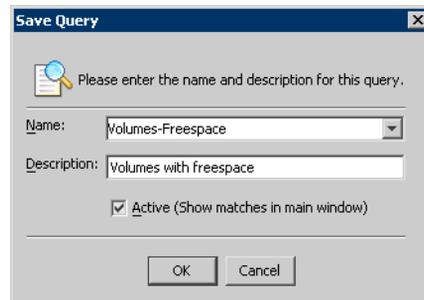
- 6 Enter the search string in the text box below the limiter box. Searches are not case sensitive.
- 7 Click the **Add** button to create the search term, which appears in the box to the right.

If more than one search term is defined, they will be joined by a logical “and” operator; that is, the result will contain all of the search terms. For example, a search for the terms “Volumes with Free Space” and “any NTFS Volumes” will result in a list of all volumes that both are formatted as NTFS and contain free space.

The logical “or” operator is not provided in this search function.

The **Remove** button can be used to delete a highlighted search term.

The **Save Query** button allows you to save the query you created for future use.



Follow these steps to save a query:

- Click the **Save Query** button to open the Save Query window.
 - Enter a name to identify the query you are saving.
 - Enter a brief description of the search that the query performs.
 - Check the **Active** checkbox if you want the results of the query displayed in the VEA console.
 - Click **OK** to save the query.
- 8 Click the **Search Now** button to complete the search.
The search results will appear in the lower pane.
You can double-click a specific storage object (disk, volume, or disk group) in the search results to bring up the information in the VEA console.

- 9 If you would like to save the results of the search, click the **Save Results** button.

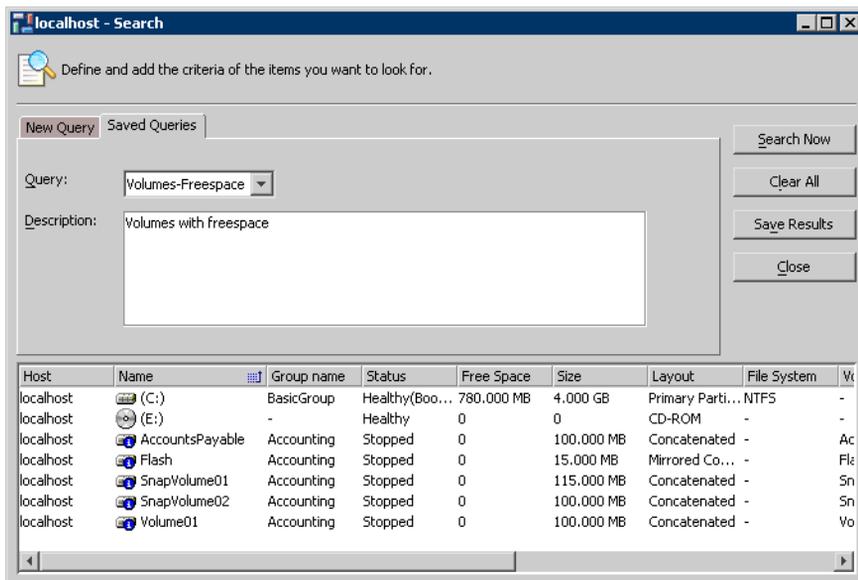
The Save dialog box appears.

- Select the folder where you want to save the file.
- Enter a name for the file in the **File name** field.
- Click **Save** to save the file and close the dialog box. The file will save as a text file with a .txt extension.

- 10 Clicking the **Clear All** button will delete all the search terms and results. This allows for a new search.

Using saved queries

- 1 Click the **Search** button on the VEA console toolbar, or select **Tools>Search** from the menu bar to open the Search window.



- 2 Click the **Saved Queries** tab in the Search window.
- 3 Select a previously saved query from the drop-down list to the right of the words “Query:” (near the top left corner of the window). The choices are all the previously saved queries.
If a description of the query was saved with the query, it will be displayed in the Description message box.
- 4 Click the **Search Now** button to run the search.

The search results will appear in the lower pane.

You can double-click a specific storage object (disk, volume, or disk group) in the search results to bring up the information in the VEA console.

- 5 If you would like to save the results of the search, click the **Save Results** button.

The Save dialog box appears.

- Select the folder you want to save the file to.
 - Enter a name for the file into the **File name** field.
 - Click **Save** to save the file and close the dialog box. The file will save as a text file with a .txt extension.
- 6 Clicking the **Clear All** button will delete the search results and allow you to run another search.

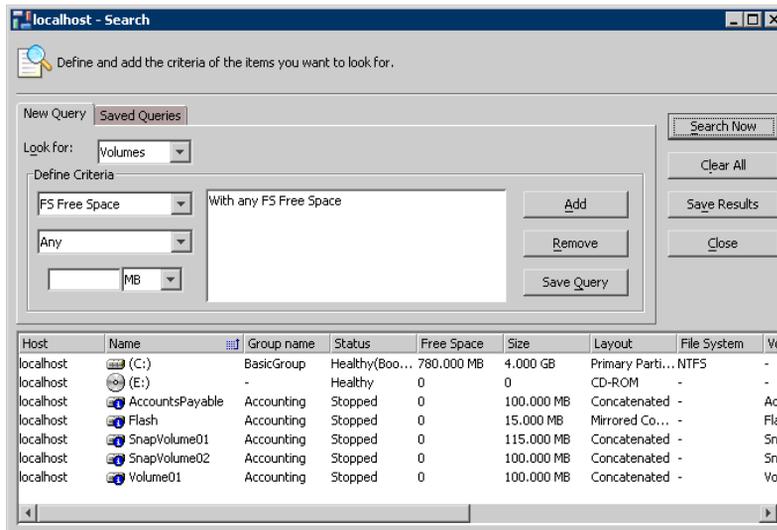
Creating search reports

This section describes how to create reports from the results of the Search feature. Using the **Search** command, it is possible to generate a wide variety of reports that provide information on the disk groups, disks, and volumes on each server. The results of these searches can be saved and imported into Microsoft Excel or any other spreadsheet or database application that accepts tab-delimited text files. The results can be sorted, displayed as graphs or charts, and imported into written reports or PowerPoint presentations.

Search reports provide a snapshot of a system at a particular point in time. By running the same search on a regular schedule (monthly, annually, etc.), information can be collected, evaluated, and used to better manage the system.

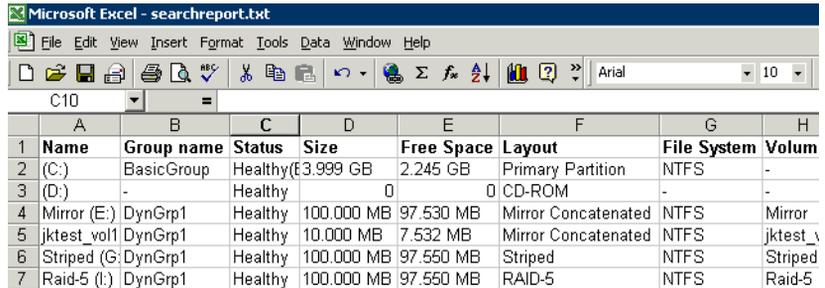
The following sample report was created by using the Search feature and Microsoft Excel.

- 1 Determine the categories you want to include in your report, and use the Search feature to output the results to a text file.



This search lists the free space available on all the volumes located on the accessed server. After the search results are saved by using the

Save Results button, a Microsoft Excel report can be generated similar to the one shown below.



	A	B	C	D	E	F	G	H
1	Name	Group name	Status	Size	Free Space	Layout	File System	Volum
2	(C:)	BasicGroup	Healthy	3.999 GB	2.245 GB	Primary Partition	NTFS	-
3	(D:)	-	Healthy	0	0	CD-ROM	-	-
4	Mirror (E:)	DynGrp1	Healthy	100.000 MB	97.530 MB	Mirror Concatenated	NTFS	Mirror
5	jktest_vol1	DynGrp1	Healthy	10.000 MB	7.532 MB	Mirror Concatenated	NTFS	jktest_\
6	Striped (G:)	DynGrp1	Healthy	100.000 MB	97.550 MB	Striped	NTFS	Striped
7	Raid-5 (I:)	DynGrp1	Healthy	100.000 MB	97.550 MB	RAID-5	NTFS	Raid-5

Follow these steps to generate the search report:

- 2 Open the Excel application.
- 3 Click File>Open to open the .txt file saved by the SFW search.
- 4 You will have to select All Files (*.*) from the Files of type drop-down menu. Navigate to the correct file and click the **Open** button.
- 5 In the Text Import wizard that appears, do the following:
 - Select the file type that best describes your data.
 - Select Tab to be the delimiter.
 - Select the General data format.
 - Click **Finish** to complete your report in Excel.
 Refer to the Microsoft Excel help for more information about the commands and features available in Excel.

Types of search reports

The type of search and search report you generate depends on the object type you base your search on.

Table 3-5 Attributes Available for Volume, Disk, or Disk Group Search

Attributes for a Volume Search	Attributes for a Disk Search	Attributes for a Disk Group Search
Name	Name	Name
Volume Name	Disk Group Name	Imported
Disk Group Name	Status	Size
Status	Size	Free Space
Device	Free Space	
FS Capacity		
FS Label		
FS Free Space		

Note: "FS" means "File System."

Each search is run only on the specific server selected. For convenience, you could write a macro to automate the Excel steps in the report. By opening the search text files from multiple servers in Excel and running the macro, you can generate a combined report for a group of servers. The table that follows lists some sample searches and the types of report that would be generated.

Table 3-6 Sample Searches and Results

Search	Criteria	Report Shows
Volume	FS Free Space, any	All volumes that contain free space
Volume	Status is degraded	Volumes whose state is degraded and that might fail soon
Disk	Size greater than 10 GB	All disks larger than 10 GB
Disk	Free Space greater than 1 GB	All disks with more than 1 GB of free space
Disk	Disk Group is DynGrp1	All disks in DynGrp1
Disk Group	Name, any	All disk groups. Useful to run the search on multiple servers

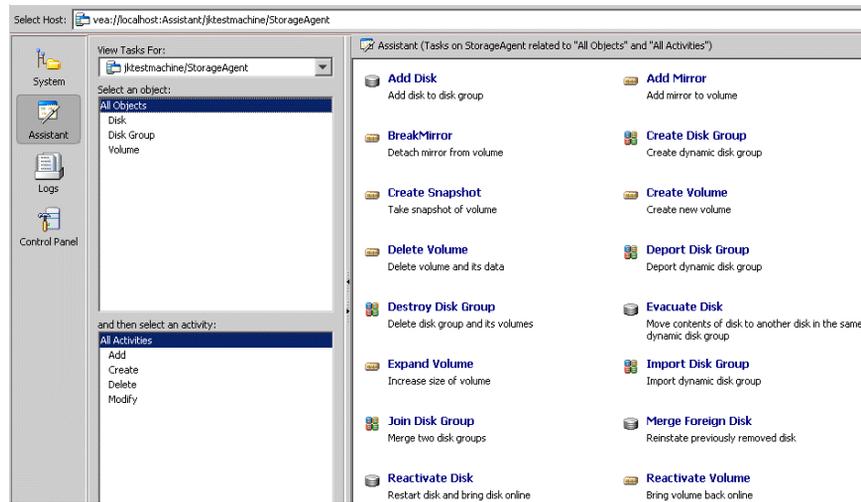
Assistant perspective

The purpose of the Assistant is to make available the most commonly used commands in the program.

To access the Assistant, select **Assistant** in the Perspective Bar. Then select the object from the drop down located on the left side of the window that you would like to perform tasks on. To perform tasks on disks, disk groups, and volumes select StorageAgent from the drop down.

Command icons appear in the pane located on the right side of the window when StorageAgent is selected. Clicking a command icon launches the dialog for the command.

Figure 3-19 Storage Foundation Assistant



The type of commands displayed in the Assistant is controlled by selecting an object in the object pane and an activity in the activity pane located on the left side of the window. For example, selecting Disk in the object pane and Modify in the activity pane displays commands that pertain to modifying disks. Selecting All Objects in the object pane and selecting All Activities in the activity pane would display all the commands that are available in the Assistant.

Logs perspective

The **Logs** perspective displays Alert Log and Task Log messages associated with the SFW storage objects. Select the appropriate tab to access the log you are interested in.

For detailed information on the Alert Log, see “[Alert log](#)” on page 234.

Figure 3-20 Alert log



The screenshot shows a window titled "Browse Domain" on the left and "Alert Log" on the right. The "Alert Log" window has a tab for "Task Log" and a "Filter Alerts" button. Below the button is a table with two columns: "Date/Time" and "Message".

Date/Time	Message
10/6/06 8:55 AM	Refresh Completed.
10/6/06 8:55 AM	VSS Writers and their Components Refreshed Succ
10/6/06 8:54 AM	Refresh Started.
10/6/06 8:49 AM	Rescan Completed.
10/6/06 8:49 AM	Rescan started.
10/6/06 8:49 AM	Refresh Completed.
10/6/06 8:49 AM	Refresh Started.

Control Panel perspective

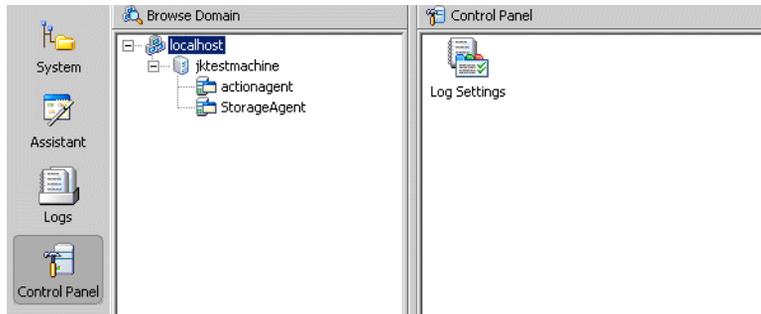
To access the Control Panel, select **Control Panel** in the Perspective bar. Expanding the tree view displays the system objects. Selecting one of the system objects displays the Control Panel objects for that system object in the right pane.

Like the Windows Control Panel, this Control Panel has icons that open up into windows with settings for various functions within the program.

Selecting localhost displays the following:

- [Log settings](#)

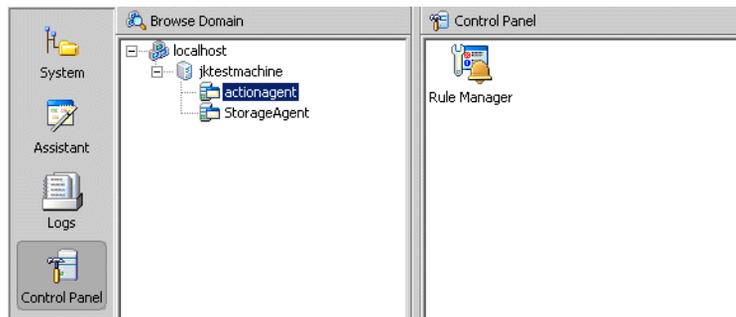
Figure 3-21 Control panel for localhost



Selecting actionagent displays the following:

- [Rule Manager](#)

Figure 3-22 Control panel for actionagent

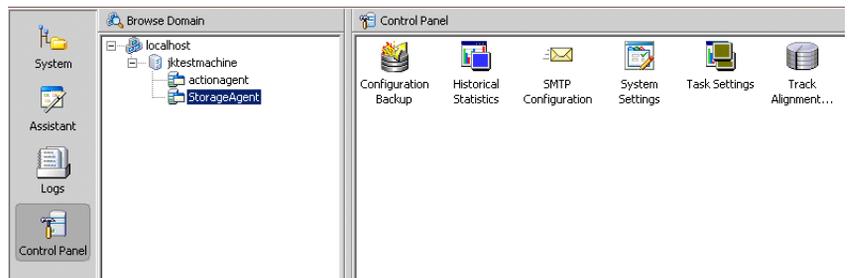


Selecting StorageAgent displays the following:

- Configuration backup
- Historical statistics
- SMTP configuration
- System settings
 - Hot relocation
 - Snap Shot
 - GUID recycle
 - SCSI Support
 - SmartMove
 - Disk Management Snap-in
- Task settings
 - Task throttling
 - Configuration task performance tuning
- Track alignment

To access any of these functions, double-click the appropriate icon in the Control Panel.

Figure 3-23 Control panel for StorageAgent



Log settings

Double-clicking the Log Settings icon brings up the Log Settings dialog box. This dialog box allows you to set the maximum amount of storage used for the Alert Log and the Task Log.

The Alert Log lists events or alerts pertaining to the Veritas Storage Foundation for Windows program.

The Task Log is a listing of tasks, such as formatting a volume or resynchronizing a volume. The Task Log Settings window allows you to set the maximum log size and to specify a policy when the maximum log size is reached. See “[Log configuration](#)” on page 236.

Rule Manager

Double-clicking this icon brings up the Rule Manager window, that allows you to configure rules for event notification messages and actions.

See “[Event notification](#)” on page 236.

Configuration backup

Double-clicking the Configuration Backup icon brings up the Configuration Backup window. Configuration Backup can preserve disk group, dynamic disk, and volume configuration information that can be used in the recovery of a disk. For information about recovering a disk, see “[vxcbr](#)” on page 404.

Configuration Backup only backs up the configuration of disk groups that are online. Any offline or deported disk groups are not processed by this operation.

Enter the following settings in the Configuration Backup window to back up the configuration of disk groups:

- Automatic Checkbox
 - Check this checkbox to have the back up operation run every time that a configuration change occurs.
 - Clear this checkbox to have the back up operation only run when clicking **OK**.
- Number of copies

The number of back up copies of the configuration to create. (Range of copies: 5-1024.)
- Number of minutes between backups

The interval of time between back up copies, when **Automatic** is selected. (Range of minutes: 60 minutes - 10080 minutes (1 week).) This setting is ignored when **Automatic** is not selected.
- Directory for automatic backup

The path of the target directory for the back up copies, when **Automatic** is selected.

- Directory for manual backup

The path of the target directory for the back up copies, when **Automatic** is not selected.

Click **OK** when all the settings have been entered. (Clicking **Reset** before clicking **OK** recalls the previously saved settings.)

Historical statistics

Double-clicking the Historical Statistics icon brings up the Historical Statistics Settings dialog box. This dialog box lets you define the file size for the files that will be used for historical data collection. It also has a setting for the data collection rate.

See “[Configuring settings in the historical statistics settings window](#)” on page 533.

SMTP configuration

Double-clicking the SMTP Configuration icon brings up the SMTP Settings dialog box. This dialog box lets you define the IP address of the SMTP mail server on your network so that email notifications can be sent automatically. It also has settings for the port of the SMTP mail server and the email address that is used for sending email.

See “[SMTP configuration for email notification](#)” on page 253.

System settings

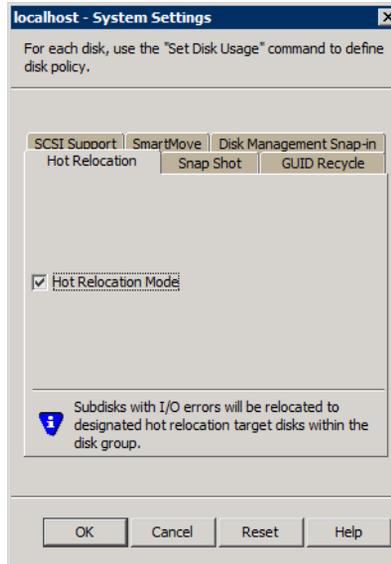
Double-clicking the System Settings icon brings up the System Settings dialog box. The dialog box lets you enable the hot relocation volume feature, set the volume snapshot method, set GUID recycling, set SCSI support, and enable SmartMove.

Hot relocation

Clicking the Hot Relocation tab brings up the Hot Relocation window. Check the Hot Relocation Mode checkbox to enable the feature. When a subdisk containing a redundant volume fails, hot relocation automatically moves the redundant volume from the failed disk to hot spare disks, or to other free space if no space is available on hot spare disks.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support Hot Relocation.

Figure 3-24 Hot relocation tab

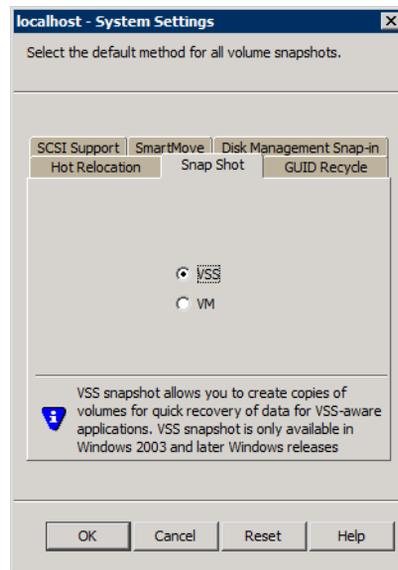


See [“Hot relocation”](#) on page 268.

Snap Shot

Clicking the Snap Shot tab brings up the Snap Shot window. Click **VSS** or **VM** to select the snapshot method to use for taking snapshots.

Figure 3-25 Snap shot tab



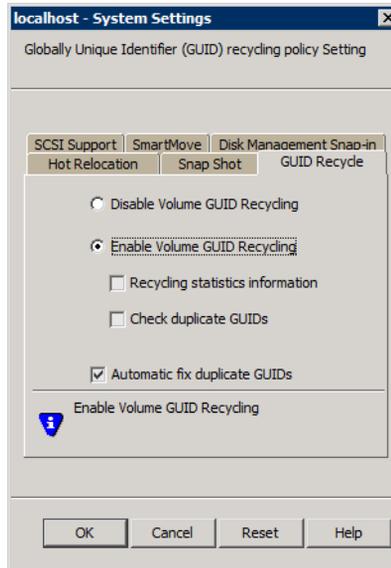
VSS and VM snapshot methods offer the following:

- The VSS snapshot method allows you to create copies of volumes for VSS-aware applications, such as Microsoft Exchange. For VSS-aware applications, the VSS snapshot method quiesces the application before taking the snapshot. For applications that are not VSS-aware, the VSS snapshot method does not quiesce the application before taking the snapshot. The VSS snapshot only creates read only snapshots.
- The VM snapshot method allows you to create copies of volumes for any application. The copies may be either read only or read/write depending on the setting of the volume being copied. In other words, a snapshot of a read only volume results in a read only snapshot and a snapshot of a read/write volume results in a read/write snapshot.

GUID recycle

Clicking the GUID Recycle tab brings up the GUID Recycle window.

Figure 3-26 GUID Recycle tab



A Globally Unique Identifier (GUID) is a Windows convention to identify components and objects in the system. In some environments, the number of GUIDs in the system may exhaust the storage in the Windows registry. Enabling volume GUID recycling helps to avoid this situation by using GUIDs from a GUID recycle list. The GUID recycle list is a list of GUIDs that have been previously used, but are no longer needed by the system.

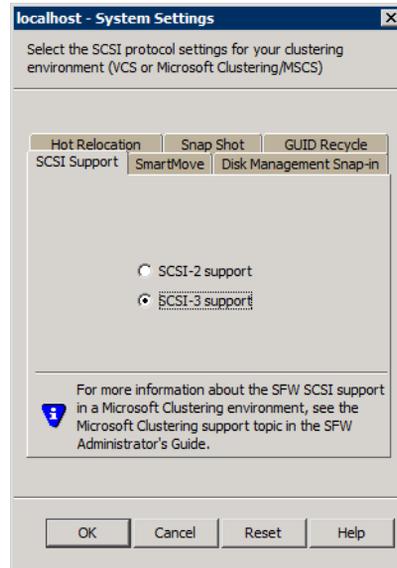
To enable GUID recycling, select **Enable Volume GUID Recycling** and the desired settings as follows:

- GUID recycling statistics
Enables the monitoring of how many times a GUID from the GUID recycle list is used.
- Check for duplicate GUIDs
Enables a check to see if a GUID selected from the GUID recycle list is already being used in the system.
- Automatically fix duplicate GUIDs
Enables the generation of another GUID when a GUID is found to be already in use in the system.

SCSI Support

Clicking the SCSI Support tab brings up the SCSI Support window.

Figure 3-27 SCSI Support tab



Click **SCSI-2 support** or **SCSI-3 support** to select the protocol setting to support your storage devices in a clustering environment (VCS or Microsoft Clustering/(MSCS)).

- For Windows Server 2003, SCSI-2 is the default setting.
- For Windows Server 2008, SCSI-3 is the default setting when SFW support for the Microsoft Failover Cluster is installed.
If SFW support for Microsoft Failover Cluster is not installed, SCSI-2 is the default setting.

Selecting SCSI-3 enables SFW clustering support to issue SCSI-3 commands to your SCSI-3 enabled storage devices. For this selection, setting the DMP DSMs for SCSI-3 support has no effect.

For more information about DMP DSMs, see [Chapter 13, “Dynamic multi-pathing software”](#) on page 717.

Selecting SCSI-2 enables SFW clustering support to issue SCSI-2 commands to your storage devices. If your storage devices are enabled for SCSI-3 commands, the DMP DSMs translate the SCSI-2 commands into SCSI-3 commands, if the DMP DSMs setting for SCSI-3 support is enabled.

Note: The SCSI Support window in the SFW Control Panel does not enable/disable SCSI-3 support of DMP DSMs.

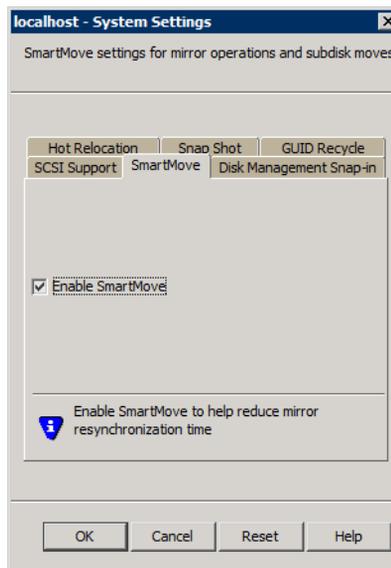
For more information about enabling SFW SCSI support for Microsoft Clustering, see “[Additional considerations for SFW Microsoft Clustering support](#)” on page 778.

For more information about enabling SFW SCSI support for VCS, see “[Additional considerations for SFW VCS support](#)” on page 794.

SmartMove

Clicking the SmartMove tab brings up the SmartMove window.

Figure 3-28 SmartMove tab



Check **Enable SmartMove** to enable the SmartMove setting to help reduce the the resynchronization time for mirror operations and subdisk moves. SmartMove reduces the resynchronization time by using NTFS file system metadata to resynchronize only those regions that the NTFS file system uses. When SmartMove is not enabled, SFW resynchronizes all regions.

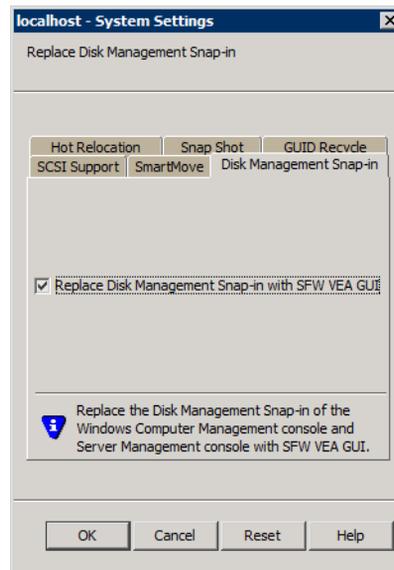
Note: SmartMove does not support non-NTFS disks.

Disk Management Snap-in

Clicking the Disk Management Snap-in tab brings up the Disk Management Snap-in window.

The Disk Management Snap-in tab is shown below.

Figure 3-29 Disk Management Snap-in tab



Check Replace Disk Management Snap-in to replace the Disk Management Snap-in in the Windows Computer Management and Server Manager consoles with the SFW VEA GUI. The SFW VEA GUI becomes accessible in both the Windows Computer Management console and the Windows Server Manager console.

Uncheck Replace Disk Management Snap-in to access the Disk Management Snap-in in the Windows Computer Management and Server Manager consoles. Also, in a similar way, the following commands can be used to make the Disk Management Snap-in or the SFW VEA GUI accessible in the Windows Computer Management and Server Manager consoles.

Replace Disk Management with VEA GUI	<code>regsvr32 "%VMPATH%\extens.dll"</code>
Enable Disk Management	<code>regsvr32 /u "%VMPATH%\extens.dll"</code>
Replace Disk Management with VEA GUI (silent mode)	<code>regsvr32 /s "%VMPATH%\extens.dll"</code>
Enable Disk Management (silent mode)	<code>regsvr32 /s /u "%VMPATH%\extens.dll"</code>

Note: Silent mode suppresses a Windows pop-up after the command is entered.

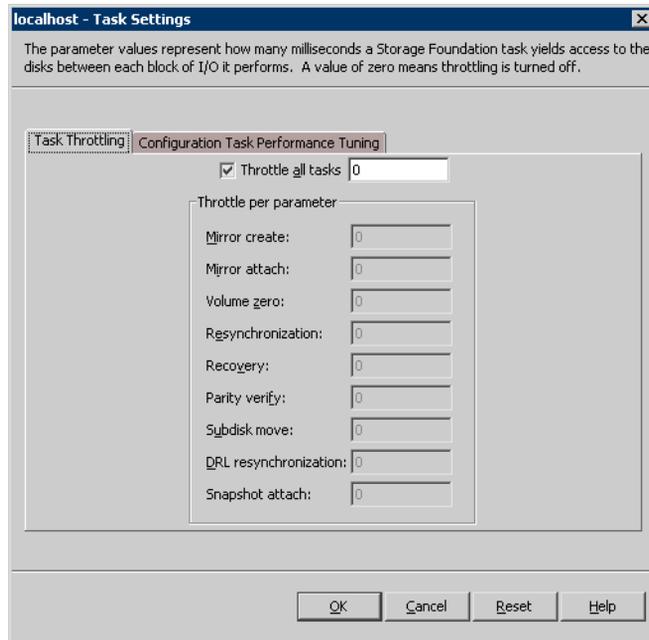
Task settings

Double-clicking the Task Settings icon brings up the Task Settings dialog box. The dialog box lets you enable the task throttling feature and set the configuration task performance tuning feature.

Task throttling

Clicking the Task Throttling tab brings up the Task Throttling window. Task throttling allows you to determine the priority of certain tasks.

Figure 3-30 Task throttling tab



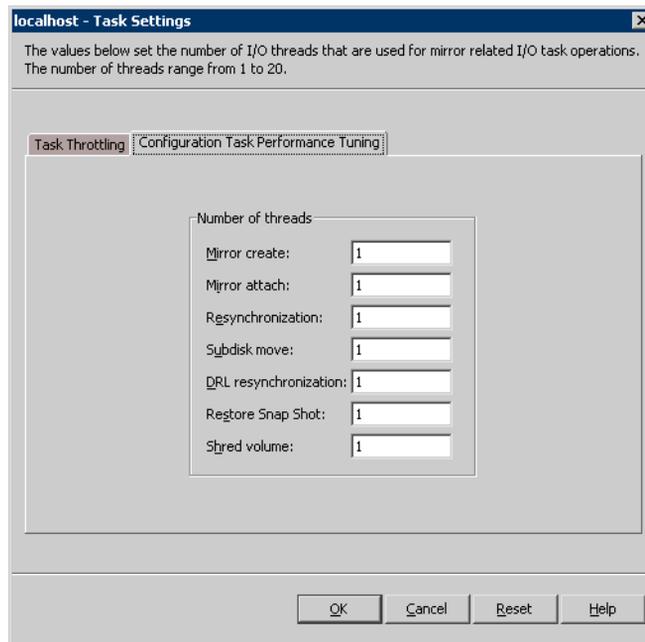
Using task throttling causes an operation to insert pauses for the specified amount of time during I/O. These pauses help to reduce any interference that may occur with the I/O of other applications running on the system. By selecting the **Throttle all tasks** checkbox, you apply the time delay that is specified in the text field to all Storage Foundation for Windows tasks. To apply the time delay to individual tasks, uncheck the checkbox, enter the number of milliseconds in each task's text field, and click **OK**. Depending on your total system I/O activity, a time delay of 300 to 500 milliseconds may result in a favorable balance of I/O

for Storage Foundation for Windows tasks and other applications. The **Reset** button restores default settings.

Configuration task performance tuning

Clicking the Configuration Task Performance Tuning tab brings up the Configuration Task Performance Tuning window.

Figure 3-31 Configuration task performance tuning



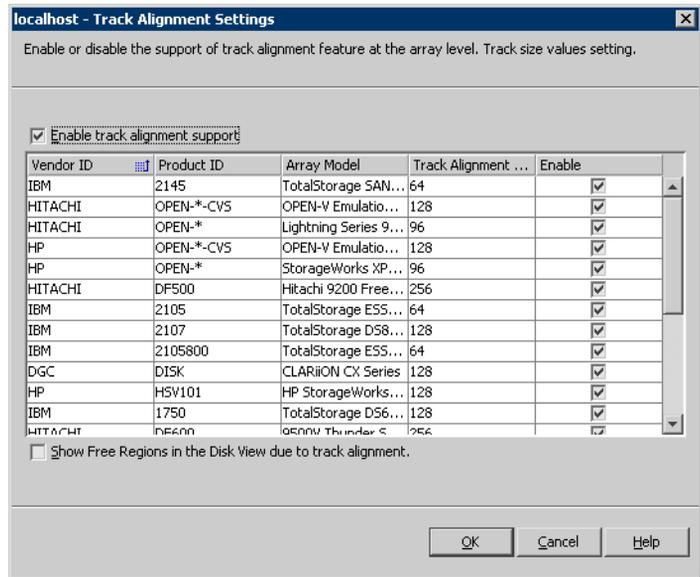
Configuration task performance tuning allows you to set the number of I/O threads to perform certain mirror-related operations, such as creating a mirror or adding a mirror. The performance of the operation is affected by the number of threads specified.

Track alignment

Double-clicking the Track Alignment icon brings up the Track Alignment Settings dialog box. This feature allows you to set dynamic volumes to store blocks of data in alignment with the boundaries of the physical track of the disk. Storing data so that it is aligned with track boundaries helps optimize I/O performance. Check the Enable track alignment support checkbox to enable the

feature for the arrays listed in the dialog box. You may also check the Show Free Region checkbox to display additional region information in the Disk View GUI.

Figure 3-32 Track alignment settings



Arrays not explicitly listed in the dialog box can be enabled as Default. (SFW sets all arrays in the Default category a vendor ID of 'default' and a product ID of 'default'.) This setting may or may not optimize I/O performance for the array. Contact your array manufacturer for details about track alignment and offset values.

You can use the CLI command “`vxdisk set track`” on page 336 to adjust the setting for track alignment for arrays enabled as Default.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support track alignment.

Working with disks, partitions, and volumes

- [Adding storage](#)
- [Disk tasks](#)
- [General Partition/Volume tasks](#)
- [Basic disk and volume tasks](#)

Adding storage

This section describes the commands that are used in adding storage to your system.

The topics are as follows:

- [Add a new disk to your system](#)
- [Add a disk signature to a disk](#)
- [Add a disk to a dynamic disk group](#)
- [Create new volumes](#)

Add a new disk to your system

To add a new disk to your system

- 1 Install the new physical disk or disks.
- 2 From the **Actions** menu, select **Rescan**.
See “[Update disk information by using rescan](#)” on page 147.

Note: On Windows Server 2008, you also need to bring the disk online to make the disk accessible. To bring the basic disk back online, right-click the disk to bring up the context menu and select the **Online** command.

- 3 After the operation is finished, the VEA console displays current information.
If Veritas Storage Foundation for Windows does not detect the new disk, you may need to reboot.
A brand new disk will have no signature or partition style. You can add a signature and partition style by using the **Write Signature** command described in the next topic.
For more information about partition styles, see “[What can you do with a basic disk?](#)” on page 183
New disks are added to the computer as basic disks. You can upgrade new disks to dynamic disks at any time.

Add a disk signature to a disk

A new disk must have a signature on it before it can be used.

When you install a new disk and then do a **Rescan**, the new disk appears under the **Disks** icon. The disk will display with the words “(No Signature)” in the tree view. If left unsigned, the disk cannot be used.

Once a signature appears on a disk, the disk displays as a basic disk. You can create partitions on the basic disk, or you can upgrade the disk to dynamic to allow you to create dynamic volumes on it.

In Volume Manager 2.7 and in earlier versions of the program, the command **Upgrade a Dynamic Disk** was used to change a basic disk to a dynamic disk. In Volume Manager 3.0 and later versions of the program, use the command **Add Disk to Dynamic Disk Group** to change a basic disk to a dynamic disk.

See “[Add a disk to a dynamic disk group](#)” on page 141

You can also make a basic disk into a dynamic disk by including it as a member disk when creating a new disk group with the **New Dynamic Disk Group** command.

See “[Create dynamic disk groups](#)” on page 53.

To add a signature to a disk

- 1 Right-click the unsigned disk.
The **Write Signature** command appears in the context menu. (The **Write Signature** command appears only if a disk does not have a signature on it.)
- 2 Select **Write Signature** from the context menu.
The Write Disk Signature dialog box will appear. Select the disks you wish to add a signature to.
To select a disk, click on it in the list of available disks and click the **Add** button. To select all the disks, click the **Add All** button.
To remove a disk from the **Selected disks** list, select the disk in the **Selected disks** list and click the **Remove** button. To remove all the disks from the **Selected disks** list, click the **Remove All** button.
- 3 Select the partition style of the disk by clicking the radio button for one of the following:
 - **MBR**
MBR (Master Boot Record) is a style that is limited to 4 primary partitions. It is available on MS-DOS, Windows 95/98, and later Windows versions.
 - **GPT**
GPT (GUID Partition Table) is a style that allows a maximum of 128 primary partitions. It is available on Windows Server 2003 and later

64-bit systems and on Windows Server 2003 SP1 and later 32-bit systems.

- 4 Once you have selected the disks and style, click the **OK** button. Click the **Cancel** button to exit without adding a signature to the disk or disks selected.

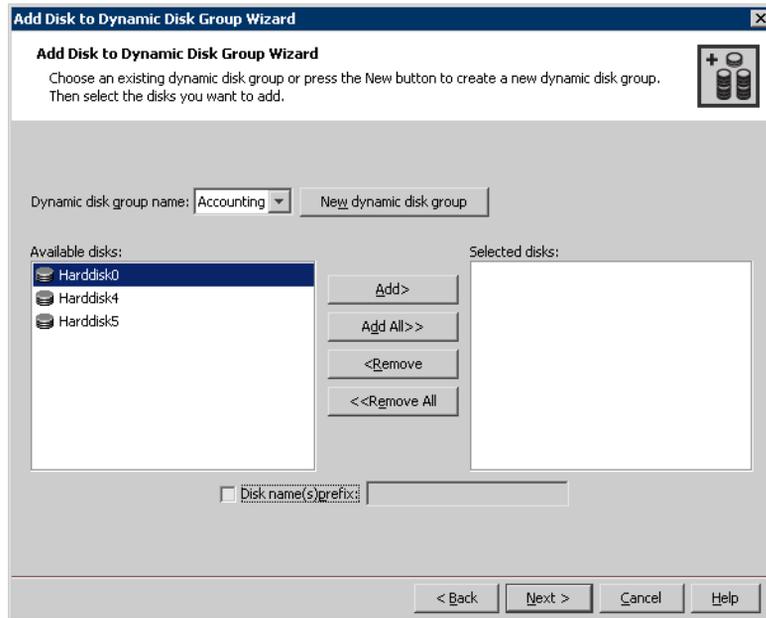
Add a disk to a dynamic disk group

If you want to add more disks to a dynamic disk group after the group is created, use the **Add Disk to Dynamic Disk Group** command. You can also use this command to first create a new dynamic disk group and then specify the disks to be added to it.

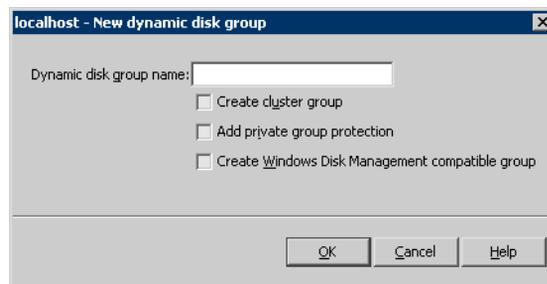
To add a disk to a dynamic disk group

- 1 Right-click a basic disk in the tree view or the **Disk View** tab in the right pane.
- 2 In the context menu that comes up, select **Add Disk to Dynamic Disk Group**.
- 3 The Add Disk to Dynamic Disk Group wizard appears. Click **Next** to continue.
- 4 In the next screen, select one or more disks and the dynamic disk group you want to add them to.

Optionally, check the **Disk names prefix** checkbox and enter a disk name prefix to give the disks in the disk group a specific identifier. The identifier precedes a system-generated numeric ID that SFW uses to distinguish the disks in the disk group. For example, entering TestGroup as the prefix for a disk group that contains three disks creates TestGroup1, TestGroup2, and TestGroup3 as internal names for the disks in the disk group. Click **Next** to continue.



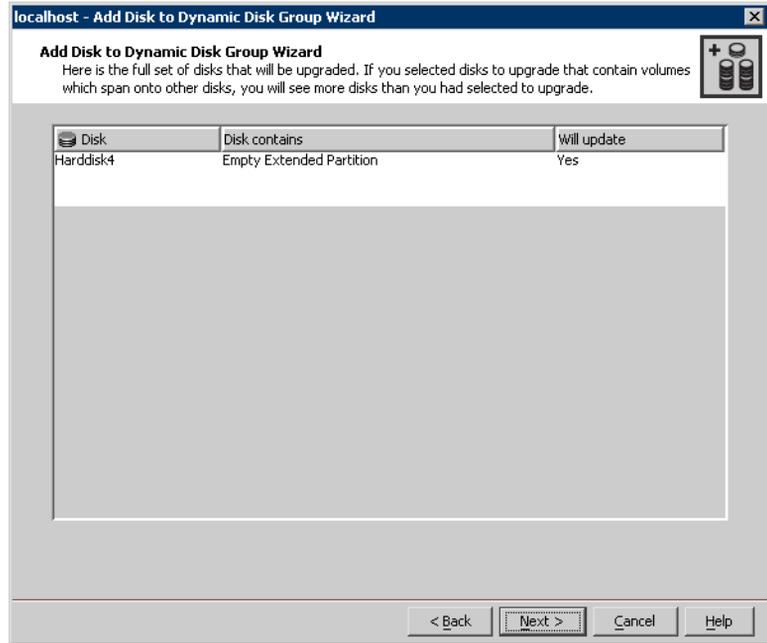
If you want to create a new dynamic disk group to add the disk to, click the **New dynamic disk group** button. The New dynamic disk group window appears to allow you to indicate the disk group name and characteristics.



For details on the options for creating a disk group, see step 4 of the procedure on creating a dynamic disk group.

See [“Steps for creating a dynamic disk group”](#) on page 55.

- 5 A confirmation screen appears listing the selected disk or disks. Click **Next** to continue if you are satisfied with the selections, or choose **Back** to go back to modify your disk selection.



For each disk, information is provided on whether it contains volumes and whether it will be updated. If it is not going to be updated, you will want to modify the selection.

- 6 Click **Finish** in the final screen.
You could also create a new disk group for the new storage.
See [“Create dynamic disk groups”](#) on page 53.
You can also remove a disk from a disk group.
See [“Remove a disk from a dynamic disk group”](#) on page 144.

Create new volumes

At this point, you are ready to create new volumes on the storage.
See [“Create dynamic volumes”](#) on page 60.

Disk tasks

This section describes commands that deal with disk changes and maintenance. Topics are as follows:

- [Remove a disk from a dynamic disk group](#)
- [Remove a disk from the computer](#)
- [Offline a disk](#)
- [Update disk information by using rescan](#)
- [Set disk usage](#)
- [Evacuate disk](#)
- [Replace disk](#)
- [Changing the internal name of a disk](#)
- [Renaming an enclosure](#)
- [Work with removable media](#)
- [View disk properties](#)

See also the following related topics:

[“Add a new disk to your system”](#) on page 138

[“Add a disk signature to a disk”](#) on page 139

[“Disk monitoring”](#) on page 242.

[“Merge foreign disk command”](#) on page 487

Remove a disk from a dynamic disk group

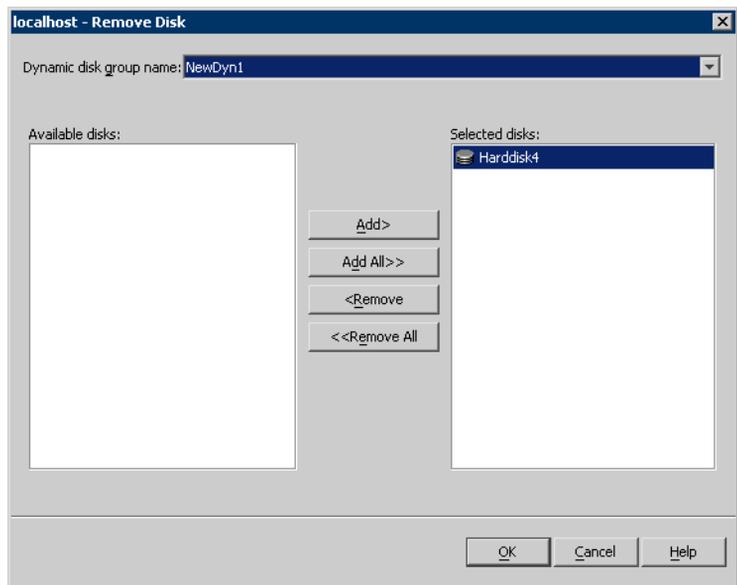
In the process of adding new storage, you may want to rearrange your disks in your existing disk groups. You can remove a dynamic disk from a dynamic disk group if there are no volumes on the disk. If volumes exist, you must delete them before you can remove the disk. Disks shown in Veritas Storage Foundation for Windows to be Unreadable or Foreign can be removed, but doing so causes you to lose all existing data on the disk that is removed from the group. If a disk has failed and is marked as Missing, you can also remove it from the dynamic disk group. However, you cannot remove the last disk from a disk group that is a Microsoft Clustering resource.

To remove a disk from a dynamic disk group, use the **Remove Disk from Dynamic Disk Group** command. Once you remove all the disks from a dynamic disk group, the disk group is removed from the GUI and the disks become basic disks.

Caution: Removing a disk that is Unreadable or Foreign from a dynamic disk group changes the disk into a basic disk and all of its data is lost.

To remove a disk from a dynamic disk group

- 1 Right-click the selected disk or on the dynamic disk group and select **Remove Disk from Dynamic Disk Group**.
- 2 Make sure the disk or disks that you want to remove are showing in the right pane of the window, and click **OK**.



Remove a disk from the computer

This section has information on removing a basic or dynamic disk from a computer.

Identifying a physical disk

To identify a physical disk that is represented by a disk that appears in the VEA GUI, use the **Ping Disk** command. This command flashes the fault light that is built into the housing of the physical disk. The command flashes the fault light until you stop the command. This is a very convenient feature when trying to identify a particular physical disk among many others.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Ping Disk** command.

To identify a physical disk

- 1 Right-click the selected disk and select **Ping Disk** from the context menu.
- 2 In the screen that appears, click **Start** to begin pinging the physical disk. The fault light flashes until you click **Stop**.
- 3 Click **Close** when you are finished using the command.

Basic disk

If you remove a basic disk from the computer and then do a rescan, the disk and its volumes will no longer show up in the VEA GUI.

Dynamic disk

If a dynamic disk's status remains Offline and Missing and you determine that the disk has a problem that cannot be repaired, you can remove the disk from the system by using the **Remove Disk from Dynamic Disk Group** command.

However, before you can remove the disk, you must delete all volumes on the disk. You can save any mirrored volumes on the disk by removing the mirror that is on the Missing disk instead of the entire volume. Deleting a volume destroys the data in the volume, so you should remove a disk only if you are absolutely certain that the disk is permanently damaged and unusable.

If a disk is marked Missing and is not connected to the computer, you can use the **Remove Disk from Dynamic Disk Group** command without worrying about the data.

Once you have removed the disk from the disk group, the disk becomes a basic disk and it can then be removed from the computer. Complete the process by doing a rescan.

See "[Remove a disk from a dynamic disk group](#)" on page 144.

Note: If you have a disk that appears to be deteriorating because it has many errors, you can easily move the data from that disk to another disk by using SFW's **Move Subdisk** command. See "[Moving subdisks](#)" on page 544.

Offline a disk

On Windows Server 2008, a basic disk can be taken offline for maintenance by using the **Offline** command. Right-click a basic disk in the VEA GUI to bring up a context menu and select the **Offline** command. To bring the basic disk back online, right-click the basic disk to bring up the context menu and select the **Online** command.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Offline** command. However, the **Online** command can be used on dynamic disks belonging to a Microsoft Disk Management Disk Group.

Update disk information by using rescan

When Veritas Storage Foundation for Windows rescans disks, it scans all disks for disk configuration changes. It also updates information about CD-ROM drives and other removable media, basic volumes, file systems, and drive letters. Rescanning disks can take several minutes, depending on the number of hardware devices installed.

Note the following:

- You should rescan disks when you remove disks from or add disks to a computer.
- From the **Actions** menu, select **Rescan**.
If you click the **Tasks** tab at the lower left corner of the VEA window, information on the progress of the rescan will display in the window's lower pane.
See also "[Additional important information about the rescan command](#)" on page 486.

Note: The **Rescan** command is only effective on the StorageAgent node and any of its sub-nodes.

Set disk usage

This command allows you to make settings for the hot relocation function, including making a disk a hot spare.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support setting disk usage.

It is described in detail in the section “[Hot relocation](#)” on page 268.

Evacuate disk

The **Evacuate Disk** command moves the entire contents of a healthy disk to the free space on another dynamic disk. If there is a failed volume on the original disk, the volume cannot be moved, and an error message will appear.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Evacuate Disk** command.

To evacuate a disk

- 1 In the left pane, right-click the disk you wish to evacuate.
- 2 Select **Evacuate Disk**.
- 3 The Evacuate Disk dialog will appear. Select either **Auto Assign destination disk** or **Manually assign destination disk**. If you chose **Manually assign destination disk**, assign the destination disk by selecting one disk from the display.
You may also check **Disable Track Alignment** to disable track alignment on the destination disk.
- 4 Click **OK** to evacuate the disk.

Replace disk

Disks most often need replacing when they fail or start to behave strangely. A failed dynamic disk can be replaced by an empty basic disk. The volume configuration will be recreated on the new disk. Active redundant volumes (mirrored and RAID-5) on the replaced disk will be resynchronized automatically after disk replacement.

Failed volumes on the replaced disk, however, will stay failed after disk replacement because no valid data is available for copy.

The disk replacement procedure can be performed only on a disk that has failed. The VEA console identifies the disk by renaming it “Missing Disk.” If the disk replacement is successful, the replacement disk will take on the attributes of the failed disk, including the disk name.

Note: This option is available only on Missing Disks.

If the original disk is returned to the system after it was replaced, it will show in the VEA console as a foreign disk and a disk group called Unknown Dg will be

created. Use the **Merge Foreign Disk** command to return the disk to the same dynamic disk group it was in before.

See “[Merge foreign disk command](#)” on page 487.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Replace Disk** command.

To replace a disk

- 1 Right-click the Missing Disk.
- 2 Select **Replace Disk**.
A dialog box appears containing a list of empty basic disks.
- 3 Select the disk you wish to use to replace the Missing Disk.
- 4 Click **OK** to perform the disk replacement.

Changing the internal name of a disk

You can change the internal name of a disk to make it easier to identify.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support changing the internal name of a disk.

To change the internal name of a disk

- 1 Expand the Disks node in the tree view.
- 2 Right-click the desired disk node.
- 3 Select **Change Disk Internal Name** from the context menu.
A dialog box appears to rename the disk.
- 4 Enter the new internal name of the disk.
- 5 Click **OK** to complete the operation.

The internal name of a disk can also be changed with the `vxedit` CLI command.

See “[vxedit](#)” on page 385.

Renaming an enclosure

You can rename an enclosure to make it easier to identify.

To rename an enclosure

- 1 Expand the Enclosures node in the tree view.
- 2 Right-click the desired enclosure node.
- 3 Select **Rename Enclosure** from the context menu.
A dialog box appears to rename the enclosure.
- 4 Enter the new name of the enclosure.
- 5 Click **OK** to complete the operation.

An enclosure can also be renamed with the `vxedit` CLI command.

See “[vxedit](#)” on page 385.

SFW provides an enclosure node in the tree view to represent the enclosure for the internal disks of your server. This enclosure cannot be renamed.

Renaming an enclosure in a cluster environment only renames the enclosure on the node that the rename operation occurs. You need to rename the enclosure on each of the other nodes in the cluster to maintain the same enclosure name throughout the cluster.

Work with removable media

Removable media include CD-ROM disks and other removable disks, such as Zip disks. There are a limited number of actions you can do in Veritas Storage Foundation for Windows for removable disks.

You can perform the following actions:

- You can create only one primary partition on removable-media devices. You cannot create extended partitions, logical drives, or dynamic volumes on removable-media devices. The primary partition must use up all unallocated space on the removable disk.
- You cannot upgrade removable-media devices to dynamic volumes.
- Removable-media devices can be formatted as FAT, FAT32, or NTFS.
- You cannot mark the primary partition on a removable-media device as active.
- You cannot delete the primary partition on a removable-media device.
- The **Eject** command allows you to eject a removable-media disk through the software rather than by a manual ejection mechanism.

Working with disks that support thin provisioning

Thin provisioning is a technology to allocate disk storage on an as needed basis. Disks that support thin provisioning are disks that are able to allocate storage as data is written to the disk. In addition, some of these disks are able to reclaim unused storage on the disk.

Disks that support thin provisioning have the following characteristics:

- Disk storage allocated as data is written to the disk.
- Unused storage may be reclaimed to minimize the amount of unused space on the disk.

Note: Not all disk vendors support storage reclamation. Disks that support both thin provisioning and storage reclamation are represented in the GUI as a disk with a green colored sector with an asterisk (*). Disks that support only thin provisioning are represented in the GUI as a disk with a red colored sector.

Reclaiming storage space from thin provisioned disks can be done for disk groups, disks, or volumes. The operation to reclaim storage may take a significant amount of time to complete.

Note: The operation to reclaim storage from thin provisioned disks is not supported for RAID-5, DCO, or VVR DCM volumes.

Note: The operation to reclaim storage is supported only for NTFS volumes.

Note: The reclaim storage operation is disabled during a shrink volume operation. The reclaim storage operation is enabled when the shrink volume operation has completed.

Reclaiming storage space from thin provisioned disks in a disk group

This section explains how to reclaim storage from thin provisioned disks in a disk group.

To reclaim storage space from thin provisioned disks in a disk group

- 1 In the VEA GUI, right-click the disk group in the tree view.
- 2 Select Thin Provisioning > Reclaim in the context menu.
- 3 On the Welcome page of the Disk Group Reclaim Wizard, click Next.
- 4 Select a reclaim type for the operation and click Next.
The reclaim types are:
 - Volumes only
Reclaim unused storage space from volumes.
 - Free space only
Reclaim free space from disks.
 - Volumes and Free space
Reclaim space from volumes and free space from disks.
- 5 Click Finish to complete the wizard.

Using a schedule to reclaim storage space from thin provisioned disks in a disk group

- 1 In the VEA GUI, right-click the disk group in the tree view.
- 2 Select Thin Provisioning > Schedule Reclaim in the context menu.
- 3 On the Welcome page of the Disk Group Reclaim Scheduler Wizard, click Next.

- 4 Select a reclaim type for the operation and click Next.
 The reclaim types are:
 - Volumes only
 Reclaim unused storage space from volumes.
 - Free space only
 Reclaim free space from disks.
 - Volumes and Free space
 Reclaim space from volumes and free space from disks.
- 5 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	Enter a unique name for the schedule. This name identifies the schedule if you later want to view information about the reclaim status. A default name consists of the ThinReclaim.1, the component name and a numbered suffix that increments with each schedule.
Description of this schedule	Optionally, enter a description to help you identify the schedule when you view information about the reclaim status.
Start Time	The time of the day to begin the reclaim operation.
End Time	The time of day to end the reclaim operation.. If a reclaim operation is in progress it is completed but a new one is not started after the end time.
Schedule takes effect on	The date on which the specified schedule takes effect. The default is the current date.
Restart task every	The interval between reclaim operations, in minutes. For example, if the interval is 360 minutes and you schedule a reclaim start time of 12 P.M. and an end time of 7 P.M, the reclaim operation occurs twice. If no interval is specified the reclaim operation occurs once.

Every	<p>Enable the Every option to have the reclaim schedule continue to occur. Otherwise the schedule applies only for one day.</p> <p>Specify the number of days before restarting the reclaim schedule.</p> <p>For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.</p>
Start On	<p>If you enable the Every option, specify the starting date.</p>
Pre Command	<p>Optionally, specify the full path of a command script to run before the scheduled reclaim occurs.</p>
Post Command	<p>Optionally, specify the full path of a command script to run after the reclaim operation is complete.</p>

6 To specify run days for the schedule, make selections on the following tabs:

Days of Week	<p>Select one or more days on one or more weeks of the month.</p> <p>You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the reclaims to occur on the first occurrence of all the week days for the month.</p>
Days of Month	<p>Select one or more days of the month. You can also check the LastDay checkbox to schedule the reclaim operation for the last day of each month.</p>
Specific Dates	<p>Select one or more specific dates to include in or to exclude from the schedule.</p> <p>Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.</p>

7 Click Next.

8 Click Finish to complete the wizard.

Reclaiming storage space from a thin provisioned disk or from a volume that resides on thin provisioned disks

This section explains how to reclaim storage from a thin provisioned disk or from a volume that resides on thin provisioned disks.

Reclaiming storage space from a thin provisioned disk

This section explains how to reclaim storage from a thin provisioned disk.

To reclaim storage space from a thin provisioned disk

- 1 In the VEA GUI, right-click the disk in the tree view.
- 2 Select Thin Provisioning > Reclaim in the context menu.
- 3 On the Welcome page of the Disk Reclaim Wizard, click Next
- 4 On the Select Disks page, you may add additional disks to the reclaim operation. Click Next to continue.
- 5 Click Finish to complete the wizard.

Using a schedule to reclaim storage space from a thin provisioned disk

- 1 In the VEA GUI, right-click the disk in the tree view.
- 2 Select Thin Provisioning > Schedule Reclaim in the context menu.
- 3 On the Welcome page of the Disk Reclaim Scheduler Wizard, click Next
- 4 On the Select Disks page, you may add additional disks to the reclaim operation. Click Next to continue.
- 5 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	Enter a unique name for the schedule. This name identifies the schedule if you later want to view information about the reclaim status. A default name consists of the ThinReclaim.1, the component name and a numbered suffix that increments with each schedule.
Description of this schedule	Optionally, enter a description to help you identify the schedule when you view information about the reclaim status.
Start Time	The time of the day to begin the reclaim operation.

End Time	The time of day to end the reclaim operation.. If a reclaim operation is in progress it is completed but a new one is not started after the end time.
Schedule takes effect on	The date on which the specified schedule takes effect. The default is the current date.
Restart task every	The interval between reclaim operations, in minutes. For example, if the interval is 360 minutes and you schedule a reclaim start time of 12 P.M. and an end time of 7 P.M, the reclaim operation occurs twice. If no interval is specified the reclaim operation occurs once.
Every	Enable the Every option to have the reclaim schedule continue to occur. Otherwise the schedule applies only for one day. Specify the number of days before restarting the reclaim schedule. For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.
Start On	If you enable the Every option, specify the starting date.
Pre Command	Optionally, specify the full path of a command script to run before the scheduled reclaim occurs.
Post Command	Optionally, specify the full path of a command script to run after the reclaim operation is complete.

6 To specify run days for the schedule, make selections on the following tabs:

Days of Week	Select one or more days on one or more weeks of the month. You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the reclaims to occur on the first occurrence of all the week days for the month.
Days of Month	Select one or more days of the month. You can also check the LastDay checkbox to schedule the reclaim operation for the last day of each month.

Specific Dates Select one or more specific dates to include in or to exclude from the schedule.

Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.

- 7 Click Next.
- 8 Click Finish to complete the wizard.

Reclaiming storage space from a volume that resides on thin provisioned disks

This section explains how to reclaim storage from a volume that resides on thin provisioned disks.

To reclaim storage space from a volume that resides on thin provisioned disks

- 1 In the VEA GUI, right-click the volume in the tree view.
- 2 Select Thin Provisioning > Reclaim in the context menu.
- 3 On the Welcome page of the Volume Reclaim Wizard, click Next
- 4 On the Select Volumes page, you may add additional volumes to the reclaim operation. Click Next to continue.
- 5 Click Finish to complete the wizard.

Using a schedule to reclaim storage space from a volume that resides on thin provisioned disks

- 1 In the VEA GUI, right-click the volume in the tree view.
- 2 Select Thin Provisioning > Schedule Reclaim in the context menu.
- 3 On the Welcome page of the Volume Reclaim Scheduler Wizard, click Next
- 4 On the Select Volumes page, you may add additional volumes to the reclaim operation. Click Next to continue.
- 5 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	<p>Enter a unique name for the schedule.</p> <p>This name identifies the schedule if you later want to view information about the reclaim status. A default name consists of the ThinReclaim.1, the component name and a numbered suffix that increments with each schedule.</p>
Description of this schedule	<p>Optionally, enter a description to help you identify the schedule when you view information about the reclaim status.</p>
Start Time	<p>The time of the day to begin the reclaim operation.</p>
End Time	<p>The time of day to end the reclaim operation.</p> <p>If a reclaim operation is in progress it is completed but a new one is not started after the end time.</p>
Schedule takes effect on	<p>The date on which the specified schedule takes effect. The default is the current date.</p>
Restart task every	<p>The interval between reclaim operations, in minutes.</p> <p>For example, if the interval is 360 minutes and you schedule a reclaim start time of 12 P.M. and an end time of 7 P.M., the reclaim operation occurs twice. If no interval is specified the reclaim operation occurs once.</p>
Every	<p>Enable the Every option to have the reclaim schedule continue to occur. Otherwise the schedule applies only for one day.</p> <p>Specify the number of days before restarting the reclaim schedule.</p> <p>For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.</p>
Start On	<p>If you enable the Every option, specify the starting date.</p>
Pre Command	<p>Optionally, specify the full path of a command script to run before the scheduled reclaim occurs.</p>
Post Command	<p>Optionally, specify the full path of a command script to run after the reclaim operation is complete.</p>

6 To specify run days for the schedule, make selections on the following tabs:

Days of Week	<p>Select one or more days on one or more weeks of the month.</p> <p>You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.</p>
Days of Month	<p>Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.</p>
Specific Dates	<p>Select one or more specific dates to include in or to exclude from the schedule.</p> <p>Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.</p>

- 7 Click Next.
- 8 Click Finish to complete the wizard.

Canceling a reclaim operation

Canceling a reclaim operation can be done for disk groups, disks, or volumes.

To cancel a reclaim operation for a disk group

- 1 In the VEA GUI, right-click the disk in the tree view.
- 2 Select Thin Provisioning > Cancel Reclaim in the context menu.
- 3 Select a reclaim type and click Next.
- 4 In the confirmation dialog box, click Yes to confirm canceling the reclaim operation.

To cancel a reclaim operation for a disk

- 1 In the VEA GUI, right-click the disk in the tree view.
- 2 Select Thin Provisioning > Cancel Reclaim in the context menu.
- 3 In the confirmation dialog box, click Yes to confirm canceling the reclaim operation.

To cancel a reclaim operation for a volume

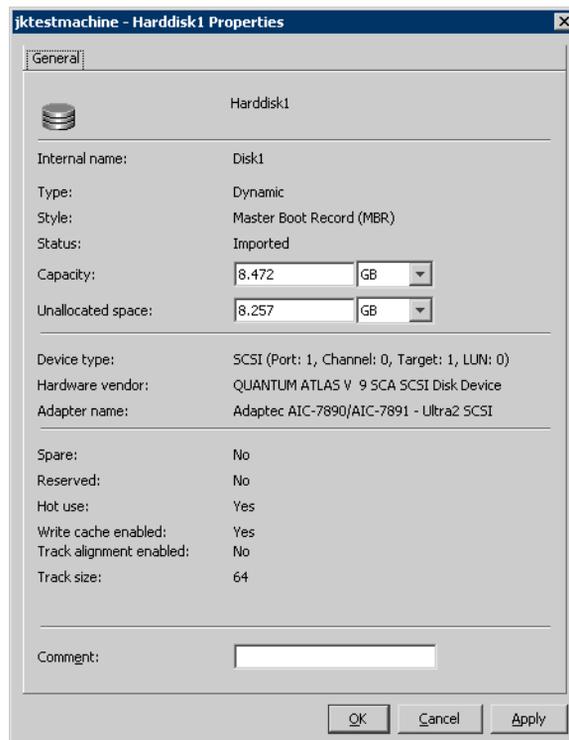
- 1 In the VEA GUI, right-click the volume in the tree view.
- 2 Select Thin Provisioning > Cancel Reclaim in the context menu.
- 3 In the confirmation dialog box, click Yes to confirm canceling the reclaim operation.

View disk properties

To check the properties of a disk:

- 1 Right-click the disk to be checked.
- 2 Select **Properties** from the context menu that appears.

The Properties window appears. The categories for the properties of a disk can differ, depending on whether the disk is basic or dynamic and whether it is directed or part of an array. The screen that follows shows an example of a Properties window for a dynamic disk.



The categories in the sample screen are described in the table that follows.

Table 4-1 Disk Properties Categories

Category	Description
Internal Name	The name of the hard disk is shown at the top of the window.
Type	Fields are Basic and Dynamic.
Style	Refers to a partition style. The two categories are Master Boot Record (MBR) and GUID Partition Table (GPT). Master Boot Record (MBR) refers to the Windows partition style that is limited to 4 primary partitions. It is available on MS-DOS, Windows 95/98, and later versions of Windows. The GPT style allows you to create 128 primary partitions. GPT is available on Windows Server 2003 and later 64-bit systems and on Windows 2003 SP1 and later 32-bit systems.
Status	Fields are Imported and Deleted.
Capacity	Size in Sectors, KB, MB, GB, TB.
Unallocated space	Amount of free space that is available to create a partition or volume.
Thin Type	Indicates the type of thin provisioned disk , Thin or Thin Reclaim. Note: For thin provisioned disks only.
Provisioned size	Current amount of storage allocated to the disk that supports thin provisioning. Note: For Thin Reclaim provisioned disks only. Not all disks that are enabled for thin provisioning provide the provisioned size value.
Allocation unit size	Minimum amount of storage that is added to a thin provisioned disk to meet current storage requirements. Note: For Thin Reclaim provisioned disks only.
Device type	The Device type category includes SCSI, Fibre, and some other less commonly used types. If a controller card is involved, gives port, channel, target, and LUN information.
Hardware vendor	Vendor information from the disk itself.
Adapter name	Gives information on the host bus adapter.

Table 4-1 Disk Properties Categories

Category	Description
Spare	Indicates whether the disk is a preferred hot relocation target.
Reserved	Indicates whether the disk is reserved—that is, excluded from use in automatic selection operations.
Hot use	Indicates whether the disk can be used to receive volumes from the hot relocation procedure.
Write cache enabled	Indicates whether the write cache is enabled.
Track alignment enabled	Indicates whether the disk is enabled for track alignment.
Track size	Indicates the size of a track on the disk.
Comment	User defined comment.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support disk comments.

You can also view disk characteristics through the Disk View in the GUI and through the GUI's right-pane view.
See "[The disk view](#)" on page 103.

General Partition/Volume tasks

This section on general partition or volume tasks has the following topics:

- [Delete a volume](#)
- [Delete a partition or logical drive](#)
- [Shredding a volume](#)
- [Refresh drive letter, file system, and partition or volume information](#)
- [Add, change, or remove a drive letter or path](#)
- [Renaming a mirror \(plex\)](#)
- [Changing the internal name of a volume](#)
- [Mount a volume at an empty folder \(Drive path\)](#)
- [Format a partition or volume with the file system command](#)
- [Cancel format](#)
- [Change file system options on a partition or volume](#)
- [Set a volume to read only](#)
- [Check partition or volume properties](#)
- [Expand a dynamic volume](#)
- [Expand a partition](#)
- [Shrink a dynamic volume](#)

See also the following related topics:

[“Create dynamic volumes”](#) on page 60.

[“Create primary and extended partitions”](#) on page 184

[“New logical drives”](#) on page 189

[“Subdisk move, split, and join”](#) on page 539.

[“Set up a dynamic boot and system volume \(Optional\)”](#) on page 70.

For troubleshooting volumes, see the following topics:

[“Bring a basic volume back to a healthy state”](#) on page 481

[“Bring a dynamic volume back to a healthy state”](#) on page 481.

Delete a volume

Caution: All data in the volume will be lost when you delete it. Make sure that the information has been backed up onto another storage medium and verified, or that it is no longer needed.

To delete a volume

- 1 Right-click the designated volume and select **Delete Volume**.
- 2 You are prompted for verification. Click **Yes** to delete or **No** to cancel. The volume is removed immediately if you click **Yes**.

Delete a partition or logical drive

Caution: All data in the partition or logical drive will be lost when you delete it. Make sure that the information has been backed up onto another storage medium and verified, or that it is no longer needed.

To delete a primary partition, an extended partition, or a logical drive

- 1 Right-click the partition or logical drive you want to delete and choose the command to delete the partition or logical drive from the context menu.
- 2 You are prompted for verification. Click **Yes** to delete or **No** to cancel. The partition or logical drive is removed immediately if you click **Yes**.
Note that you cannot delete a partition with the system files (the boot volume).

Shredding a volume

Shredding a volume destroys the data stored on a volume by overwriting the volume with a digital pattern. SFW provides the following methods for overwriting the volume.

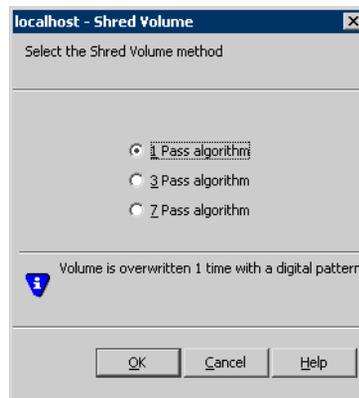
- **1 Pass algorithm**
Overwrites the volume with a pattern of zeroes.
- **3 Pass algorithm**
The volume is overwritten a total of 3 times. The volume is first overwritten with a pre-selected digital pattern, then overwritten with the binary complement of the pattern. In the last pass, the volume is overwritten with a randomly selected digital pattern. This 3 pass approach is based on the specifications in the US Department of Defense standard 5220.22-M (3).
- **7 Pass algorithm**
The volume is overwritten a total of 7 times. Each pass consists of overwriting the volume with a randomly selected digital pattern or with the binary complement of the previous pattern. This 7 pass approach is based on the specifications in the US Department of Defense standard 5200.28-STD (7).

Caution: All data in the volume will be lost when you shred it. Make sure that the information has been backed up onto another storage medium and verified, or that it is no longer needed.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Shred Volume** command.

To shred a volume

- 1 Right-click the designated volume in the VEA GUI and select **Shred Volume**.
- 2 Select the method to shred the volume and click **OK** to continue.



- 3 In the confirmation dialog box, click **Yes** to confirm the operation. The volume is entirely overwritten and removed immediately when the operation has completed.

Refresh drive letter, file system, and partition or volume information

To refresh system information, select **Refresh** from the **Actions** menu. The command refreshes drive letter, file system, volume, and removable-media information on the current computer. It also checks to see whether previously unreadable volumes are now readable. It may not pick up disk changes that occurred since the last reboot or rescan if there was no I/O occurring on the changed disk.

Click the **Tasks** tab in the lower pane to see a progress bar that displays the percentage of completion for the refresh process.

Note: The **Refresh** command is only effective on the StorageAgent node and any of its sub-nodes.

Add, change, or remove a drive letter or path

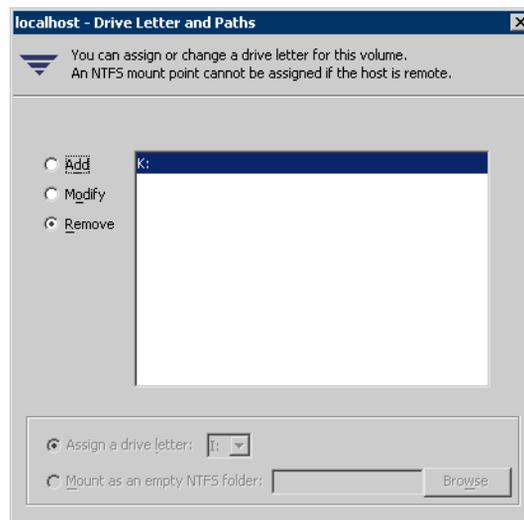
You cannot change the drive letter or path of the active volume (the computer's boot volume). In previous versions of Volume Manager for Windows, the command **Change Drive Letter and Path** was on the context menu for a volume or partition. Now it is a subcommand under the **File System** command that is on the volume or partition context menu.

Caution: Changing the drive letter or path of a partition or volume may cause programs installed on that partition or volume to no longer run.

To add, change, or remove a drive letter or path

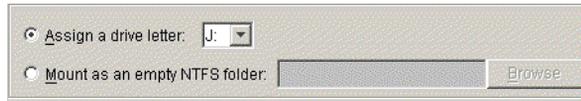
- 1 Right-click the designated partition or volume and on the context menu, select **File System > Change Drive Letter and Path**.

The Drive Letter and Paths screen appears.

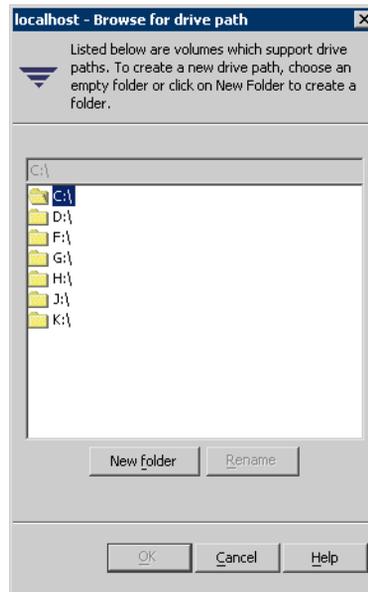


- 2 Select **Add**, **Modify**, or **Remove**, depending on what you want to do.
 - If a partition or volume does not have a drive letter or path, select **Add**.
 - If you want to change an existing drive letter or path, select **Modify**.

- If you want to remove a drive letter or drive path, select **Remove**.
- 3 Select **Add** to add a drive letter or path to a partition or volume.
You can select **Assign a drive letter** or **Mount as an empty NTFS folder**.



- The **Assign a drive letter** option allows you to select a drive letter from the drop-down list. Click **OK** to assign the drive letter after you have made your selection.
- The **Mount as an empty NTFS folder** option allows you to specify the folder. To specify the folder, click the **Browse** button.
The Browse for drive path window appears:



Navigate to an existing folder or create a new folder by using the **New folder** button. Click **OK** to mount the volume.

For details on mounting a volume at an empty folder, see "[Mount a volume at an empty folder \(Drive path\)](#)" on page 170

- 4 Select **Modify** to modify the drive letter. The **Assign a drive letter** box allows you to specify the drive letter. Select a new drive letter from the drop-down list, and click **OK** to assign the drive letter

- 5 Select **Remove** to remove a drive letter. Click **OK** to continue. Click **Yes** in the confirmation screen that appears to complete the operation.
 - If you try to assign a drive letter to a volume that is in use, a dialog box will ask you whether you want to forcibly reassign the drive letter. You can click **Yes** to do so.
 - If you want to modify an existing drive path, you will not be able to do so in this window. You have to remove the drive path and recreate it. Select the **Remove** option. Then you have to invoke the command again to recreate the drive path with the **Add** button.

Renaming a mirror (plex)

You can change the name of a mirror to make it easier to identify.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Rename Plex** command.

To change the name of a mirror

- 1 Expand the Volumes node in the tree view.
- 2 Select the desired volume node that contains the mirror that you want to rename.
- 3 Click the **Mirrors** tab in the right pane of the VEA GUI.
- 4 Right-click the desired mirror and select **Rename Plex** from the context menu.

A dialog box appears to rename the mirror (plex).

- 5 Enter the new name of the mirror (plex).

- 6 Click **OK** to complete the operation.

The name of a mirror (plex) can also be changed with the `vxedit` CLI command. See “[vxedit](#)” on page 385.

Changing the internal name of a volume

You can change the internal name of a volume to make it easier to identify.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support changing the internal name of a volume.

To change the internal name of a volume

- 1 Expand the Volumes node in the tree view.
- 2 Right-click the desired volume node.
- 3 Select **Change Volume Internal Name** from the context menu.
A dialog box appears to rename the volume.
- 4 Enter the new internal name of the volume.
- 5 Click **OK** to complete the operation.

The internal name of a volume can also be changed with the `vxedit` CLI command.

See “[vxedit](#)” on page 385.

Mount a volume at an empty folder (Drive path)

Veritas Storage Foundation for Windows allows you to mount a volume at any empty folder on a local NTFS volume. SFW assigns a drive path to the volume rather than a drive letter. Drive paths are useful because they eliminate the 24-drive-letter limit on hard-disk volume names. (Drive letters A and B are reserved for floppy drives.) The volume can be a partition, a logical drive that was created in Disk Administrator, or a dynamic volume.

For example, you can mount the `C:\Temp` folder as another drive to provide additional disk space for temporary files.

The only restrictions are that the folder you mount the volume to must be empty and it must be on an NTFS volume on a local computer. You cannot mount volumes to network-accessible drives. You can, however, assign multiple drive paths to a single volume.

Mounted drive folders are distinguished from ordinary folders by having a drive icon instead of the normal folder icon.

You can assign the drive path when you create the volume with the New Volume wizard at the Assign Drive Letter screen. You can also use the command **Change Drive Letter and Path** after the volume is created. A volume that already has a drive letter assigned can also have one or more drive paths. It does not have to be an unlabeled volume.

The **Change Drive Letter and Path** command is used to mount a volume.

See “[Add, change, or remove a drive letter or path](#)” on page 167.

See also “[View all drive paths](#)” on page 172.

Unmount a volume

To unmount a volume with a drive path, use the command **Change Drive Letter and Path**, select the drive path, and click **Remove**.

Note: To modify a drive path, remove it and then create a new drive path using the new location. You cannot modify the drive path directly.

View all drive paths

This command lets you view all volumes that have a drive path on a selected server.

To view all mounted volumes

- 1 Right-click the computer icon and select **View All Drive Paths**. In addition, if the computer icon is already selected, you can choose **View All Drive Paths** from the **Actions** menu.
The View All Drive Paths window appears.
- 2 If you want to unmount any volume listed in this window, select the drive path and click **Remove Drive Path**.
You can also use the **Change Drive Letter and Path** command to remove a drive path.
- 3 Click **OK**.
See also “[Mount a volume at an empty folder \(Drive path\)](#)” on page 170.

Format a partition or volume with the file system command

In versions of Volume Manager for Windows before version 3.0, there was a **Format** command for formatting a partition or volume that was available from the partition or volume context menu. Since Volume Manager 3.0, if you want to format a volume after it has been created, you select the command **File System** from the context menu and then choose the subcommand **Replace File System**.

Caution: All data in the partition or volume will be lost when you format it.

To format a partition or volume

- 1 Right-click the volume or partition you want to format, click **File System** from the context menu, and then click the subcommand **Replace File System**.
- 2 Choose NTFS, FAT, or FAT32 as the file system to use.
- 3 Select an allocation size, or use the default, which is automatically selected.
- 4 Enter a label for the volume. This label appears on the VEA console. If a name has been selected, this name appears in this text box, but you can change it here.
- 5 If desired, select the following formatting options:
 - Perform a quick format – Formats the volume or partition without scanning for bad sectors in the volume or partition.

- Enable file and folder compression – Can be used only if you choose NTFS format.
- 6 Click **OK**.
A confirmation screen appears, warning that formatting will erase data.
 - 7 Click **OK** in the confirmation screen to begin formatting.
You can view the percentage of completion for the formatting process in the bottom pane of the console on the **Tasks** tab.

Cancel format

The **Cancel Format** subcommand is a third option from the **File System** menu. This command appears only during the time the file system is being formatted and gives the user the option to cancel the formatting operation.

Change file system options on a partition or volume

When a partition or volume is created, a file system options screen is included with the Create Partition or New Volume wizard. Once the partition or volume is created, you can access the same file system options screen by using the **File System** command and then make desired changes to the options.

To change file system options

- 1 Right-click the partition or volume and choose the commands **File System>Replace File System** from the context menu.
- 2 Once the File System screen appears, change the desired attributes.
You may want to format the partition or volume.
See [“Format a partition or volume with the file system command”](#) on page 172.

Set a volume to read only

Note: Changing a volume from read/write to read only may affect the applications that access the volume.

To set a volume to read only

- 1 Right-click the volume to be set to read only.
- 2 Choose **Properties** from the context menu that appears. The Properties window comes up.
- 3 Check the **Read only** checkbox.
- 4 Click **OK**.

Check partition or volume properties

To check the properties of a partition or volume

- 1 Right-click the partition or volume to be checked.
- 2 Choose **Properties** from the context menu that appears.

The Properties window comes up. The categories for the properties of a volume differ, depending on the volume type. The screen that follows shows the Properties window for a striped volume.



The categories for the striped volume shown in the sample screen are described in the following table:

Table 4-2 Volume Properties Categories

Category	Description
Name	The volume name is shown at the top of the window.
Layout	Indicates volume layout type. The layout categories are concatenated, striped, RAID-5, mirrored, mirrored striped.
Status	Status of the volume.
Copies	Number of mirrors the volume has.
Columns	Number of columns. It will be two or more for striped volumes.

Table 4-2 Volume Properties Categories

Category	Description
Log	Whether there is a DRL or RAID-5 log or FastResync.
Stripe unit width	The amount of data in sectors that is striped across each physical drive in the striped volume.
Group name	Basic or dynamic disk group the volume is associated with.
Device path	The path to the device.
Size	Size of the volume in Sectors, KB, MB, GB, TB.
Comment	User defined comment.
File system type	Fields are FAT, FAT 32, NTFS.
File system label	Operating system file system label.
File system capacity	Size of file system.
File system free space	Amount of free space available in file system.
Aligned	Whether the volume is track aligned or not.
Attributes	Checkbox to enable volume as read only.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support volume comments.

Expand a dynamic volume

The **Expand Volume** command allows you to increase a dynamic volume's size. You can have the program automatically assign destination disks, or you can manually assign these disks.

You can expand a volume only in case of the following:

- the volume is formatted with NTFS or is a raw dynamic volume
and
- there is unallocated space on a dynamic disk within the dynamic disk group onto which the volume can be extended.

You cannot expand a volume if one of the following is true:

- The volume is formatted with FAT or FAT32.
- The volume is set to read only.
- There is not enough unallocated space available on the dynamic disks within the dynamic disk group to extend the volume.

You can extend volumes onto a maximum of 256 disks. No portion of an extended volume can be deleted without deleting the entire volume.

A system or boot volume is extended in increments of the disk's cylinder size and only into contiguous space at the end of the volume.

Note: If a dynamic boot or system volume fails to extend, see [“Cannot extend a dynamic boot or system volume”](#) on page 498.

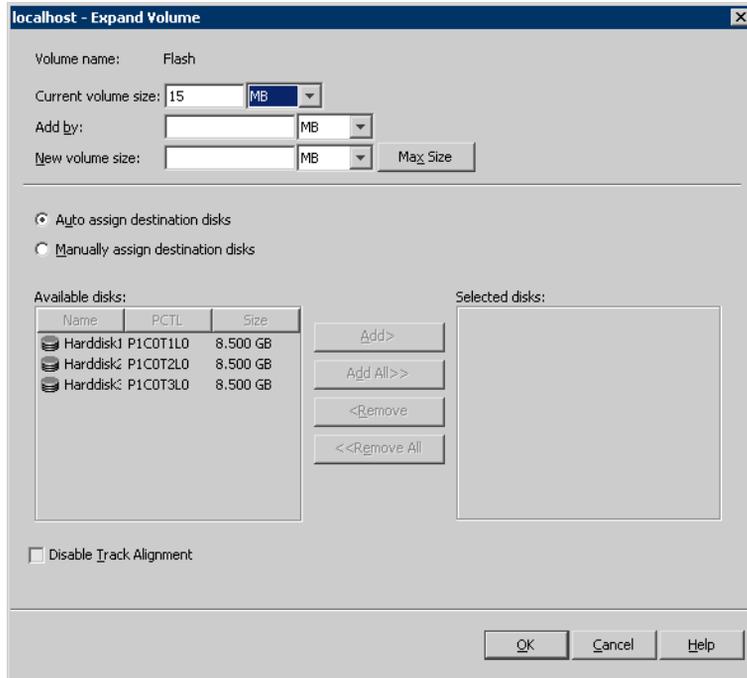
To expand a dynamic volume

- 1 Right-click the dynamic volume you want to expand, highlight **Resize Volume**, and then click **Expand Volume** in the context menu that appears.
- 2 Enter a number in the desired text box.
The options are as follows:
 - The **Add by** option allows you to add a specific amount to the volume by entering a number in the box.
 - The **New volume size** option allows you to specify the total volume size you want.
Clicking the **Max Size** button enters the maximum partition size in the **New volume size** entry box.
The drop-down lists next to the volume size text entry boxes allow you to indicate the size in Sectors, KB, MB, GB, or TB.
- 3 Choose to allow the default **Auto assign destination disks**, or click the **Manually assign destination disks** radio button to assign the disks

manually. To assign the disks manually, use the buttons for adding and removing disks to move the disks you want assigned as destination disks to the right pane of the window.

If desired, check **Disable Track Alignment** to disable track alignment for the volume.

- 4 Click **OK** to complete the command.



Expanding a volume that has a snapshot

If you expand a volume that has a snapshot or detached mirror, then you also need to consider increasing the size of the DCO volume that tracks the changes made to the volume. Increasing the size of the DCO volume allows for a more efficient mirror resynchronization process.

Before expanding the volume, you should perform snap back and snap abort operations on the volume. The snap abort operation should be done with the **Convert into normal mirror** option. This deletes the existing DCO volume and the snap volume becomes the mirror volume with a DCO volume. Right-click the volume and **Select remove log** to remove the DCO volume. After you expand the volume and prepare the volume for a snapshot with the **Select existing mirror for snap** option, a new DCO volume is created automatically at the optimal size for the expanded volume.

For more information about snapshots, see “[Snapshot commands](#)” on page 577.

For more information about DCO volumes, see “[Disk change object \(DCO\) volume](#)” on page 572.

Expand a partition

With SFW, the capability has been added to expand a partition (also known as a basic volume). The command is done online and is similar in concept to the command to expand a dynamic volume.

To expand a partition (basic volume)

- 1 Right-click the basic volume you want to expand, and then click **Expand Partition** in the context menu that appears.
- 2 Enter a number in the desired text box.
The options are as follows:
 - The **Add by** option allows you to add a specific amount to the partition by entering a number in the entry box.
 - The **New Partition size** option allows you to specify the total partition size you want in the entry box.
Clicking the **Max Size** button enters the maximum partition size in the **New Partition size** entry box.
The drop-down lists next to the entry boxes allow you to indicate the size in Sectors, KB, MB, GB, or TB.
- 3 Click **OK** to complete the command.

Shrink a dynamic volume

You can decrease or shrink the size of a dynamic volume using the Shrink Volume command. This command is helpful in reclaiming unused space to better utilize your resource. The Shrink Volume command supports all dynamic volume types which include simple, spanned, striped, mirrored, and RAID-5 volumes.

Note: The shrink volume operation is disabled during a reclaim storage operation for thin provisioned disks. The shrink volume operation is enabled when the reclaim storage operation has completed.

About Shrink Volume

The Shrink Volume command allows you to decrease a dynamic volume's size. The command calculates the amount of space that can be freed from the volume to create a new smaller volume size. The size of a volume after the shrink volume operation is approximately the difference of the current volume size and the amount of unused space, plus a small amount of unused space. This extra amount of unused space is approximately 15% of the new volume size and is

added to the new volume to enable defragmentation. The new volume size is displayed in the VEA GUI.

During the shrink volume operation, data may be relocated on the volume so that the volume can be made into the smaller specified size.

The shrink volume operation can be stopped before it completes. However, the size of the volume as a result of being cancelled can range from the original size of the volume to the specified smaller volume size. The file system on the volume is preserved even though the shrink volume operation was cancelled.

Other important points about shrinking a dynamic volume are as follows:

- You can shrink a volume only if the dynamic volume is either unformatted (RAW) or an NTFS volume.
- The volume must be offline, that is, no application is using the volume.
- Shrink Volume does not support NTFS volumes that are greater than 2TB.
- Shrink Volume does not support basic disks.
- Shrink Volume cannot be performed on a snapshotted volume. To shrink a volume that has been snapshotted, you must first snapback the volume and then shrink the volume. After shrinking a volume, you can snapshot the volume again.
- After shrinking a volume, you may be able to shrink the volume again by a small amount. This is due to changes in the size of the system files contained on the volume.

Shrinking a dynamic volume

Follow the steps below to shrink a dynamic volume.

To shrink a dynamic volume

- 1 Right-click the dynamic volume you want to shrink, highlight **Resize Volume**, and then click **Shrink** in the context menu that appears.
- 2 Enter a number in the **Shrink by** entry box, **New volume size** entry box, or click the **Max Shrink** button.

The options offer the following:

- The **Shrink by** entry box allows you to specify an amount to decrease the volume.
- The **New volume size** entry box allows you to specify the new size of the volume.
- The **Max Shrink** button allows you to decrease the volume by the maximum amount possible.

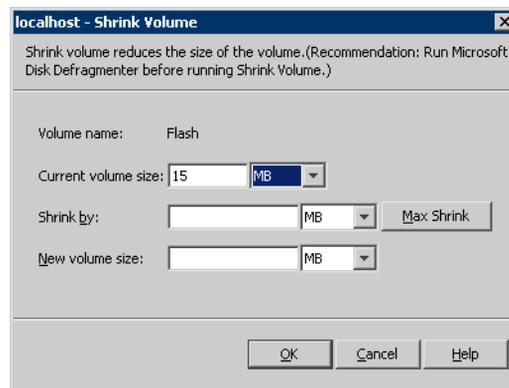
The drop-down lists next to the entry box allow you to indicate the amount in Sectors, KB, MB, GB, or TB.

After entering a value in the **Shrink by** entry box or clicking the **Max Shrink** button, the volume size that results from the Shrink Volume command is calculated and displayed in the **New volume size** entry box.

Click **OK** to continue.

Note: Using the **Max Shrink** button with RAID-5 volumes may not yield optimal results due to the configuration of disks supporting the volume.

- 3 Click **OK** to confirm the settings and complete the command.



Canceling the shrink volume operation

Follow the steps below to cancel the shrink volume operation.

To cancel the shrink volume operation

- 1 Right-click the dynamic volume you want to cancel the shrink volume operation, highlight **Resize Volume**, and then click **Cancel Shrink** in the context menu that appears.
- 2 Click **OK** to confirm the cancellation and complete the command.

Basic disk and volume tasks

This section describes the procedures for working with basic disks and volumes under SFW's control.

The topics are as follows:

- [What can you do with a basic disk?](#)
- [Converting the partition style of a disk](#)
- [Create primary and extended partitions](#)
- [New logical drives](#)
- [Delete a partition or logical drive](#)
- [Mark a partition as active](#)
- [Change a basic disk to dynamic](#)
- [Troubleshoot basic disks and volumes](#)

See also "[Expand a partition](#)" on page 180.

What can you do with a basic disk?

When you first install Veritas Storage Foundation for Windows, all physical disks on your system are defined as basic. You can then upgrade them to dynamic disks.

In general, a basic disk is managed with the Master Boot Record (MBR) or GUID Partition Table (GPT) partitioning scheme and may have partitions defined on it, but this is not required. The MBR style is supported in MS-DOS, Windows 95/98, and later Windows versions. MBR disks can contain up to four primary partitions or three primary partitions plus an extended partition. The extended partition may be further divided into logical drives. The GPT style allows a maximum of 128 primary partitions. It is available on Windows Server 2003 and later 64-bit systems and on Windows Server 2003 SP1 and later 32-bit systems. GPT disks do not support extended partitions.

With the MBR style, you can also create new logical drives that reside in extended partitions. The logical drives are simple volumes that are limited to the space on the extended partitions. They cannot span multiple drives.

Basic disks can also contain RAID volumes that were originally created in Windows NT Disk Administrator, including simple and spanned volumes (volume sets), mirrored volumes (mirror sets), striped volumes (stripe sets), and RAID-5 volumes (stripe sets with parity). These volumes are also called "FT volumes" in Windows NT documentation.

SFW 5.0 and SFW 5.1 do not support FT volumes. Only earlier versions of SFW provide support for FT volumes.

Versions of SFW earlier than SFW 5.0 allow you to maintain and repair these volumes but not to create new ones. Although you cannot create new NT Disk Administrator-type volumes on a basic disk, you can upgrade the existing volumes of this type to dynamic. Then these volumes will have the full capabilities of other SFW dynamic volumes.

Converting the partition style of a disk

For Windows Server 2003 and later 64-bit systems and Windows Server 2003 SP1 and later 32-bit systems, the partition style of a disk can be either Master Boot Record style (MBR) or GUID Partition Table style (GPT). You can convert the partition style of a disk if the disk does not contain any data.

To convert the partition style of a disk

- 1 Right-click the basic disk to display the context menu, and select **Convert to MBR Disk**, if you have a GPT disk; or select **Convert to GPT Disk**, if you have an MBR disk.
The convert pop-up window appears.
- 2 Read the information in the pop-up window and click **Yes** to confirm the conversion.

Create primary and extended partitions

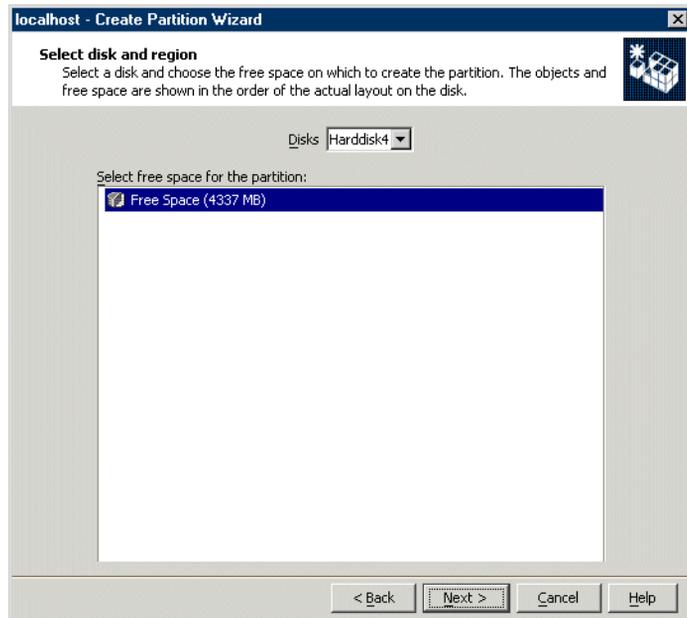
A partition is a portion of a physical disk that functions as if it were a physically separate disk. Partitions can be created only on basic disks. Partitions cannot span disks; they must be contiguous regions. An MBR disk can contain up to four primary partitions or three primary partitions plus an extended partition. The extended partition may be further divided into logical drives. A GPT disk can contain a maximum of 128 primary partitions.

Use the Create Partition wizard to create primary partitions and extended partitions on a basic disk.

To create primary and extended partitions

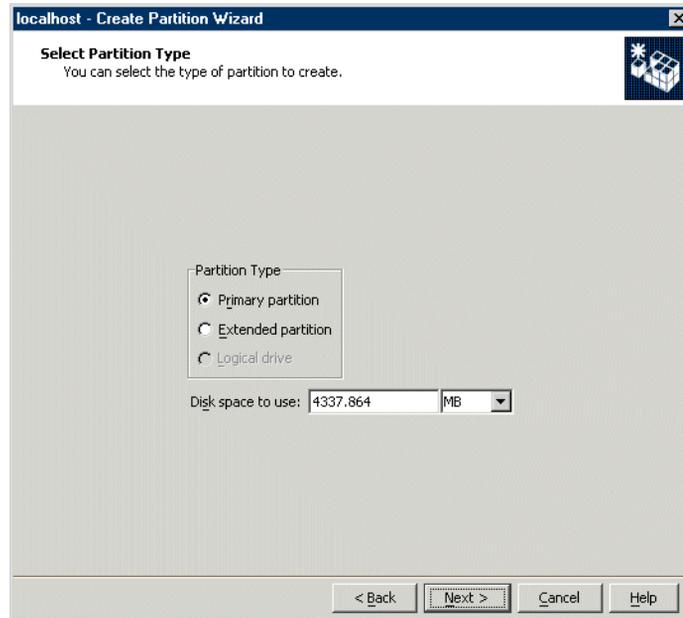
- 1 Right-click a basic disk to display the context menu, and select **New Partition**.
The Create Partition Wizard window appears.
- 2 Read the information on the first screen and then click **Next** to continue.

The Select disk and region window comes up.



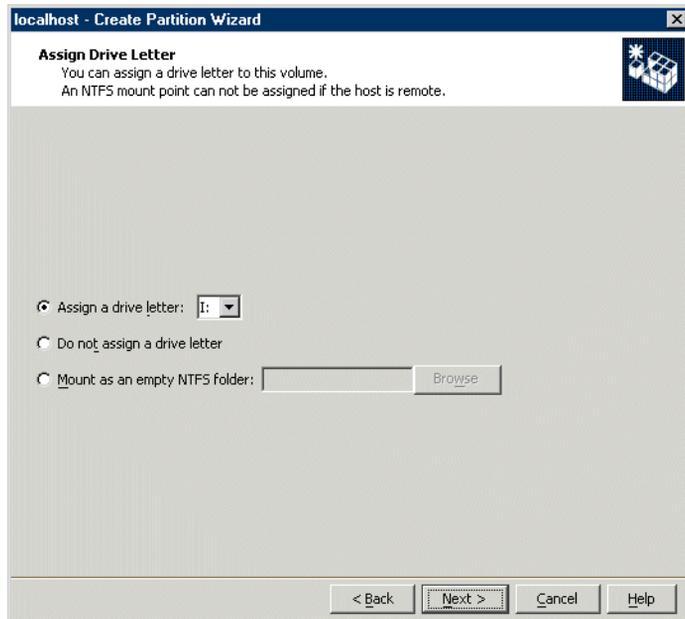
- 3 Select a disk and free space on which to create the partition.
The dialog box shows a list of available disks and free spaces. Check the box for the disk and free space you want to use, and click **Next** to continue. If there is no free space on the selected disk, the free space selection and the **Next** button are grayed out. Click **Cancel** to exit the wizard. If the free space selection is grayed out, you cannot continue. This can occur if the disk already has the maximum number of partitions (either four primary partitions or three primary partitions and one extended partition). It also can happen if the available free space is in an extended partition, because only logical drives (not partitions) can be created there.

The Select Partition Type window comes up next.



- 4 Select a partition type (primary or extended) and indicate the size of the partition. The pull-down list to the right of the entry box for the disk space allows you to select Sectors, KB, MB, GB, or TB. Click **Next** to continue.

The Assign Drive Letter screen comes up next.



- 5 Assign a drive letter or drive path to this volume if you want to format the partition. You can also assign a drive letter after creating the partition. Click **Next** to continue.

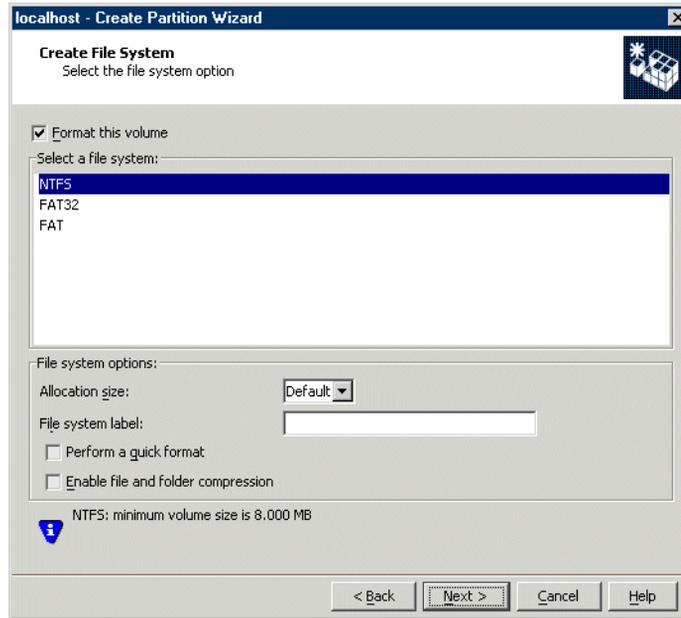
When you mount a local drive at an empty folder on an NTFS volume, the operating system assigns a drive path to the volume rather than a drive letter.

To mount a volume at an empty NTFS folder, click the radio button **Mount as an empty NTFS folder** and type the path to the empty folder, or click the **Browse** button to locate it.

See "[Mount a volume at an empty folder \(Drive path\)](#)" on page 170.

Note: When creating an extended partition, no additional information is required and the final screen appears. Click **Finish** to complete the operation.

- 6 In the Create File System screen that appears next, select the **Format this volume** checkbox if you want to format the partition using NTFS, FAT, or FAT32.



Each of these options offer the following:

- FAT (File Allocation Table) – A file system used by MS-DOS, Windows 3.x, and Windows 95/98. Later versions of Windows also can use the FAT file system. The operating system maintains a table to keep track of the status of various segments of disk space used for file storage.
 - FAT32 (File Allocation Table) – An enhanced implementation of the FAT file system. FAT32 uses smaller cluster sizes; therefore, disk space is used more efficiently, disk performance is increased, and larger drives are supported.
 - NTFS (NT File System) – An advanced file system designed for use specifically within Microsoft Windows operating systems. Use this format if you want to use file and folder compression. Note that NTFS cannot be used by MS-DOS, Windows 3.x, or Windows 95/98.
- 7 Select an allocation unit size in bytes, if you want to use a size other than the default. Default settings are strongly recommended for general use.
 - 8 To name the partition, type a label in the “File system label” entry box. Give the partition a label that will be helpful to you in identifying it.
 - 9 If desired, select the following formatting options:

- Quick format – Use this method to skip scanning for bad sectors in the partition during formatting.
 - Enable file and folder compression – Use this method to compress the folders and files that are added to the volume. This option is available only if the partition is being formatted with NTFS.
- 10 Click **Next** to continue.
The final screen displays the properties of the partition.
 - 11 Click **Finish** in the final screen.
You can view the percentage of completion for the formatting process in the bottom pane of the console, but the **Tasks** tab must be selected.

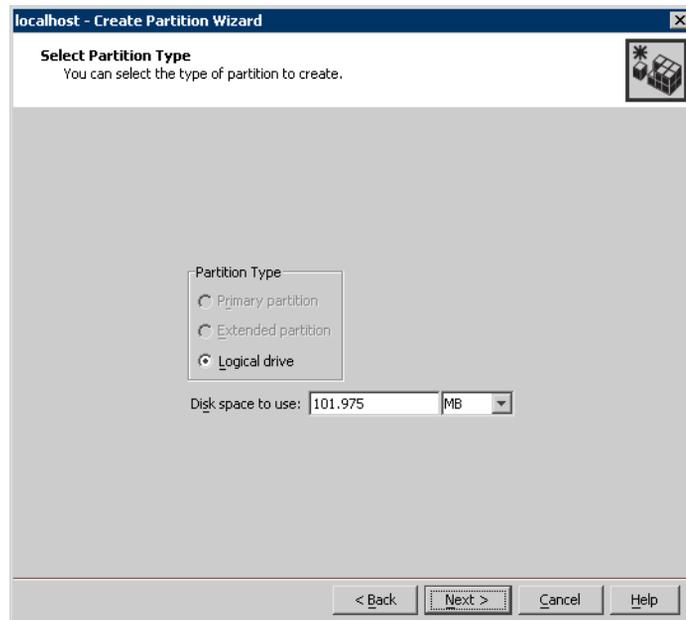
New logical drives

An extended partition can be subdivided into as many as 32 logical drives. You can use all or part of the free space in an extended partition when creating logical drives. An extended partition or a logical drive cannot span multiple disks.

To create a new logical drive

- 1 Right-click an extended partition from the left panel tree view, or click the **Disk View** tab in the right pane and right-click the extended partition in that view.
- 2 In the context menu that appears, click **New Logical Drive**.
The initial screen of the Create Partition wizard appears. Click **Next**.
- 3 Click the **Free Space** checkbox to select the free space to use for that logical drive. Click **Next**.
- 4 Click **Next** to move through the wizard's Select disk and region screen.
The Select Partition Type screen appears. The **Logical drive** radio button is automatically selected, and the screen displays the largest logical drive size that can be created in the extended partition.

- 5 If desired, change the size of the disk space to use, or accept it as shown.



- 6 Type the size of the logical drive that you want to create, and then click **Next**.
The Assign Drive Letter screen appears.
- 7 Choose a drive letter, mount point, or neither (a drive letter can be assigned later). Click **Next** to continue.
The Create File System screen comes up next.
- 8 Select the file system type and options, and then click **Next** to continue.
- 9 Review your selections and click **Finish** to complete the process.

Note that you cannot mark a logical drive as active. An active volume or partition is the volume or partition from which the computer starts up.

Mark a partition as active

The **Mark Partition Active** command lets you designate a basic primary partition as active. An active partition is the partition from which the computer starts up. The system partition or volume must be a primary partition that has been marked as active for startup purposes and must be located on a disk that the computer accesses when starting up the system. There can be only one active system partition at a time, which displays as **Active** in the status field.

The **Mark Partition Active** command can be used only on a basic primary partition, not on a dynamic volume.

The names commonly used for partitions or volumes containing the startup and operating system files are the *system volume* and *boot volume*, respectively. The system volume refers to the partition or volume containing the startup files. The boot volume is a partition or volume that contains the operating system files. The boot volume can be (but does not have to be) the same as the system volume. The boot volume also cannot be part of a spanned, striped, or RAID-5 volume.

To mark a basic volume as the active volume

- 1 Select the primary partition that contains the startup files for the operating system that you want to activate.
- 2 Right-click to display the partition's context menu, and click **Mark Partition Active** on that menu.
A message appears, advising you that the partition will be started when you reboot your computer.
- 3 Click **Yes** to proceed.

Change a basic disk to dynamic

To change a basic disk to dynamic, you need to create a dynamic disk group first with the **New Dynamic Disk Group** or **Add Disk to Dynamic Disk Group** command. When you do create a dynamic disk group, you are able to specify basic disks for the group that become dynamic through the command. If you want to add more disks later, you use the **Add Disk to Dynamic Disk Group** command.

See “[Create dynamic disk groups](#)” on page 53.

See “[Add a disk to a dynamic disk group](#)” on page 141.

Troubleshoot basic disks and volumes

The following topics are helpful in troubleshooting basic disks and volumes:

- [Bring a basic disk back to an online state.](#)
- [Bring a basic volume back to a healthy state.](#)
- [Starting and stopping the Veritas Storage Foundation for Windows Service](#)

Dealing with disk groups

- [About disk groups](#)
- [Delete a dynamic disk group](#)
- [Upgrade a dynamic disk group version](#)
- [Importing a dynamic disk group to a cluster disk group](#)
- [Rename a dynamic disk group](#)
- [Importing and deporting dynamic disk groups](#)
- [Partitioned shared storage with private dynamic disk group protection](#)
- [Dynamic disk group properties](#)
- [Troubleshooting problems with dynamic disk groups](#)

About disk groups

Veritas Storage Foundation for Windows organizes disks into disk groups. Disk groups provide a way of organizing disks and simplifying storage management for systems with large numbers of disks. They also allow you to move disks between computers so that you can easily transfer the storage between computers.

Topics in this section are as follows:

- [Basic and dynamic disk groups](#)
- [Moving dynamic disk groups between computers](#)
- [Primary and secondary dynamic disk groups](#)
- [Cluster disks and cluster dynamic disk groups](#)
- [Private dynamic disk group protection](#)

See also the following related topics:

[“Create dynamic disk groups”](#) on page 53

[“About dynamic disk group split and join”](#) on page 597.

Basic and dynamic disk groups

Veritas Storage Foundation for Windows assigns one group for all basic disks, called the *Basic disk group*. Dynamic disks, however, can have multiple disk groups, which are called *dynamic disk groups*. Disks within a dynamic disk group share a common configuration. Dynamic volumes are created within a dynamic disk group and are restricted to using disks within that group.

When SFW is run for the first time on a server, all disks are in the Basic disk group. In order to upgrade basic disks to dynamic, one or more dynamic disk groups have to be created with the **New Dynamic Disk Group** command.

Moving dynamic disk groups between computers

You can move a dynamic disk group between computers by deporting it on one computer, moving the disk or disks that contain the dynamic disk group to another computer, rescanning on the new computer, and then importing the dynamic disk group. You will be able to use the volumes from the imported dynamic disk group without having to reboot if you have hot-swappable disks.

Before moving the disks in a dynamic disk group, make sure that the disks are online and the volumes are healthy. You should move all disks that are part of the dynamic disk group; otherwise, the volumes will have Degraded status when the disks are moved to the other computer.

Primary and secondary dynamic disk groups

Veritas Storage Foundation for Windows makes a distinction between primary and secondary dynamic disk groups. In the user interface, the primary or secondary designation is shown in parentheses after each dynamic disk group name.

For versions of the program before Volume Manager 3.0, the first dynamic disk group that was created or imported became the primary dynamic disk group. Any remaining disk groups were secondary dynamic disk groups. In Volume Manager 3.0 and 3.1, the primary dynamic disk group is the disk group that contains the computer's boot or system disk. Thus, in Volume Manager 3.0 and 3.1, if you have not included the computer's boot or system disk in any dynamic disk group, you will not have a primary dynamic disk group. The only exception is a primary dynamic disk group that was originally created in Windows 2000 Disk Management or an earlier version of Volume Manager and then the software for the storage that contained that disk group was upgraded to Volume Manager 3.0 or 3.1. In that situation, SFW will retain the primary dynamic disk group label on this disk group. A primary disk group upgraded from Disk Management or an earlier version of Volume Manager for Windows software does not have to contain a boot or system disk.

In Veritas Storage Foundation for Windows and all versions of Volume Manager for Windows, only one primary dynamic disk group can exist on a single host computer. Additional groups that are created or imported on that computer are secondary dynamic disk groups.

Note: A primary disk group upgraded from Microsoft Disk Management with SFW running on Windows Server 2008 always becomes a secondary dynamic disk group.

You might wonder what happens in later releases of Volume Manager or SFW if you have a primary dynamic disk group that was upgraded from Microsoft Disk Management or earlier versions of Volume Manager and that has no boot or system disk and then you create another dynamic disk group that has the computer's boot or system disk. Once this second disk group is created, it becomes the primary dynamic disk group, and the other disk group that was upgraded from the earlier software becomes a secondary dynamic disk group.

The primary dynamic disk group that contains the computer's system or boot disk cannot be deported because doing so would make the computer unbootable.

Note: A primary dynamic disk group should not be renamed.

The concept of importing dynamic disk groups is also used in Veritas Storage Foundation for Windows in connection with a single computer. If a computer is rebooted, SFW makes available or “auto-imports” the primary dynamic disk group and any secondary dynamic disk groups that previously existed on the computer before the reboot, providing these groups have not been deported to another computer.

Cluster disks and cluster dynamic disk groups

Veritas Storage Foundation for Windows has a special category of disk groups for disks involved in supporting Veritas Cluster Server (VCS) and Microsoft Clustering software.

In order for SFW to work with VCS or Microsoft Clustering, you create a cluster dynamic disk group for the disks that are part of the cluster. To create a cluster dynamic disk group, you use the **New Dynamic Disk Group** command and click the **Create Cluster Dynamic Disk Group** checkbox.

For Microsoft Clustering, see “[Create a cluster dynamic disk group](#)” on page 759.

For VCS clusters, see “[Creating cluster dynamic disk groups and volumes](#)” on page 787.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support cluster disk groups.

Private dynamic disk group protection

This feature, which was introduced in Volume Manager 3.0, allows you to partition shared storage on a SAN or shared array for exclusive ownership by a single machine. The storage is partitioned by using a secondary dynamic disk group. Private dynamic disk group protection provides hardware locking to the disks in the secondary dynamic disk group through a SCSI reservation thread.

See “[Partitioned shared storage with private dynamic disk group protection](#)” on page 209.

Note: Microsoft Disk Management Disk Groups do not support private dynamic disk group protection.

Delete a dynamic disk group

Deleting a dynamic disk group can be done two ways. The recommended procedure is a two-part process and is described as follows:

- First, all the volumes in the dynamic disk group must be moved or deleted by using the **Delete Volume** command, then all the disks in the dynamic disk group must be removed from the disk group by using the **Remove Disk from Dynamic Disk Group** command. Once you remove all the disks from a dynamic disk group, the dynamic disk group will automatically be deleted.
- The alternative procedure is to use the **Destroy Dynamic Disk Group** command, which permanently removes the disk group and all its volumes in a one-step process.

Note: All data in a volume will be lost when you delete the volume. Make sure that the information has been transferred elsewhere or that it is no longer needed.

Recommended method for deleting a disk group

To delete a dynamic disk group by using the recommended method

- 1 Delete each volume by right-clicking on the volume in the tree view or in the right-pane Disk View. Select **Delete Volume** from the context menu.
- 2 You are prompted for verification. Click **Yes** to delete the volume.
- 3 Repeat steps 1 and 2 until all volumes in the dynamic disk group have been deleted.
- 4 Right-click on the dynamic disk group to be deleted. Select **Remove Disk from Dynamic Disk Group** from the context menu.
- 5 In the Remove Disk window that appears, use the **Add** or **Add All** button to move all the disks in the dynamic disk group to the **Selected Disks** column in the right pane of the window.
- 6 Click **OK**. The dynamic disk group will be removed from the tree view automatically.

Alternative method for deleting a disk group

The alternative method for deleting a disk group is to use the **Destroy Dynamic Disk Group** command. Because this command permanently removes the disk group and all its volumes, please use caution in implementing this command.

Note: Microsoft Disk Management Disk Groups do not support the **Destroy Dynamic Disk Group** command.

Caution: This command permanently removes all volumes and disks within the disk group.

To delete a dynamic disk group with the alternative method

- 1 Right-click the storage object representing the server being managed (the computer icon at the top of the tree for the server being managed).
- 2 Select **Destroy Dynamic Disk Group** from the context menu.
- 3 Enter the name of the dynamic disk group you want to delete in the dialog box that appears.
- 4 Click **OK**.
A confirmation box appears asking if you are sure you want to destroy the disk group.
- 5 Click **Yes** to delete the dynamic disk group or **No** to cancel the operation.
After the dynamic disk group is destroyed, the disks revert to basic disks and become part of the Basic disk group.

Upgrade a dynamic disk group version

If you have upgraded to Veritas Storage Foundation for Windows from an earlier version of Volume Manager for Windows 2000 or Windows NT or a related program (such as Microsoft Disk Management) and have existing dynamic disk groups that you created on your system, you most likely will want to upgrade those dynamic disk groups so that they are compatible with the dynamic disk group capabilities of Veritas Storage Foundation for Windows.

If you don't plan to make changes to these existing disk groups, you do not have to upgrade them; upgrading them allows you to use additional features that affect a disk group, such as SFW's support for VSS, the Volume Shadow Copy Service feature available in Windows Server 2003 and later Windows releases. SFW incorporates VSS support into FlashSnap. If you plan to use the FlashSnap option with these existing disk groups, then you should upgrade them to the current disk group version.

Note: If you upgrade a disk group to SFW, you will not be able to import it on another server that is running Volume Manager 3.1 or any earlier version of Volume Manager or Microsoft Disk Management. Once a disk group version is upgraded, it cannot be changed back to an earlier disk group version.

Note: Microsoft Disk Management Disk Groups do not support upgrading the disk group version.

Note that in earlier versions of Volume Manager for Windows 2000 or Windows NT, it was possible to have a dynamic disk group name longer than the 18-character limit that was put into effect with Volume Manager 3.0. If you upgrade the dynamic group version of such a disk group, you will be asked to shorten the name. It is possible that you will be asked to shorten the name to fewer than 18 characters if the disk group's volumes also have very long names.

You can also use the command line to upgrade a disk group to the current SFW disk group version. The command line has the additional capability of upgrading a disk group created in Microsoft Disk Management or Volume Manager releases earlier than Volume Manager 3.0 to the disk group version used in SFW.

See "[vxdg upgrade](#)" on page 312.

To upgrade a dynamic disk group version:

- 1 In the tree view, right-click the disk group you want to upgrade and select **Upgrade Dynamic Disk Group Version** from the disk group context menu. A confirmation screen appears with the text "Are you sure you want to upgrade the dynamic disk group?"

- 2 Click **Yes** to upgrade the dynamic disk group.

Importing a dynamic disk group to a cluster disk group

Importing a dynamic disk group as a cluster disk group can be done by using the **Import as cluster disk group** option of the **Import Dynamic Disk Group** command. This conversion to a cluster disk group requires that the dynamic disk group be connected to a shared bus.

See also “[Import a dynamic disk group](#)” on page 207.

Note: Microsoft Disk Management Disk Groups do not support the **Import Dynamic Disk Group** command.

To import a dynamic disk group to a cluster disk group

- 1 In the tree view, right-click the disk name in the dynamic disk group or the dynamic disk group name in the tree view and select **Import Dynamic Disk Group**.
- 2 Select the **Import as cluster disk group** option to import the dynamic disk group as a cluster disk group.

Rename a dynamic disk group

Note: You should not rename a primary dynamic disk group if it contains the boot or system volume.

Note: Microsoft Disk Management Disk Groups do not support the **Rename Dynamic Disk Group** command.

To rename a dynamic disk group

- 1 In the tree view, right-click the disk group and select the command **Rename Dynamic Disk Group** from the context menu.
- 2 The Rename Dynamic Disk Group dialog box comes up. Type the new name in the **New Name** text entry box, and click **OK**.
The dynamic disk group name is limited to 18 characters. It cannot contain spaces or forward and backward slashes. Also, a period cannot be the first character of the name.

Detaching and attaching dynamic disks

Veritas Storage Foundation for Windows supports detaching and attaching disks of dynamic disk groups. This feature allows you to detach dynamic disks for maintenance or other reasons and then attach the dynamic disks when they become available for use. Detached disks are no longer accessible and cannot be operated on until they are reattached.

Detaching and attaching disks using the VEA GUI is described in this section.

The topics in this section are:

- [Detaching dynamic disks](#)
- [Attaching dynamic disks](#)

You can also detach and attach a disk using the `vxdisk` CLI command.

See “[vxdisk](#)” on page 329.

Detaching dynamic disks

The **Detach Disk** command stops disk access and disconnects the disks from SFW control.

Note the following:

- The detach disk operation can only be performed on disks that are in the attached state.
- You may detach disks that may or may not contain any data.
- This operation can be used on all the disks in a dynamic disk group, however at least one disk in the dynamic disk group must remain in attach state to maintain the last active configuration or log copy.
- Detaching disks of dynamic disk groups is not recommended for disks that contain system or boot volumes, or disks that contain a page file or quorum resource.

Note: This operation fails the volume if all the plexes of a redundant volume are contained only on the disks specified for the detach operation.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Detach Disk** command.

To detach disks

- 1 Stop all processes using the volumes in the dynamic disk group, including all I/O to files.
If you do not stop the processes using the volumes, there is the possibility that data written to internal buffers may not get written to disk, resulting in data loss. It is also recommended that you back up all data on your volumes before you detach disks.
- 2 Make sure the status of the volumes on the disks is Healthy and the disks are online.
If the status is not Healthy, you should repair the volumes before you detach the disks.
- 3 Right-click on the disk names in a dynamic disk group or the individual disk in the tree view, and select **Detach Disk** from the menu that appears.
A warning message asks if you are sure you want to detach the disks.
- 4 Click **Yes** to detach the disk.
When disks are detached, their redundant volumes are shown as degraded. For non-redundant volumes, the disks are shown as failed.
If a disk is enabled for Hot Relocation and is detached, its subdisks are not hot relocated. Also subdisks cannot be hot relocated from other disks to a disk that has been detached.
- 5 Remove the disks from the system.
You may need to prepare disks for removal in some cases. See your hardware manual for information.

Attaching dynamic disks

The **Attach Disk** command connects the disks and enables access to the disks.

Note the following:

- The attach disk operation can only be performed on disks that are in the detach state.
- You may attach disks that may or may not contain any data.
- When attaching a disk and bringing it online, the disk's volumes should be reactivated and any redundant volumes should be synchronized automatically.
- When an **Attach Disk** command is issued for the disks, the disks come back online and volumes return to the state they were in at the time of the detach (assuming that all the disks in the disk group are present).

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Attach Disk** command.

To attach disks

- 1 Right-click on the disk names in a dynamic disk group or the individual disk in the tree view, and select **Attach Disk** from the menu that appears.
- 2 Click **Yes** to attach the disks.
The **Attach Disk** command automatically resynchronizes the plexes of redundant volumes that are contained on the specified disks. However, non-redundant volumes must be reactivated manually.

Importing and deporting dynamic disk groups

Veritas Storage Foundation for Windows supports deporting and importing of dynamic disk groups. This feature allows you to move disks belonging to a dynamic disk group between computers and make their storage available for use. If you have hot-swappable disks, it is possible to move disks between systems without a system shutdown and reboot.

Note: You must have administrator privileges on the source and destination computers to be able to move Veritas Storage Foundation for Windows storage between computers.

The topics in this section are as follows:

- [Deport a dynamic disk group](#)
- [Import a dynamic disk group](#)

Deport a dynamic disk group

The **Deport Dynamic Disk Group** command stops access to disks. If you are moving hot-swappable disks between computers, it is important to use the **Deport Dynamic Disk Group** command. Using the command ensures that the data has been preserved in a clean state before you move the disks to the other computer. The **Deport Dynamic Disk Group** command also clears the host ID of the computer on which the disk group is located, so that it can be imported on another computer.

Caution: Though it is possible to deport dynamic disk groups containing volumes that are in a Degraded state, this is not recommended. If a disk failed during transport between systems or during the import, it is possible that data would be lost for volumes running in the Degraded state.

Note: Microsoft Disk Management Disk Groups do not support the **Deport Dynamic Disk Group** command.

To deport a dynamic disk group

- 1 Stop all processes using the volumes in the dynamic disk group, including all I/O to files.

If you do not stop volume processes, there is the possibility that data written to internal buffers may not get written to disk, resulting in data

loss. It is also recommended that you back up all data on your volumes before you move disks to another computer.

- 2 Make sure the status of the volumes on the disks is Healthy and the disks are online.
If the status is not Healthy, you should repair the volumes before you move the disks.

- 3 Right-click on a disk name in the dynamic disk group or the dynamic disk group name in the tree view, and select **Deport Dynamic Disk Group** from the menu that appears.
A warning message asks if you are sure you want to deport the disk group.

- 4 Click **Yes** if you wish to deport the dynamic disk group or **No** if you decide not to deport the dynamic disk group.
The process of deporting a dynamic disk group puts the contained disks in the Offline state and all volumes in the Stopped state. This applies only while the dynamic disk group is deported. Once an **Import Dynamic Disk Group** command is issued, disks will come back online and volumes will return to the state they were in at the time of the deport (assuming that all the disks in the disk group are present).

- 5 Remove the disks from the current system.
If the disks are hot swappable, you can move disks between systems without performing a system shutdown. If the drives are NOT hot swappable, it is necessary to shut down and power off the computer to remove or install the drives.

You may need to prepare disks for removal in some cases. See your hardware manual for information.

Be sure to move all the disks that are members of the dynamic disk group at the same time.

Normally, you need to move all the disks in the dynamic disk group to the other computer. The only exception would be if you were moving disks temporarily to another computer to copy one or more of the volumes that resided on some of the disks. In that case, when you import the disks to the other computer, the volumes that are not complete because of missing disks will display a Missing status. If you reactivate the disks and the volumes, the true status of the volumes will appear, such as Failed or Degraded. Once you move the disks back to the original computer, rescan, and reimport the dynamic disk group, all the volumes in the dynamic disk group should come back in a Healthy state. You may need to use the **Merge Foreign Disk** command.

See “[Merge foreign disk command](#)” on page 487.

Note: Veritas Storage Foundation for Windows does not allow you to deport a cluster disk group that is a Microsoft Clustering disk group resource.

Import a dynamic disk group

Note: Normally, you cannot import a dynamic disk group on a computer without having deported it on the computer where the disk group was located previously. However, the **Import Dynamic Disk Group** command has an option to clear the host ID of the previous computer, so that you can do an import operation. This option should be used with caution.

Note: Microsoft Disk Management Disk Groups do not support the **Import Dynamic Disk Group** command.

Once you have deported a dynamic disk group and disconnected the disks from the original machine, do the following to import the dynamic disk group

- 1 Reinstall the hardware in the destination machine.
- 2 If the disks are hot swappable, open the VEA console on the destination machine and issue a **Rescan** command. If the system had to be shut down to install the disks, it will have done a rescan automatically during the reboot. Once the rescan completes or the system reboots, the dynamic disk group and disks should be listed; but the dynamic disk group will be in a Deported state, and the disks will be in the Offline or Foreign state. Occasionally, you may have to rescan a second time to get the disks showing as Offline or Foreign, particularly if you do the first rescan very quickly after installing the disks on the second computer system.
- 3 Right-click on a disk name in the dynamic disk group or the dynamic disk group name in the tree view, and select **Import Dynamic Disk Group** from the menu that appears.
- 4 If you want to change the dynamic disk group's name, type in a new name for the group in the screen that comes up. The dynamic disk group name is limited to 18 characters. It cannot contain spaces or forward and backward slashes. Also, a period cannot be the first character of the name. If the disk group you are importing has a name longer than 18 characters (as was possible in earlier versions of Volume Manager for Windows), you may be asked to shorten the disk group name at this point. It is possible that

you will be asked to shorten the name to fewer than 18 characters if the disk group's volumes also have very long names.

Do not rename a dynamic disk group that contains a system or boot volume. Otherwise an error can occur.

See "[Error that the boot device is inaccessible, bugcheck 7B](#)" on page 504.

On this screen, you may also check **Clear host ID** to clear the host id of the previous computer that had the dynamic disk group.

This screen also allows you to import the dynamic disk group as a cluster disk group. Select **Import as cluster disk group** to import the dynamic disk group as a cluster disk group. Importing the dynamic disk group to a cluster disk group requires that the dynamic disk group be connected to a shared bus.

The **Import as cluster disk group** option is already selected if you are importing a cluster disk group. Select **Import as dynamic disk group** to import the cluster disk group as a dynamic disk group.

- 5 If you have not done a deport command on the computer where the disk group was located previously, click the checkbox to clear the host ID of the other computer.
- 6 Click **OK** to import the dynamic disk group.
If the volumes in the dynamic disk group come up as Failed or Degraded, you need to repair the volumes.
See "[Repair a volume with degraded data after moving disks between computers](#)" on page 482.

Partitioned shared storage with private dynamic disk group protection

Partitioned shared storage with private dynamic disk group protection allows administrators to partition storage and assign exclusive ownership in a SAN or shared disk array. In early releases of Volume Manager for Windows, partitioned shared storage was implemented through cluster disk groups without the use of a cluster application. In later releases of Volume Manager and Veritas Storage Foundation for Windows, the feature of private dynamic disk group protection makes it possible to partition shared storage with a regular dynamic disk group.

Private dynamic disk group protection uses hardware locking techniques to protect secondary dynamic disk groups located on shared storage from access by other hosts connected to the shared storage pool. The hardware locking is implemented by using a SCSI reservation thread to maintain a current reservation for each disk in a protected group.

In later releases of Volume Manager and SFW, partitioned shared storage is available for secondary dynamic disk groups on shared storage. Private dynamic disk group protection can be assigned when a secondary dynamic disk group is created, or it can be added to an existing secondary dynamic disk group. The protection is in place as long as the disk group is imported; and since secondary dynamic disk groups are auto-imported, protected disk groups come online at system startup with a SCSI reservation thread started automatically.

If disks are being added to a dynamic disk group that has a SCSI reservation, they will get a reservation automatically. However, if a new disk group is being created, you must choose to add private group protection to the disk group.

Private dynamic disk group protection can be removed if the disk group no longer needs protection or is being reassigned to another Veritas Storage Foundation for Windows host. If you deport the dynamic disk group and move it to another host, the protection will be removed and you will need to add it back again. Also, if you uninstall Veritas Storage Foundation for Windows and then reinstall it, the group protection will have been removed and you will need to reapply the protection.

Note: Microsoft Disk Management Disk Groups do not support private dynamic disk group protection.

This section on partitioned shared storage with private dynamic disk group protection has the following topics:

- [Create a new dynamic disk group with private dynamic disk group protection](#)

- [Add private dynamic disk group protection to an existing dynamic disk group](#)
- [Remove private dynamic disk group protection from a dynamic disk group](#)

Create a new dynamic disk group with private dynamic disk group protection

The following steps describe how to use the VEA console to partition shared storage using private dynamic disk group protection.

Note: Microsoft Disk Management Disk Groups do not support private dynamic disk group protection.

To use the VEA console to partition shared storage using private dynamic disk group protection

- 1 Identify the set of shared basic disks you want to assign to a particular Veritas Storage Foundation for Windows server.
- 2 Use the VEA console to connect to Veritas Storage Foundation for Windows on that machine.
- 3 In the tree view or the right pane of the VEA console, right-click one of the basic disks you wish to upgrade, and select **New Dynamic Disk Group** from the context menu that comes up.
- 4 The initial screen of the New Dynamic Disk Group wizard appears. Click **Next** to continue.
- 5 The screen for entering the disk group attributes comes up. Do the following:
 - Type a name for the new group in the **Group Name** entry box.
 - Click the **Add private group protection** checkbox.
 - Move each of the basic disks that you want to include in the new disk group from the left pane of the wizard to the right pane by using the **Add** button.
 - Click **Next** to continue.
- 6 Click **Next** to confirm the group of disks to be included in the new dynamic disk group.
- 7 Select **Finish** on the next screen to create the new group.

The icon for the new disk group will include a lock icon superimposed on its lower right quadrant. The disk group Properties display will show that the group is of type “Dynamic(Secondary,Private).”

Using the vxdg init command

It is possible to perform the operation described above by using the following command line command:

```
vxdbg init -g<NewDynamicGroupName> -R <DiskName> ...
```

where <DiskName> is of the form `harddisk0`, `harddisk1`, etc.

Disks added to the group, either through the Add Disk to Dynamic Disk Group wizard or by a Join Dynamic Disk Group operation, will be automatically protected as soon as the add operation is complete. Disks that are removed from the group, using either the Remove Disk from Dynamic Disk Group or Split Dynamic Disk Group operations, will no longer be protected.

Add private dynamic disk group protection to an existing dynamic disk group

Note: Microsoft Disk Management Disk Groups do not support private dynamic disk group protection.

To add private dynamic disk group protection to an existing secondary disk group

- 1 Right-click on the disk group in the tree view of the VEA console. It must be a secondary dynamic disk group.
- 2 Select **Add Private Dynamic Disk Group Protection**.
- 3 A popup confirmation window will appear. Click **Yes**.
The disk group's icon will now include a lock icon superimposed on its lower right quadrant. The disk group properties display will show that the group is of the type `Dynamic(Secondary,Private)`.

Using the vxdg protect command

It is possible to perform the operation described above by using the following CLI command:

```
vxdbg -g<DynamicDiskGroupName> protect
```

Remove private dynamic disk group protection from a dynamic disk group

Note: Microsoft Disk Management Disk Groups do not support private dynamic disk group protection.

To remove private dynamic disk group protection from a disk group

- 1 Right-click on the disk group in the left pane of the VEA GUI.
- 2 Select **Remove Private Dynamic Disk Group Protection**.
- 3 A popup confirmation window will appear. Click **Yes**.
The lock icon previously superimposed on the disk group icon's lower right quadrant is removed. The disk group properties display will show that the group is of type Dynamic(Secondary).

Using the `vxdg` release command

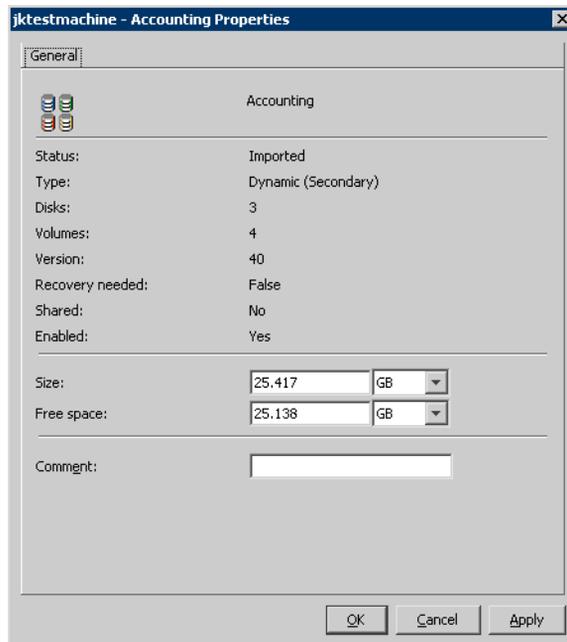
It is possible to perform the operation described above by using the following CLI command:

```
vxdg -g<DynamicDiskGroupName> release
```

Dynamic disk group properties

If you right-click a dynamic disk group object in the tree view and then select the **Properties** command from the context menu that comes up, a Properties window for that dynamic disk group displays. The screen below is an example of the Dynamic Disk Group Properties screen. The status category is either Imported or Deleted. “Current Version” refers to the disk group version that supports advanced disk group features (such as SFW’s support of VSS, the Volume Shadow Copy Service available in Windows Server 2003) that were introduced in SFW 4.0.

Figure 5-1 Disk group properties window



The categories for the Accounting disk group shown in the sample screen are described in the table that follows:

Table 5-1 Dynamic Disk Group Properties Categories

Category	Description
Name	The disk group name is shown at the top of the window and in the title bar.

Table 5-1 Dynamic Disk Group Properties Categories

Category	Description
Status	Fields are Imported and Deported.
Type	Fields are Dynamic (Primary) and Dynamic (Secondary).
Disks	Number of disks in the disk group.
Volumes	Number of volumes in the disk group.
Version	Fields are 20, 30, 40, 43, and 50. See the description of disk group versions below this table.
Recovery needed	Fields are True and False. Indicates whether the disk group has volumes that are degraded.
Shared	Fields are Yes and No. Indicates whether the disk group has private dynamic disk group protection. See “Partitioned shared storage with private dynamic disk group protection” on page 209.
Enabled	Fields are Yes and No. Indicates whether the disk group is functioning or not.
Size	Size of the disk group.
Free space	Free space remaining in the disk group.
Comment	User defined comment.

Note: Microsoft Disk Management Disk Groups do not support disk group comments.

There are five disk group versions:

Version Number	Version Used in:
20	Microsoft Windows Disk Management, Volume Manager for Windows NT, Volume Manager 2.5 and 2.7 for Windows 2000
30	Volume Manager 3.0 and 3.1 for Windows 2000
40	Storage Foundation for Windows 4.0, 4.1, and 4.2
43	Storage Foundation for Windows 4.3
50	Storage Foundation for Windows 5.0 and 5.1

Troubleshooting problems with dynamic disk groups

The following troubleshooting topics in the Troubleshooting chapter are helpful in troubleshooting problems with dynamic disk groups:

- [Repair a volume with degraded data after moving disks between computers](#)
- [A disk is marked as foreign](#)

iSCSI SAN support

- [About iSCSI SANs](#)
- [Configuring an iSCSI SAN with SFW](#)
- [Managing an iSCSI SAN with SFW](#)

About iSCSI SANs

An iSCSI SAN is a storage array network that uses the iSCSI protocol that is built on top of TCP/IP for block level I/O. In an iSCSI SAN the basic unit of data transport is called a protocol data unit (PDU). The PDU is transmitted over a session with one or more TCP/IP connections. Each TCP/IP connection is called a portal and is a member of a portal group.

Data stored in an iSCSI SAN is stored on iSCSI targets. An iSCSI target can be a hardware array or a software iSCSI target node such as Microsoft's iSCSI Software Target. An iSCSI initiator is a server that initiates requests to and receives responses (I/O) from an iSCSI target. An iSCSI session is started when an iSCSI initiator sends a login request to an iSCSI target. The iSCSI target then responds with a login response. To complete the login, a series of key=value pairs are negotiated and agreed upon. Logins can be made persistent so that the associated storage is available to the iSCSI initiator following a reboot.

Challenge Handshake Authentication Protocol (CHAP) and Internet Protocol Security (IPSec) can be used to make the transmission of commands and data secure in an iSCSI SAN. CHAP can be used with IPSec to ensure an authorized connection between an iSCSI initiator and an iSCSI target.

About iSNS servers

An Internet Storage Name Service (iSNS) Server processes iSNS registrations and queries from iSNS clients. It maintains a database to manage the registrations.

The role of the iSNS Server in an iSCSI SAN is to allow iSCSI initiators and iSCSI targets to register and to query for other registered iSCSI initiators or iSCSI targets.

A Discovery Domain (DD) is a security and management mechanism used by iSNS Servers to administer access and connectivity to iSCSI initiators or iSCSI targets (storage nodes) in an iSCSI SAN.

A Discovery Domain Set (DDS) is a mechanism to store sets of discovery domain mappings in an iSNS database. A discovery domain set may contain one or more discovery domains and a discovery domain can be a member of one or more discovery domain sets. Multiple discovery domain sets may be active at the same time.

For the purpose of query and registration, discovery domains are viewed as containers for storage nodes and portal objects. A discovery domain is active if it is a member of at least one active discovery domain set. Discovery domains that are not members of an enabled discovery domain set are considered disabled. A storage node can be a member of one or more discovery domains. An enabled

discovery domain establishes connectivity among the storage nodes in that discovery domain.

At the storage node level, a discovery domain is used to make iSCSI targets inaccessible to iSCSI initiators that are not members of the discovery domain. When first identified by the iSNS server, the Default DD in an iSCSI SAN contains all storage nodes except ones already assigned to a discovery domain. SFW enables you to register with Microsoft's iSNS service and to manage discovery domains and discovery domain sets.

Configuring an iSCSI SAN with SFW

The SFW VEA GUI provides support for managing an iSCSI SAN.

On an iSCSI initiator node, SFW enables you to define iSCSI target portals, log into and out of iSCSI targets, and view the target portal group configuration. With SFW, you can also connect to and manage iSNS objects on a Microsoft iSNS server. If your server's iSCSI initiator is connected to a Microsoft iSCSI Software Target, you can view the set of LUNs that are accessible to your initiator and assign LUNs on the Target to any of its defined targets from an initiator.

Considering prerequisites

When configuring an iSCSI SAN with SFW, you should consider the following prerequisites and the requirements (minimum) for each as described in the documentation that accompanies them:

- For Windows Server 2003:
 - VDS 1.1 Update.
- For Windows Server 2003 SP2 or Windows Server 2008:
 - VDS 1.1 is included with these versions.
- Microsoft iSCSI initiator 2.06 or above.
- VDS iSCSI Hardware Provider (Microsoft)
(optional; available as part of Windows Storage Server).

Setting up an iSCSI SAN

Setting up an iSCSI SAN requires configuring target portals, setting up the iSCSI targets and iSCSI initiators, configuring the storage, assigning access rights, and registering with an iSNS server.

Setting up the iSCSI targets and configuring the storage should be done according to the instructions of the manufacturer of the storage device.

Setting up the iSCSI initiators requires that iSCSI initiator software be installed on each server to enable them to connect to the iSCSI targets. Optionally, the iSNS server software needs to be installed on a server to allow automatic discovery of the iSCSI targets on the network.

If the iSCSI target you plan to connect to is not displayed in the VEA GUI, under the iSCSI Initiators node, you need to add a target portal for it. This occurs when iSNS is not used or the iSCSI target is not registered with iSNS. This also occurs when there is an iSCSI HBA that is not configured to connect to a particular target.

To assign access rights

- 1 In the tree view of the VEA GUI, click the iSCSI node.
If DHCP has been configured to report iSNS servers, the iSNS server automatically discovers the initiators and targets. Expanding the iSCSI node displays all the available initiators and targets in the network. If DHCP has not been configured, you need to register the initiator with iSNS to display the available initiators and targets.
- 2 Login to the desired targets to make them available to the initiator.

To login to a target and make them available to initiators

- 1 Select a target and select Login from its context menu.
- 2 Check any desired optional login settings. The available login settings are to allow persistent restore of the login or to enable multi-path login.
- 3 To set any security settings, such as CHAP or IPsec, check Advanced Settings to access the security settings dialog.
Make sure that the security settings are compatible with the settings that were set up for the storage device.

Using SFW vxdg latestart for iSCSI

SFW provides for dynamic disk groups that contain iSCSI storage to be available at system start up. SFW automatically does this by configuring the Veritas DG Delayed Import Service (VxDgDI) and issuing the `vxdg latestart` command when a dynamic disk group is created. This automatic configuration of the dynamic disk group is only done on the system where the dynamic disk group is created. SFW also automatically checks the dynamic disk group for persistent login to the iSCSI target where the iSCSI disks are located. If necessary, SFW configures the iSCSI target where the iSCSI disks are located for persistent login.

If this dynamic disk group is moved to another system, you must manually configure the VxDgDI service, issue the `vxdg latestart` command, and set up iSCSI target persistent login (if required) to make the iSCSI storage available at system startup on the new system.

You can do this by making the VxDgDI service dependent on the iSCSI service (MSiSCSI) in the Windows registry and issuing the `vxdg latestart` command. You must also change the VxDgDI service startup type to automatic. This allows SFW access to the iSCSI storage when it becomes available. You must also manually configure the iSCSI target where the iSCSI disks are located for persistent login.

See “[vxdg](#)” on page 302.

In addition to automatically enabling the lateststart feature for dynamic disk groups that are created, SFW automatically maintains or disables the feature as appropriate for the following operations:

- Destroy disk group
- Remove disk from disk group
- Add disk to disk group
- Upgrade dynamic disk group version
- Split disk group
- Join disk group

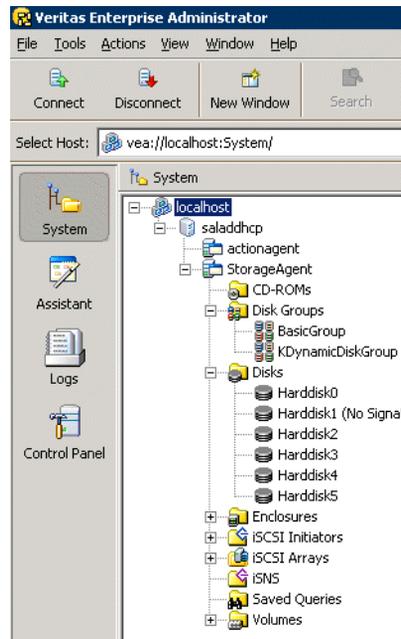
Managing an iSCSI SAN with SFW

SFW allows components of the iSCSI SAN to be accessed and managed with the VEA Console.

Managing with the VEA Console

When an iSCSI SAN has been configured and the Microsoft iSCSI initiator service is installed, SFW displays an iSCSI Initiators node, an iSNS node, and an iSCSI Arrays node in the tree view of the VEA Console.

When managing an iSCSI SAN, you should be already familiar with the usage and settings described in the documentation that accompanies each of the pieces of software that these nodes represent.



About the iSCSI initiators node

Double-clicking the iSCSI Initiators node in the tree-view displays the initiators on the local machine. Selecting one of the nodes enables the display of the initiator adapters, target portals, and the targets for the initiator. These are displayed by clicking the appropriate tab in the right pane. Fully expanding the

iSCSI Initiators node in the tree-view displays the target portals and the targets for each initiator in the tree-view.

Selecting a target portal in the tree view displays information about the target portal in the right pane.

Selecting a target node in the tree view displays information about the target portal groups and the sessions of the target in the right pane. Clicking on the portal groups tab displays details about the portal. Clicking on the sessions tab displays details about the connection between the target and initiator. Fully expanding the target node in the tree-view displays the target portals, LUNs associated with the target, and the target sessions for the target.

The following functions to manage the initiators are available in a context menu for each initiator node:

- Configure iSNS Server
 - Add
 - Remove
- Add Target Portal
- Set Initiator Shared Secret
- Set All IPSec Tunnel Mode Addresses
- Set IPSec Group Preshared Key
- Properties

The following functions to manage the targets portals are available in a context menu for each target portal:

- Remove Target Portal
- Properties

The following functions to manage the targets are available in a context menu for each target node:

- Login To Target
- Logout From Target
- Remove Persistent Login
- Properties

The following functions to manage the sessions are available in a context menu for each session node:

- Add Connection
- Logout
- Properties

Configuring an iSNS server

To register the initiator with an iSNS server, right-click the initiator node and select the Configure iSNS Server to open the dialog box. The dialog box allows you to add or remove the initiator from an iSNS server and to enter the IP address or DNS name of the server.

Adding a target portal

To add a target portal to an initiator, right-click the initiator node, select Target Portal, and select Add to launch the Add Target Portal Wizard. The wizard also allows you to enter the security settings for communicating with the target.

Setting up security for an initiator

You can use the following to set up the security for an initiator:

- Set Initiator Shared Secret
- Set All IPsec Tunnel Mode Addresses
- Set IPsec Group Preshared Key

To access the appropriate dialog box, right-click the initiator node and select the type of security. For enabling persistent login to the target, check **Persist** in the Set All IPsec Tunnel Mode Addresses dialog box.

Removing a target portal

To remove a target portal from an initiator, use the Remove Target Portal dialog box. To access the dialog box, right-click the appropriate target portal node and select Remove Target Portal. Click **Yes** to complete the operation.

Login to a target and setting security

To login to a target, right-click the target node, select Login To Target, to launch the Login to Target Wizard. The wizard also allows you to enter the login settings and security settings for communicating with the target.

The available login settings are to allow persistent login and to enable multi-path login.

Check the Advanced Settings checkbox to open the dialog box for security settings.

The following security settings are available:

- General Settings tab:
 - Initiator Adapter
 - Target Portal
 - CHAP Logon Settings
 - Perform mutual authentication

- CRC/Checksum Data digest and/or Header digest
- IPsec Settings tab:
 - Pre-shared Key
 - IKE protocols
 - ESP protocols
 - Perfect Forward Secrecy

Logout from a target

To logout of a target, use the Logout From Target dialog box. To access the dialog box, right-click the target node and select Logout From Target.

Removing persistent login from a target

Enabling persistent login for a target causes the target to be logged in automatically across system reboots. Removing or disabling persistent login means that manual login to the target is required after a reboot.

To remove the persistent login from a target, use the Remove Persistent Login dialog box. To access the dialog box, right-click the target node and select Remove Persistent Login.

Adding a connection

To add a connection to a session, right-click the session node and select Add Connection to launch the Add Connection window. The window allows you to select initiators and portals to establish the connection.

Note: Not all iSCSI initiators, such as the Microsoft iSCSI Initiator, allow you to add connections.

Logout from a session

To logout of a session, use the Logout dialog box. To access the dialog box, right-click the session node and select Logout.

About multiple sessions

SFW supports multiple sessions to a target. Multiple sessions are used to support fault tolerance for the iSCSI storage using the Microsoft multipath input/output (Microsoft MPIO) solution, and SFW's Veritas Dynamic Multi-pathing option. Installing the DMP Device Specific Module (DMP DSM), VITARGET, and configuring the connections to the sessions, allows you to set up fault tolerance for the iSCSI storage.

See "[Dynamic multi-pathing software](#)" on page 717.

About the iSCSI arrays node

If a VDS iSCSI hardware provider for the storage array is installed on the SFW server, then expanding the iSCSI array node displays the Microsoft iSCSI Software Target subsystem that contain the LUNs and physical disks that make up your iSCSI SAN. The LUNs in a subsystem can be one of the following types shown in the following table.

Table 6-1 Description of LUNs

Icon	Name	Description
	LUN	LUN contained in the subsystem and assigned to this iSCSI initiator.
	Foreign LUN	LUN contained in the subsystem and assigned to another iSCSI initiator.
	Idle LUN	LUN contained in the subsystem, but not assigned to any iSCSI initiator.

Selecting a subsystem displays the tabs that allow you to view lists of the targets, LUNs, or drives in the right pane.

You can view additional information as follows:

- Double-clicking an entry in the list of targets displays the tabs that allow you to view the sessions and the portal groups of the target.
- Double-clicking an entry in the list of LUNs displays the tabs that allow you to view the paths that connect to the physical disk, details of the physical disk, and the targets that the LUN supports.
- Double-clicking an entry in the list of drives displays its details.

Selecting a LUN under the subsystem node displays the tabs that allow you to view the paths that connect to the physical disk, details of the physical disk where the LUN is located on the target server, and targets.

Expanding a LUN in the tree-view that is assigned to the iSCSI initiator, displays the physical disk for the LUN. Selecting the physical disk displays details of the physical disk in the right pane.

To support an SFW Dynamic Multi-pathing (DMP DSMs) environment, the MPIIO option of the Microsoft iSCSI Initiator and the appropriate DSM for the iSCSI target need to be installed. (SFW provides the VITARGET DSM to support Microsoft iSCSI Target.)

In an SFW Dynamic Multi-pathing environment, selecting a physical disk under the subsystem node displays the tabs that allow you to view the volumes, disk regions, disk views, and alerts associated with the physical disk.

The following functions to manage the targets are available in a context menu for each LUN node:

- Assign To Target
- Unassign Target
- Properties

Assign to target

To assign a LUN to a target, right-click the LUN node (under the tree view of the target, under the tree view of the array, or under the LUNs tab when selecting an array), select Assign To Target to launch the Assign LUN To Target Wizard. The wizard allows you to select from a list of available targets.

Unassign target

To unassign a LUN from a target, right-click the LUN node (under the tree view of the target, under the tree view of the array, or under the LUNs tab when selecting an array), select Unassign Target to launch the Unassign LUN From Target Wizard. The wizard allows you to select from a list of assigned targets.

About the iSNS server node

Note: The iSNS server node appears in the tree view after performing the Configure iSNS Server option to register the Microsoft iSCSI initiator with the iSNS server you wish to manage.

Expanding the iSNS server node displays the discovery domains (DD), discovery domain sets (DDS), and the targets and initiators registered with the server.

Generally speaking, discovery domains and discovery domain sets are a way to organize and control access to various initiators and targets. Discovery domains contain a collection of initiators and targets. Discovery domain sets are a collection of discovery domains.

Selecting one of the iSNS server nodes enables the display of discovery domains and discovery domain sets. These are displayed by clicking the appropriate tab in the right pane.

Selecting one of the discovery domain nodes enables the display of the set of targets, initiators, and portal groups assigned to the discovery domain. These are displayed by clicking the appropriate tab in the right pane.

Selecting one of the discovery domain set nodes enables the display of discovery domains for the discovery domain set. These are displayed in the right pane.

The following functions to manage the iSNS servers are available in a context menu for each iSNS server node:

- Login
- Log out
- Create Discovery Domain
- Create Discovery Domain Set

The following functions to manage the discovery domains are available in a context menu for each discovery domain node:

- Add node
- Remove node
- Delete

The following functions to manage the discovery domain sets are available in a context menu for each discovery domain set node:

- Add Discovery Domain
- Remove Discovery Domain
- Delete
- Disable
- Enable

Login to an iSNS server

To view or manage an iSNS server you must first login to the iSNS server. To login to an iSNS server, use the Login to iSNS Server dialog box. To access the dialog box, right-click the iSNS server node and select Login.

Log out of an iSNS server

To log out from an iSNS server, use the Log out from iSNS Server dialog box. To access the dialog box, right-click the iSNS server node and select Log out.

Creating discovery domains

To create a discovery domain, use the Create Discovery Domain dialog box. To access the dialog box, right-click the iSNS server node and select Create Discovery Domain. Select from the available iSCSI nodes to add to the discovery domain.

Creating discovery domain sets

To create a discovery domain set, use the Create Discovery Domain dialog box. To access the dialog box, right-click the iSNS server node and select Create Discovery Domain Set. Select from the available discovery domains to add to the discovery domain set.

Adding nodes to a discovery domain

Adding a node to a discovery domain adds an iSCSI initiator or an iSCSI target to the discovery domain. To add nodes to a discovery domain, use the Add Node dialog box. To access the dialog box, right-click the discovery domain node and select Add Node. Select from the available nodes to add to the discovery domain.

Removing nodes from a discovery domain

Removing a node from a discovery domain removes an iSCSI initiator or an iSCSI target from the discovery domain. To remove nodes from a discovery domain, use the Remove Node dialog box. To access the dialog box, right-click the discovery domain node and select Remove Node. Select from the available nodes to remove from the discovery domain.

Deleting a discovery domain

To delete a discovery domain, use the Delete dialog box. To access the dialog box, right-click the discovery domain set node and select Delete.

Adding discovery domains to a discovery domain set

To add discovery domains to a discovery domain set, use the Add Discovery Domain dialog box. To access the dialog box, right-click the discovery domain set node and select Add Discovery Domain. Select from the available discovery domains to add to the discovery domain set.

Removing discovery domains from a discovery domain set

To remove discovery domains from a discovery domain set, use the Remove Domain dialog box. To access the dialog box, right-click the discovery domain set node and select Remove Discovery Domain. Select from the available discovery domains to remove from the discovery domain set.

Deleting a discovery domain set

To delete a discovery domain set, use the Delete dialog box. To access the dialog box, right-click the discovery domain set node and select Delete.

Disabling a discovery domain set

Disabling a discovery domain set makes all the discovery domains in the discovery domain set not available for discovery by other registered targets and initiators in the iSCSI SAN. To disable a discovery domain set, use the Disable dialog box. To access the dialog box, right-click the discovery domain set node and select Disable.

Enabling a discovery domain set

Enabling a discovery domain set makes all the discovery domains in the discovery domain set available to other registered targets and initiators in the iSCSI SAN. To enable a discovery domain set, use the Enable dialog box. To access the dialog box, right-click the discovery domain set node and select Enable.

Settings for monitoring objects

- [Event monitoring and notification](#)
- [Disk monitoring](#)
- [Capacity monitoring](#)
- [Automatic volume growth](#)
- [SMTP configuration for email notification](#)

Event monitoring and notification

Veritas Storage Foundation for Windows reports storage subsystem events that you can view in the Alert Log. The log can provide information on significant incidents, such as a disk failure. Also, Veritas Storage Foundation for Windows provides event notification by SMTP email, by pager, and through SNMP traps that can be displayed in HP OpenView, IBM Tivoli, and CA Unicenter.

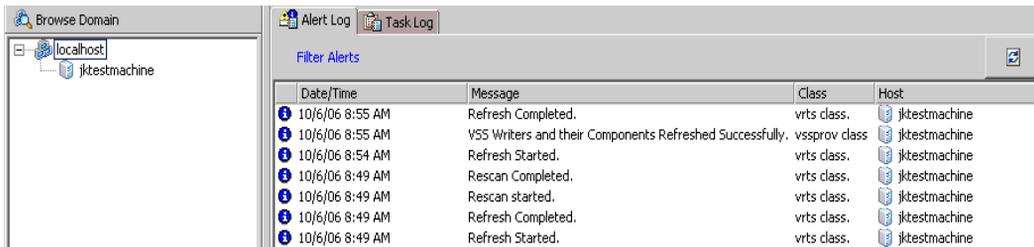
This section covers the following topics:

- [Alert log](#)
- [Severity levels](#)
- [Log configuration](#)
- [Event notification](#)

Alert log

Click the Logs folder in the Logs Perspective to display the Alert Log, a listing of alerts that pertain to the Veritas Storage Foundation for Windows program. For each alert listing, you will see information about the date and time of the message, the message text, and its class.

Figure 7-1 Alert log

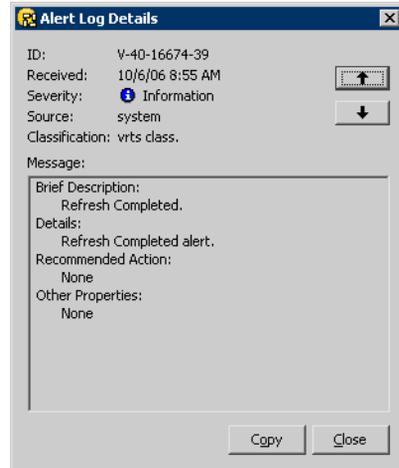


The most recent alert listings can also appear in the new section at the bottom of the VEA Console. This happens when the **Console** tab is selected at the bottom left corner of the VEA Console. If the **Tasks** tab is selected, text appears in the bottom section of the window that gives the progress of system tasks, such as format, refresh, and rescan. These items also appear in the Logs Perspective under the **Task Log** tab.

You can view specific information on each event by double-clicking on it to display the Alert Log Details dialog box. This shows an alert description, recommended action, and properties. The dialog box provides an easier way to

read the description of the event. The arrows that appear at the upper-right corner can be used for scrolling in the alerts listing.

Figure 7-2 Alert log details



Severity levels

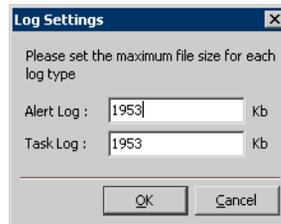
Alerts listed in the Alert Log have the following severity levels:

- **Critical** – Indicates alerts of high importance involving a system crash or unrecoverable data loss.
- **Error** – Indicates a loss of functionality or data.
- **Warning** – Indicates recoverable errors and no data corruption.
- **Information** – Indicates an informational event, such as a new disk has been added to the system.

Log configuration

You can configure the Alert Log and Task Log through the Log Settings dialog box. To access this dialog box, select the Control Panel Perspective, select the host you are connected to, and double-click the **Log Settings** icon in the right-pane. The following dialog box appears:

Figure 7-3 Log settings



In this dialog box, you can enter the maximum log size for each of the logs. You can access the Event Log through the VEA console.

Event notification

Veritas Storage Foundation for Windows provides event notification by SMTP email, by pager, and through SNMP traps that can be displayed in HP OpenView, CA Unicenter, and IBM Tivoli. You can configure the notification service to send messages to specific individuals or groups and also set up rules for filtering the event messages. You can also set up rules that will run a script when specified conditions apply.

This section presents an overview of the Rule Manager utility, which provides the event notification service for Veritas Storage Foundation for Windows. The full details for this utility are given in the online help module titled "Optional Rules for Handling Events." To access the online help, select **Contents** from the SFW **Help** menu.

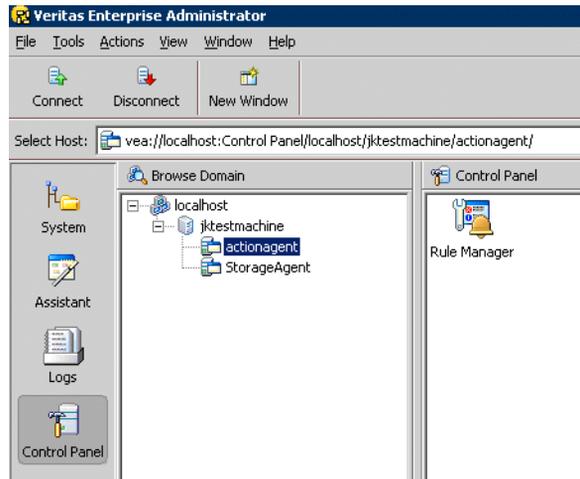
This section covers the following topics:

- [Accessing the Rule Manager utility](#)
- [Preliminary setup](#)
- [Steps for creating rules](#)
- [Accessing the SFW SNMP MIB files](#)

Accessing the Rule Manager utility

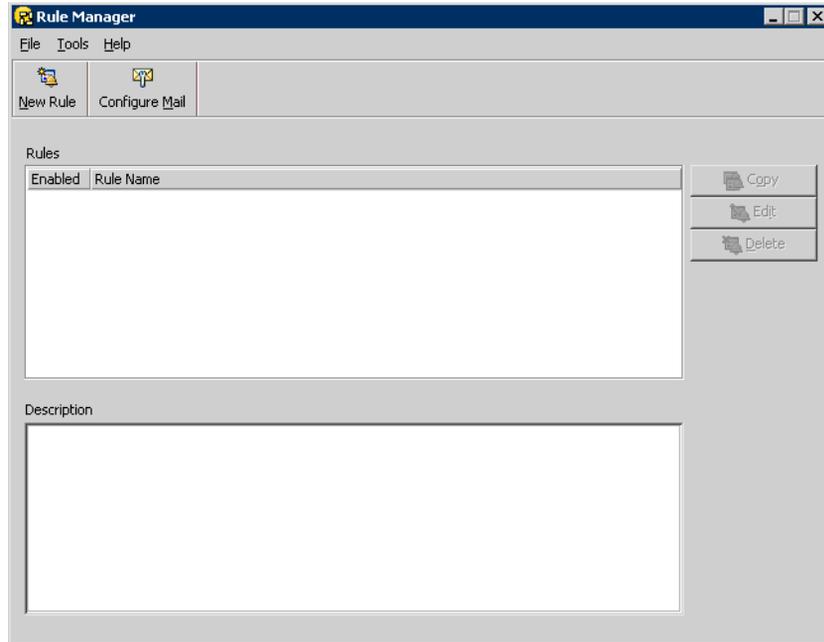
The commands for configuring the service are all accessed through the **Rule Manager** icon. If you click **Control Panel** in the Perspective bar and expand the tree view, the **actionagent** node is displayed. Clicking the **actionagent** node displays the **Rule Manager** icon in the right pane.

Figure 7-4 Rule Manager



Double-click the **Rule Manager** icon to bring up the Rule Manager window. All functions relating to event notification rules are initiated from this window.

Figure 7-5 Rule Manager window



From the Rule Manager, you can create, enable, disable, modify, and delete rules relating to event notification. The **New Rule** button at the top of the window is used to create new rules. The **Configure Mail** button is used to configure settings, such as the settings for the Mail Server, Default Sender, and SMTP Port.

Preliminary setup

Prior to creating rules, you must configure the SMTP mail notification settings you want to use.

Note: Note that this is a one-time setting. After providing this information, you don't need to repeat this step unless the Mail Server changes for your system.

To configure the SMTP mail notification settings

- 1 From the VEA Control Panel perspective, select the **actionagent** node in the tree view.
- 2 Double-click **Rule Manager** in the right pane.

- 3 Click **Configure Mail**.
The Mail Settings window is displayed.
- 4 Provide information about your Mail Server, Default Sender, and SMTP Port. The default SMTP Port is 25.
Check the Enable checkbox and click **OK**.

Steps for creating rules

After the preliminary setup, you create rules for notifications.

To create rules

- 1 From the VEA Control Panel perspective, select the **actionagent** node in the tree view.
- 2 Double-click **Rule Manager** in the right pane.
The Rule Manager window is displayed.
- 3 Click **New Rule** to start the New Rule Wizard.
The New Rule Wizard Welcome appears.
- 4 Review the steps of the wizard and click **Next** to continue.
- 5 On the Rule Properties window, do the following:
 - Enter a name for the rule.
 - Select the type of rule you want to create. Choose one of the following:
 - A rule based on the Alert topic.
 - A rule based on the severity of alerts.
 - Further define your rule by selecting either an Alert topic or a severity level as follows:
 - Enter a topic or click **Select** to select a topic from a list if you chose a rule based on an Alert topic.
 - Select one of the severity levels if you chose a rule based on the severity of the alerts.Click **Next** to continue.
- 6 On the Select host for Rule window, select **Trigger rule for alerts originating from specific hosts** and check the appropriate host in the lower part of the window.
Click **Next** to continue.
- 7 On the Select Actions window configure one or more of the following actions to be taken when the events are detected:
 - Send email notification to recipients.
Enter the email addresses that are to receive notification.

- Send SNMP Trap notification to a host.
Specify the hostname and port number to use to send the notification.
- Execute command on a host.
Specify the name of the host, source host that has the source file (script), path of the source file, and the parameters for the source file. The source file can be of any executable file type, such as .cmd or .bat; and the source file must not be dependant on any libraries. Separate the parameters by spaces or by the delimiter recognized by the source file. In standalone mode, the host and source host identify the same host.
An individual log file is created and maintained for each rule that executes a command on a host. Each time the command is executed entries are made into its log file. The log files are located at C:\Documents and Settings\All Users\Application Data\Veritas\VRTSaa\Log.

Click **Next** to continue.

- 8 On the Finish Rule Setup window, review your settings and check the **Enable Rule** checkbox.
Click **Finish** to complete setting up the rule.

About SNMP traps

If you are planning to send SNMP traps, the MIB files should be loaded and compiled into the management application to which traps will be sent. To accomplish this, do the following:

- Load the product-specific MIB into your SNMP management software database according to instructions provided by your management platform.
See [“Accessing the SFW SNMP MIB files”](#) on page 241.
- If the platform you’re using requires a configuration file, such as `trapd.conf`, you should load that file as well. Consult the user’s guide for the management platform to determine how to map your traps to the platform’s alarm system.
Any configuration files associated with your product are stored in the same location as the MIB files.

Note: For details on creating rules, see the “Optional Rules for Handling Events” online help module. To access this module, select **Contents** from the Help menu.

Accessing the SFW SNMP MIB files

If you want to receive Veritas Storage Foundation for Windows SNMP traps on a management platform (such as HP OpenView), you will need to compile and load the Veritas SNMP MIB files into your management platform, following the procedures outlined in the documentation for your specific platform.

When you install Veritas Storage Foundation for Windows, the Veritas MIB files are installed on a local hard drive along with the Veritas Object Bus files and the SFW installation files. (The Veritas Object Bus is associated with the VEA console and is needed to run Veritas Storage Foundation for Windows.)

The default path to the MIB files directory is as follows.

- For 32-bit servers
C:\Program Files\Veritas\VRTSaa\snmpmibfiles
- For 64-bit servers
C:\Program Files (x86)\Veritas\VRTSaa\snmpmibfiles

The Veritas Storage Foundation for Windows MIB file for the Veritas Object Bus is **VRTS-vm.mib** and can be found in the **snmpmibfiles** directory.

Disk monitoring

Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) is available on many new SCSI disks. S.M.A.R.T. provides a way for disks to self-check certain physical conditions that are useful predictors of disk failure and send an alert when conditions indicate that a failure may occur soon. This allows the system administrator to take preventive action to protect the data on the disk. In order to receive alerts in the Veritas Storage Foundation for Windows Event Log, S.M.A.R.T. monitoring must be enabled for the global configuration and also on each disk you want checked. The default is to have S.M.A.R.T. monitoring disabled.

If S.M.A.R.T. predicts that a failure will occur, an alert is sent to the Event Log. You can also receive event notification by SMTP email, by pager, and through SNMP traps that can be displayed in HP OpenView, IBM Tivoli, and CA Unicenter.

See [“Event notification”](#) on page 236.

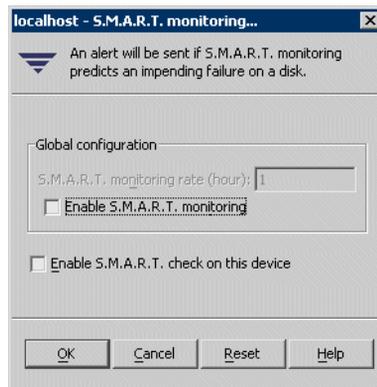
Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support S.M.A.R.T. monitoring.

To enable S.M.A.R.T. monitoring

- 1 Right-click on a disk for which you want to enable S.M.A.R.T. monitoring.
- 2 Select **S.M.A.R.T. Monitoring** from the context menu.

If the **S.M.A.R.T. Monitoring** command on the context menu is grayed out, then the S.M.A.R.T. monitoring technology is not available on that disk.

A S.M.A.R.T. monitoring dialog box will appear as shown below.



- 3 If it is not already checked, check the **Enable S.M.A.R.T. monitoring** checkbox in the global configuration.
The **Enable S.M.A.R.T. monitoring** checkbox acts as an on/off switch for the entire system and allows you to temporarily disable S.M.A.R.T. monitoring if desired.
- 4 Select the rate in hours for S.M.A.R.T. monitoring to occur.
Since this is a global configuration, the monitoring rate will be the same for all disks in the system. The default rate is one hour.
S.M.A.R.T. monitoring will use system resources as it checks the device.
- 5 Check the **Enable S.M.A.R.T. check on this device** checkbox at the bottom of the window to have S.M.A.R.T. monitoring be performed on the specific disk you selected.
- 6 Click **OK**.
- 7 Repeat steps 1, 2, 5, and 6 for each disk you want to monitor.

Capacity monitoring

Capacity monitoring is a feature that monitors the capacity of Veritas Storage Foundation for Windows dynamic volumes so that when the used disk space on a volume reaches a user specified threshold, an alert message is logged.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support capacity monitoring.

You can use SFW's Rule Manager event notification function to set up an email message that is sent when thresholds are reached.

See [“Accessing the Rule Manager utility”](#) on page 237.

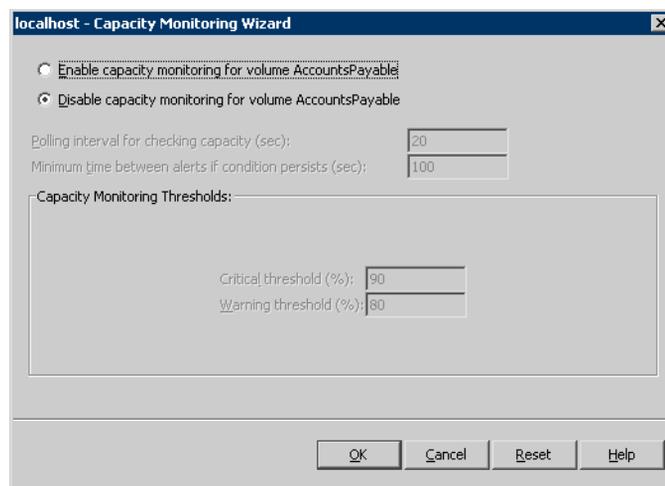
Capacity monitoring is set at the individual volume level and is turned off by default. You will need to enable it for each volume you want to monitor.

The capacity monitoring settings you establish only affect existing volumes. new volumes that are added to a server after any capacity monitoring settings are made have the default capacity monitoring settings applied to them. If the default is not appropriate, you must change the settings for any new volumes that are added.

To enable a volume warning notification

- 1 Right-click on the volume you want to manage and click **Capacity Monitoring**.

The Capacity Monitoring window appears.



- 2 Click **Enable capacity monitoring**.

- 3 Set the capacity monitoring parameters as follows:
 - **Critical threshold**
The percentage of volume capacity that Storage Foundation for Windows reports an error.
The default critical threshold is 90% of capacity.
 - **Warning threshold**
The percentage of volume capacity that Storage Foundation for Windows logs a warning alert message. This is a warning that the volume is reaching full capacity.
The default warning threshold is 80% of capacity.
 - **Polling interval for checking capacity**
The polling interval is the interval of time, in seconds, at which Storage Foundation for Windows checks volume capacities.
The minimum and default value is 20 seconds.
 - **Minimum time between alerts**
To keep the event log file from getting full, you can limit how often an alert message is generated after the warning threshold is reached for a volume.
The default is 100 seconds between messages.
- 4 Click **OK** to enable the settings.

Automatic volume growth

The Automatic Volume Growth feature is a GUI command to have an individual volume grow (increase capacity) automatically by a user specified amount when the used disk space on the volume reaches a certain threshold. This threshold is set in the Capacity Monitoring wizard.

By automating the growth process, the Automatic Volume Growth feature enhances the capability of dynamic volumes to expand without requiring that the underlying disks be off-line.

The advantages of this automatic process include the following:

- Reduced need for a System Administrator to monitor volume capacity at all times.
- Disk space is allocated on an as-needed basis; no idle excess capacity.
- Space will always be available for mission-critical data.

Automatic Volume Growth is set at the individual volume level and is turned off by default. You will need to enable it for each volume you want to grow. Enabling a volume for Automatic Volume Growth requires the volume to be enabled for Capacity Monitoring.

The following gives more information about configuring Automatic Volume Growth in a cluster environment.

See [“Configuring Automatic Volume Growth in a cluster environment”](#) on page 249,

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support Automatic Volume Growth.

A policy file is used to record the settings for the volumes that use the Automatic Volume Growth feature. This XML file is automatically set up when Automatic Volume Growth is enabled, and it reflects the current settings for a volume. You can view and change the current settings with the Automatic Volume Growth wizard. This policy file is also used to record the settings for the VxCache feature.

Alternately, you can use SFW’s Rule Manager event notification function to grow a volume automatically. With Rule Manager, you can set up a script that can grow a volume automatically when a specified threshold is reached.

The current Automatic Volume Growth settings of all your volumes are also available to help you manage your volumes. Right-clicking the Volumes icon in the tree-view of the VEA GUI and selecting Automatic Volume Growth Information in the context menu, displays the growth size, the maximum

growth limit, and if Automatic Volume Growth is enabled or not for each of your volumes.

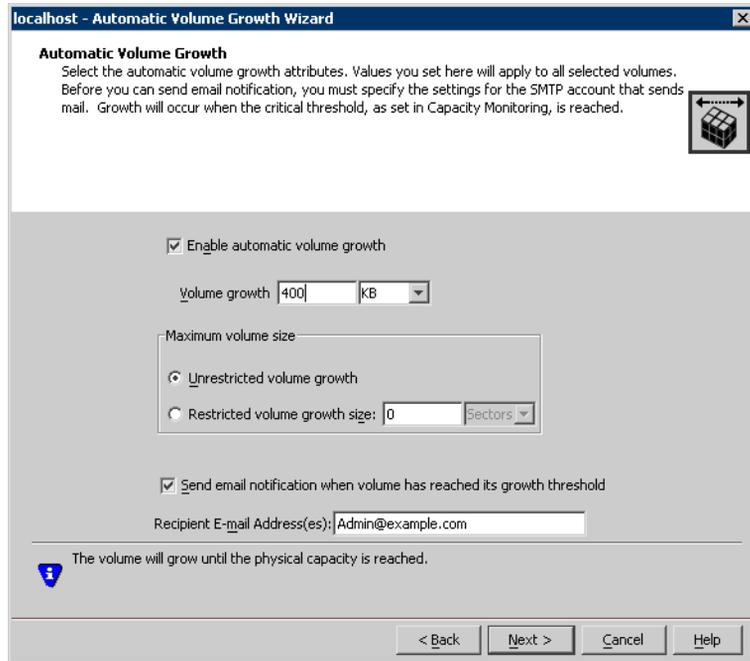
The following topics give more information on Rule Manager:

- [“Automatic volume growth script for volume capacity monitoring”](#) on page 249.
- [“Accessing the Rule Manager utility”](#) on page 237.

Caution: If you use a script to enable volume growth, do not enable the Automatic Volume Growth function through the **Automatic Volume Growth** wizard. If you enable a volume growth script and enable the Automatic Volume Growth function for a volume, the volume will increase in size by the combined amount. If you prefer to use the new feature, you must disable the script.

To enable automatic volume growth

- 1 Right-click on the volume you want to manage and click **Automatic Volume Growth**.
The Automatic Volume Growth wizard appears.
Click **Next** to continue.
- 2 Highlight any additional volumes you want to manage and click **Add**.
Click **Next** to continue.
- 3 Check the **Enable automatic volume growth** checkbox.
- 4 Set the Automatic Volume Growth parameters as follows.
 - **Volume growth**
Enter the size by which you want the volume to expand each time the growth threshold is reached.
 - **Maximum volume size**
Select the maximum volume size for the volume.
 - **Unrestricted volume growth** is the default. It allows the volume to grow without an upper limit to the volume size.
 - **Restricted volume growth** allows you to enter a maximum size for the volume. The volume growth is limited to this specified size. This setting may be useful to manage a database volume that may be vulnerable to uncontrolled rapid growth due to malicious updates, spam, or virus attack.
- 5 Enable notification by email (optional) as follows.



■ **Send email notification when volume has reached its growth threshold**

Check this checkbox, if you want an email sent when a volume has reached its growth threshold.

Enter the email address(es) to where the notifications should be sent in the Recipient E-mail Address(es) box. Separate multiple addresses with commas.

Make sure the SMTP Configuration settings have been set. If they have not, you should set them now.

See “[SMTP configuration for email notification](#)” on page 253.

Click **Next** to continue.

6 Select which disks to automatically grow the volume as follows.

■ **Auto select disks**

SFW automatically selects which disks to grow.

■ **Manually select disks**

Highlight which disks you want to grow and click **Add**.

Click **Next** to continue.

7 Review the summary of the Automatic Volume Growth settings and click **Finish** to apply.

Configuring Automatic Volume Growth in a cluster environment

In a cluster environment, you must configure the Veritas Scheduler Service on all nodes in the cluster environment to allow the transfer of Capacity Monitoring and Automatic Volume Growth settings to other nodes after failover. These settings are done once for each node after installing or upgrading SFW.

To configure the Veritas Scheduler Service in a cluster environment

- 1 Create a domain user that has administrator privileges that can access every cluster node.

Note: Note: For Windows Server 2008, the user must be the domain administrator.

- 2 From Windows Computer Management or Windows Administrative Tools, access Services, and select Veritas Scheduler Service.
- 3 Right-click Veritas Scheduler Service and select Properties from the context menu.
- 4 Click the Log On tab on the Properties GUI.
- 5 Click the This Account option and enter the domain user/administrator ID and password that was created in an earlier step of this procedure. Confirm the password and click Apply, then OK.
- 6 In the Windows Services GUI, restart the Veritas Scheduler Service to complete the configuration.

Automatic volume growth script for volume capacity monitoring

The volume capacity monitoring feature can send alert messages when dynamic volumes reach certain size thresholds. In addition, with the use of a script, volume capacity monitoring can automatically grow a volume when it reaches a specified capacity. With a script, you can conserve disk space on your servers because space is distributed automatically on an as-needed basis. You do not have to manually allocate the additional disk space when it is required.

The following steps set up a rule for growing a volume when a Capacity Monitoring threshold error occurs. The volume capacity monitoring feature monitors the capacity of the volume on your system; it has two thresholds—a Warning threshold with a default setting of 80% of capacity and a Critical threshold with a default setting of 90% of capacity. These are the points at

which the volume capacity monitoring feature sends an alert. To automate volume growth, you can associate an executable file, **volgrow.cmd**, with a Rule Manager rule so that when the Critical threshold is passed, a command to expand the volume is automatically sent.

Before setting up a new rule to execute a command, you must enable the VEA service and the GridNode service to interact with the desktop. These steps are not required if the new rule is only sending email notifications.

To enable the VEA service and the GridNode service to interact with the desktop

- 1 Stop the following services in the order shown below before configuring a new rule:
 - Action Agent
 - Storage Agent
 - Veritas Enterprise Administrator
 - GridNode
- 2 Right-click the Veritas Enterprise Administrator service. Select Properties, click **Allow service to interact with desktop** under the Log On tab, and click **OK**.
- 3 Right-click the GridNode service. Select Properties, click **Allow service to interact with desktop** under the Log On tab, and click **OK**.
- 4 Start the following services in the order shown below after configuring a new rule:
 - GridNode
 - Veritas Enterprise Administrator
 - Storage Agent
 - Action Agent

To configure a new rule to execute volume growth when capacity thresholds are met

- 1 Make sure that the volume capacity monitoring feature is turned on for the volume you want to monitor and that the thresholds are set to the desired percentages. The volume capacity monitoring feature is off by default. To enable volume capacity monitoring:
 - Right-click the volume and select **Capacity Monitoring**.
 - Select enable capacity monitoring for the volume.
 - Change the appropriate settings.
You may want to set the **Minimum time between alerts if condition persists** to a large number, such as 3600 seconds (equivalent to one

hour), so that you won't get so many messages while the volume is being enlarged.

- Click **OK** after the settings are completed.
- 2 If you have not already done so, set up the recipient or recipients that will receive the alert messages about the capacity threshold.
See "[Event notification](#)" on page 236.
 - 3 Select the Control Panel perspective in the VEA GUI.
 - 4 Click the **actionagent** node in the tree view.
 - 5 Double-click the **Rule Manager** icon to display the Rule Manager window.
 - 6 Click the **New Rule** button to display the Rule wizard.
Click **Next** to continue.
 - 7 In the window that appears:
 - Enter a name for the rule and select **A rule based on the alert topic**.
 - Click **Select** to select the Alert topic.
 - Check the **Volume capacity reached error condition** alert checkbox to select the alert.
 - Click **OK** to close the windows and return to the wizard.
Click **Next** to continue the wizard.
 - 8 Specify if the rule is triggered for alerts from any host or from specific hosts. If you specify alerts originating from specific hosts, then check the appropriate hosts in the lower part of the window.
Click **Next** to continue.
 - 9 Check both checkboxes in the Select actions window to enable the following actions:
 - **Send Email Notification**
Enter the email addresses of the recipients.
 - **Execute Command**
Enter the name of the hosts, the source host, and the path of the source file.
Enter the path for the `volgrow` command file for the source file. The default path for `volgrow.cmd` is:
`C:\Program Files\Veritas\Veritas Volume Manager
5.1\Sig\volgrow.cmd <VolumeName| DriveLetter>`
Click **Next** to continue.
 - 10 Check **Enable Rule** and click **Finish** to complete the setup.
The Rule Manager window displays listing the new rule. With the new rule, once the amount of data in the volume reaches the point where the error

threshold is reached, the rule activates, a message is sent that the error threshold has passed, and the command to grow the volume is implemented immediately. Once the process for growing the volume is complete, you will stop receiving error messages about the volume capacity.

Note: The included `volgrow.cmd` script is set to grow a volume by 150 MB. The size for growing the volume can be changed by modifying the `volgrow.cmd` script to a desired number. Please read the comments in the script for more information.

SMTP configuration for email notification

Note: The SMTP Configuration settings are global settings and need to be set only once for all the capacity monitoring and automatic volume growth email messages that are sent.

To configure SMTP

- 1 From the VEA Control Panel Perspective, select the StorageAgent node in the tree view.
- 2 Select **SMTP Configuration** in the right pane. The SMTP Settings screen appears.
- 3 Enter the following information:
 - SMTP server: enter the name or IP address of the SMTP mail server on your network.
 - Port: the default port for the SMTP mail server is usually 25.
 - Sender: enter the name that should appear as the sender.
 - Sender email address: enter the full SMTP email address for the sender.
- 4 Click **OK** to save your settings.

Standard features for adding fault tolerance

- Mirroring
- RAID-5 and RAID 0+1
- Hot relocation
- Dirty region logging (DRL) and RAID-5 logging
- Dynamic relayout

Overview

Fault tolerance is the capability of ensuring data integrity when hardware and software failures occur. This chapter focuses on the Veritas Storage Foundation for Windows standard features that provide fault tolerance.

Note: Additional fault tolerance for your storage can be gained through the program's options. The Microsoft Clustering (MSCS) Support option provides fault tolerance for up to eight servers through clustering. The Dynamic Multi-pathing option provides multiple paths from the server to a storage array to ensure application availability.

Mirroring

This section covers the following topics:

- [About mirroring](#)
- [Add a mirror to a volume](#)
- [Two methods for creating a mirror](#)
- [Break or remove a mirror](#)
- [Set the mirrored volume read policy](#)
- [Mirror a dynamic boot or system volume](#)
- [Reactivate a mirrored volume](#)
- [Repair a mirrored volume](#)

In addition, the following advanced procedures exist for mirrored volumes:

- [Dirty region logging for mirrored volumes](#)
- [FastResync](#)

FastResync is a feature that is part of the FlashSnap option, which is purchased as a separate license. FlashSnap is not included with the base Veritas Storage Foundation for Windows program.

About mirroring

A mirrored volume consists of at least two subdisks of identical size located on separate disks. Each time a file system or application writes to the volume, Veritas Storage Foundation for Windows transparently writes the same data to each of the volume's subdisks. With Veritas Storage Foundation for Windows, you can have up to 32 mirrors for all volume types except for RAID-5.

The primary purpose of mirroring is to provide fault tolerance; however, mirrored volumes can also improve I/O performance for most I/O-intensive applications, which make substantially more read requests than writes. With mirrored volumes, write requests may take longer than with non-mirrored volumes, but the effects are typically minor. Another important use of mirroring is the practice of breaking off a third mirror that can be used as a snapshot for backup or for other activities, such as uploading or updating data warehouses or performing application testing.

Two methods for creating a mirror

You can create a mirror on an existing volume or create a new mirrored volume. For details, see the following:

- To create a mirror on an existing volume, use the **Add Mirror** command. See “[Add a mirror to a volume](#)” on page 258
- To create a new mirrored volume, use the New Volume wizard. You select a mirrored layout when you create the volume. See “[Create dynamic volumes](#)” on page 60.

Note: The mirroring process is disabled if the volume cannot be mirrored or if there is no unallocated space on another dynamic disk large enough to mirror the volume. A RAID-5 volume cannot be mirrored.

Add a mirror to a volume

The basic process of adding a mirror is described in this section.

The Add Mirror wizard also enables you to implement the Dynamic Relayout feature.

See “[Dynamic relayout](#)” on page 277.

If you create more than one mirror at a time, you may see inconsistent information on the progress bar. Also, the generation of multiple mirrors does affect system resources. After creating a mirror, you may want to wait until it has finished generating before creating another mirror.

Caution: Adding mirrors to a volume involves a certain amount of time for mirror resynchronization. Take care not to perform actions on the volume until the command is complete. Also, if you inadvertently shut down the server or deport the disk group containing the volume before mirror resynchronization completes, any mirrors that were being added to the volume will be deleted when the disk group with the volume comes online again.

Note: The SmartMove feature can help reduce mirror resynchronization time. See “[SmartMove](#)” on page 130.

To add a mirror to a volume

- 1 Right-click on the volume you want to mirror.
- 2 Select **Mirror>Add** from the context menu.

The Add Mirror wizard appears.

- 3 Specify how many mirrors you want to add to the volume, and, if desired, manually assign the destination disks for the mirrors.
To assign the disks manually, click the **Manually select disks** radio button. Then use the buttons for adding and removing disks to move the disks you want assigned as destination disks to the right pane of the window.
You may also check **Disable Track Alignment** to disable track alignment for the mirrors.
Click **Next** to continue.

- 4 In the Specify the attributes dialog box, select the Concatenated or Striped volume layout type. If you are creating a striped mirror, the **Columns** and **Stripe unit size** boxes need to have entries. Defaults are provided.
You may also specify a mirror that mirrors across disks with the following attributes:

- Connected by port
- Identified by target
- Contained in an enclosure
- Connected by channel

In addition for a striped layout, you may specify to have the stripe across disks done by the following:

- Port
- Target
- Enclosure
- Channel

Click **Next** to continue.

The operation to create a new dynamic volume fails if the appropriate resources are not available to support the selected attributes to mirror across disks.

- 5 On the summary page, click **Finish** to add the mirror.

Break or remove a mirror

You can *break* or *remove* a mirror. It is important to understand the difference between these operations.

Breaking a mirror takes away a redundant mirror (or plex) of a volume and assigns it another drive letter. The data on the new volume is a snapshot of the original volume at the time of breaking. Breaking off a plex of the mirrored volume does not delete the information, but it does mean that the plex that is

broken off will no longer mirror information from the other plex or plexes in the mirrored volume.

Removing a mirror from a volume “removes” or destroys the data from the selected mirror and leaves the other mirror or mirrors intact. After you remove a mirror, the space on the disk used by the removed mirror becomes unallocated free space.

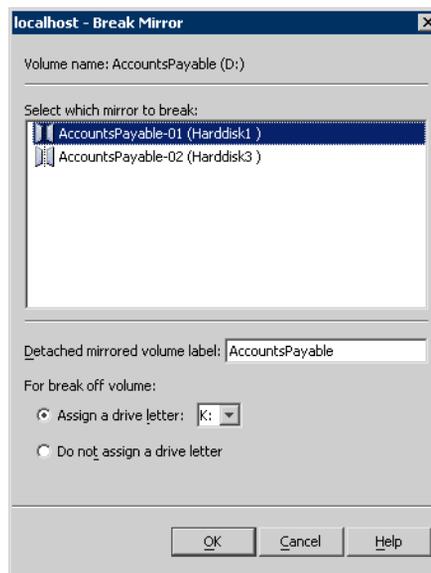
Note: Veritas Storage Foundation for Windows does not allow you to remove the mirror of the volume that Windows is using to boot from. Also, if you break a mirrored boot volume, you cannot boot from the portion that was broken off.

The details on breaking and removing a mirror are included in the next two sections, “Break Mirror” and “Remove Mirror.”

Break mirror

To break a mirror

- 1 Right-click on the volume from which you want to break a mirror. Click **Mirror** on the context menu that comes up, and then select **Break** from the submenu.



- 2 In the Break Mirror dialog box that appears, select the mirror you want to break off.

Choose whether or not to assign a drive letter to the broken-off volume. You may assign a specific letter from the drop-down list or accept the default. You can also assign a label to the detached mirror.

When you are satisfied with your choices, click **OK**.

Once the command is completed, the broken-off plex is no longer part of the mirrored volume and is assigned the drive letter specified, if **Assign a drive letter** was selected. The broken-off plex retains all other volume layout characteristics except the mirroring. For example, if you had a mirrored striped volume, the broken-off plex would become a striped volume.

Note: If you have a mirrored volume with two plexes and you break one off, the remaining plex is no longer a mirrored volume. It too assumes its other layout characteristics without the mirroring, but it does keep the drive letter of the original mirrored volume.

Remove mirror

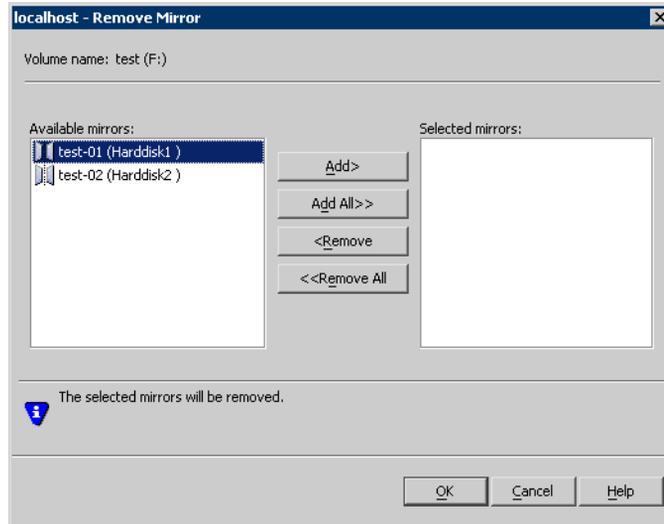
After a mirror is removed, the space formerly allocated to it reverts to free space.

Caution: When a mirror is removed, all of the data on the removed mirror is deleted.

To remove a mirror

- 1 Right-click on the volume from which you want to remove the mirror.
- 2 Select **Mirror>Remove**.

The Remove Mirror dialog box will appear as shown below:



The name of the volume with the mirror appears in the upper left.

- 3 The available mirrors will appear in the left pane. Use the **Add** or **Add All** button to move the desired mirrors to the list of mirrors selected to be removed in the right pane. To move mirrors from the **Selected mirrors** list to the **Available mirrors** list, select them in the right pane and click the **Remove** button. To move all of the mirrors from the **Selected mirrors** list back to the **Available mirrors** list, click the **Remove All** button.
- 4 Click **OK** to remove the mirror or mirrors.
- 5 Click **Yes** at the message warning you that removing mirrors will reduce the redundancy of the volume.

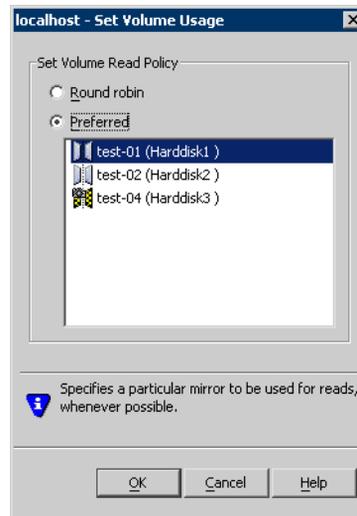
Set the mirrored volume read policy

Setting the read policy on a dynamic volume allows you to specify either that a particular mirror be used for reads or that all mirrors be read in turn in “round-robin” fashion for each nonsequential I/O detected. The default is that mirrors be read “round robin.”

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support setting the volume read policy.

To set the volume read policy

- 1 Right-click on the volume you wish to set the read policy for.
- 2 Select **Set Volume Usage** on the context menu.
The Set Volume Usage dialog appears.



- 3 Select either the **Round robin** or **Preferred** option.
 - The **Round robin** option reads each plex in turn in “round-robin” fashion for each nonsequential I/O detected. Sequential access causes only one plex to be accessed. This takes advantage of the drive or controller read-ahead caching policies.
 - If you select the **Preferred** option, you must select the mirror you wish to set as the preferred option from the list of mirrors shown. This mirror will be used for reads whenever possible.
This can improve your system’s read performance, particularly if the drive used for the target mirror is a high-performance drive or if the target mirror is located on a drive that is geographically closer.
If a mirror has already been set as preferred, you will see the text “(Preferred plex)” after the mirror’s name in the dialog box.
When a preferred plex has an error, the read operation is completed by another plex. This happens automatically, as if there were no preferred plex.
- 4 Click **OK** to set the volume usage, or click the **Cancel** button to exit without setting the read policy.

Mirror a dynamic boot or system volume

This section presents items to consider when you plan to mirror a dynamic boot or system volume.

You need to be aware of the following:

- Be sure to back up any data on the system before you create the mirror.
- If you decide you want your system to boot from the mirror, make the necessary change to the **boot.ini** file on a system running Windows Server 2003. For Windows Server 2008, refer to the Microsoft documentation for more information.
- If a break-mirror operation is performed on a mirrored boot volume, the resulting new volume—the broken-off mirror—will not be usable as a boot volume.

Under certain conditions, you may be unable to create a mirror on a boot or system volume or get an error message during the process.

See “[An attempt to mirror a boot or system volume fails or has an error message](#)” on page 499.

You must follow specific steps in setting up a dynamic boot or system volume.

See “[Set up a dynamic boot and system volume \(Optional\)](#)” on page 70.

Reactivate a mirrored volume

If there is a problem with one of the disks on which a mirrored volume resides, make sure that the disk is properly connected, and then try to bring that disk back online by first using **Rescan**. If **Rescan** does not work, then use the **Reactivate Disk** command. In most cases, **Reactivate Disk** will bring the disk online and all of the volumes will be healthy.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Disk** command.

However, if any of the mirrors of the mirrored volume are still not healthy, you may need to resynchronize the degraded volume with the **Reactivate Volume** command. Resynchronizing makes the data consistent on all mirrors of a mirrored volume.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Volume** command.

Right-click on the volume to bring up the context menu, and then click **Reactivate Volume**.

The mirrored volume should come back to a Healthy state unless there is a serious problem with the volume.

See also the following topics:

- [Rescan command](#)
- [Reactivate disk command](#)
- [Reactivate volume command](#)

Repair a mirrored volume

When a disk on which a mirrored volume resides fails, the volume displays a Degraded status. The disk's name is changed to Missing Disk, and an icon (X) appears on the Missing Disk icon. The status of the disk will be Offline.

You can use the **Repair Volume** command to repair a mirrored volume.

See "[Repair volume command for dynamic mirrored volumes](#)" on page 493.

RAID-5 and RAID 0+1

This section describes the fault tolerance capabilities of RAID-5 and RAID 0+1.

RAID-5

A RAID-5 volume is a fault-tolerant volume with data and parity striped intermittently across three or more physical disks. Parity is a calculated value that is used to reconstruct data after a failure. If a portion of a physical disk fails, the data on the failed portion can be recreated from the remaining data and parity. You can create RAID-5 volumes only on dynamic disks. You cannot mirror RAID-5 volumes.

The advantage of RAID-5 is that it provides fault tolerance with less hardware than that required for mirroring. RAID-5 supports the configuration of any number of data disks with the hardware cost of only one disk for parity. Mirroring requires separate disks for each mirror. RAID-5 protects against data loss when one disk fails. However, it is necessary to resynchronize the data from the other disks to access the data. With mirroring, if one disk fails, the data is available from another mirror right away. Also, RAID-5 does not have the advantage of adding more mirrors for increased fault tolerance. With mirroring, you can have three or more mirrors so that if more than one disk fails, there is still fault tolerance. With RAID-5, once two disks fail, the RAID-5 volumes on multiple disks will fail. Now that the cost of storage has decreased, mirroring is a better choice for fault tolerance.

You can resynchronize a RAID-5 volume after it is degraded (having lost one disk).

See “[Repair volume command for dynamic RAID-5 volumes](#)” on page 493.

RAID 0+1

Mirroring with striping, RAID 0+1, offers the protection of mirroring and the speed of striping.

The following are some advantages of RAID 0+1 volumes:

- Very large fault-tolerant volumes can be created that can hold large databases or server applications.
- Read performance is very high. A preferred plex can be designated. Within each plex, striping balances the load.
- The write penalty (that is, the multiple writes SFW must perform to keep all plexes' contents synchronized) is mitigated by the striping of data across multiple disks.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support RAID 0+1.

About the only disadvantage to RAID 0+1 is the hardware cost. The user must purchase, house, power, and operate twice as much raw storage capacity as the data requires. Today with lower storage costs, mirroring with striping is becoming a preferred RAID layout for mission-critical data.

Hot relocation

“Hot relocation” describes the ability of a system to automatically react to I/O failures. It is an automatic process that relocates subdisks from a disk that has I/O errors.

The default for Veritas Storage Foundation for Windows is to have automatic hot relocation mode inactive. This means that if an I/O error occurs in a redundant subdisk, the subdisk is not automatically relocated to another disk. The tasks to enable the hot relocation mode are described in the following hot relocation setup section.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support hot relocation.

This section covers the following topics:

- [Hot relocation overview](#)
- [Hot relocation setup summary](#)
- [Hot relocation mode](#)
- [Customize target disks with set disk usage](#)
- [Undo hot relocation](#)
- [Clear hot relocation information](#)

Hot relocation overview

In hot relocation mode, if there are I/O errors on a subdisk containing a redundant volume (RAID-5 or mirrored), the redundant volume’s subdisks are moved from the failed subdisk to a hot spare disk. If there is not enough free space on designated hot spare disks, then free space on any available disk will be used. Depending on available disk space, the subdisks will not always be moved to the same disk, but may be scattered within the dynamic disk group. The **Undo Hot Relocation** command can be used to move the subdisks back to their original location after the failed disk has been repaired or replaced.

Note: The hot relocation operation is performed only for redundant subdisks with I/O errors if there are healthy plexes of the volume available elsewhere within the dynamic disk group. Nonredundant subdisks with I/O errors are not relocated; the volume fails, and an alert message is sent to the Event Log.

When selecting space for relocation, hot relocation preserves the redundancy characteristics of the dynamic volume that the relocated subdisk belongs to. For

example, hot relocation ensures that a failed subdisk is not relocated to a disk containing its mirror. If redundancy cannot be preserved by using any available spare disks or free space, hot relocation does not take place. If relocation is not possible, the system administrator is notified and no further action is taken.

When hot relocation takes place, the failed subdisk is removed from the configuration database, and Veritas Storage Foundation for Windows takes precautions to ensure that the disk space used by the failed subdisk is not recycled as free space.

The default is to have all disks available as targets for hot-relocated subdisks. Using the **Set Disk Usage** command, you can choose to designate specific disks as not available.

See “[Disk usage options](#)” on page 270.

Note: The **Reset** button restores default settings.

Hot relocation setup summary

There are two tasks that must be done to ensure that the hot relocation mode is properly configured.

The first task uses the **Hot Relocation** command from the **System Settings** in the Control Panel to verify that the hot relocation mode is enabled.

The second task uses the **Set Disk Usage** command to define within each disk group which disks, if any, should be selected as preferred targets for hot-relocated subdisks or never used as targets for hot-relocated subdisks.

Hot relocation mode

The default for Veritas Storage Foundation for Windows is to have automatic hot relocation mode inactive. This means that if an I/O error occurs in a redundant subdisk, the subdisk is not automatically relocated to another disk. Use the **Set Disk Usage** command to designate preferred disks as targets for hot relocation.

The option to enable the hot relocation mode is available from **System Settings** in the Control Panel or from **Edit Configuration** in the Storage Foundation Assistant.

To enable the hot relocation mode

- 1 Open **System Settings** in the Control Panel or open **Edit Configuration** in the Storage Foundation Assistant.

- 2 Click the **Hot Relocation** tab in **System Settings** or click **Hot Relocation** in **Edit Configuration**.
- 3 Check the checkbox to enable the hot relocation mode. If automatic hot relocation is disabled and an I/O failure occurs, an alert will be sent to the Event Log, but no further action will take place.
- 4 When you are satisfied with your selection, click **OK**.

Customize target disks with set disk usage

The **Set Disk Usage** command allows you to specify how individual disks within a dynamic disk group will be used by Veritas Storage Foundation for Windows. If an I/O failure occurs, SFW looks for free space on preferred or secondary target disks within the dynamic disk group that contains the failing disk to determine where to move the subdisks. Thus, it is important to consider the entire disk group when configuring disk usage. In addition, you need to consider the track alignment settings of the failing disk and the target disks. SFW does not preserve the track alignment settings of the failing disk. SFW adopts the track alignment settings of the target disk after hot relocation takes place.

The default for each disk is “secondary hot relocation target.” This will probably be the state you prefer for the majority of disks within each disk group. If hot relocation occurs and subdisks from a specific disk are scattered throughout the disk group, it is possible to repair or replace the failed disk and then use the **Undo Hot Relocation** command to return all the subdisks back to their original location.

Disk usage options

The **Set Disk Usage** command offers the following options:

- Reserved for manual use
Disks reserved for manual use are not available in automatic selection operations, including hot relocation. In an automatic selection operation, Veritas Storage Foundation for Windows chooses the storage where the operation occurs. Generally, the user is given a choice between allowing SFW to “Auto select disks” or “Manually select disks.” Examples of commands that allow automatic selection are **New Volume** and **Add Mirror**. Reserving a disk for manual use allows you to prevent any unwanted volumes or subdisks from being placed on that disk and gives you complete control over the disk.

There are three options related to how a disk is used as a target for hot-relocated subdisks. In considering how to mark each disk, remember that the hot relocation operation occurs at the disk group level, and only target disks within the same disk group will be considered.

The three options are as follows:

- Preferred hot relocation target
If there is an I/O failure anywhere in the system, SFW first looks for space on disks that have been marked as preferred hot-relocation targets for redundant subdisks.
- Secondary hot relocation target
This is the default for all disks. During the hot relocation operation, if there are no disks selected as preferred targets or if there is no space available on those disks, SFW chooses space on disks marked as secondary targets.
- Not used as a hot relocation target
This option does not allow any hot-relocated subdisks to be moved to the selected disks. It differs from the “Reserved for manual use” option in that the disk remains available for other automatic selection operations.

To set disk usage

- 1 Right-click on the desired disk.
- 2 Select **Set Disk Usage** from the context menu.
The Set Disk Usage dialog box appears.
- 3 Choose how you want Veritas Storage Foundation for Windows to use the disk.
- 4 When you are satisfied with your selection, click **OK**.
You can review the settings for all your disks by selecting the Disks node in the tree view and then viewing the **Disks** tab in the right pane. The settings for each disk are listed in the Reserved and Hot Use columns.

Undo hot relocation

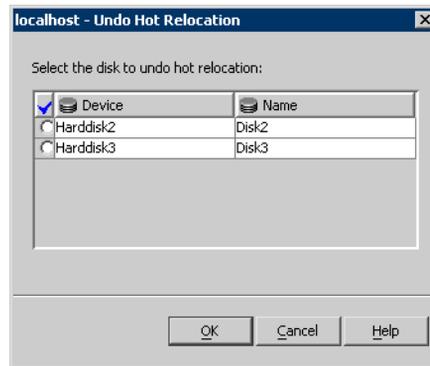
The command **Undo Hot Relocation** relocates subdisks back to their repaired original disk or replacement disk and restores a system to its original configuration, less any failed volumes. If hot relocation scattered subdisks from a failed disk to several disks within a dynamic disk group, the **Undo Hot Relocation** command will move all of them back to a single disk without requiring the user to find and move each one individually.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Undo Hot Relocation** command.

Note: This command is available only after a hot relocation procedure has occurred.

To undo a hot relocation

- 1 Right-click on the dynamic disk group that contains the hot-relocated volumes.
- 2 Select **Undo Hot Relocation** from the context menu.
A window appears showing the original disks that had I/O errors.



- 3 Click in the column under the checkmark to select the disks you wish to restore. The hot-relocated subdisks will return to this disk.
- 4 Click **OK**.

Clear hot relocation information

The **Clear Hot Relocation Information** command deletes the information that describes the original location of any subdisks that have been moved via the hot relocation process. Use this command only if you do not plan to move the hot-relocated subdisks back to their original configuration.

Caution: Once you clear the hot relocation information, you will not be able to perform an **Undo Hot Relocation** command for that dynamic disk group.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Clear Hot Relocation Information** command.

To clear hot relocation information

- 1 Right-click on a disk group that contains hot-relocated subdisks.
- 2 Select **Clear Hot Relocation Information** from the context menu.
- 3 A dialog box will appear asking if you are sure you want to clear the relocation information for the dynamic disk group. Click **Yes** if you want to clear the hot relocation information.

Dirty region logging (DRL) and RAID-5 logging

This section describes the dirty region logging (DRL) and RAID-5 logging features. These two features greatly speed up the time that it takes to recover from a system crash for mirrored volumes and RAID-5 volumes.

This section covers the following topics:

- [Dirty region logging for mirrored volumes](#)
- [RAID-5 logging](#)
- [Add a log](#)
- [Remove a log](#)

Dirty region logging for mirrored volumes

DRL uses a log-based recovery method to quickly resynchronize all the copies of a mirrored volume when a system is restarted following a crash. If DRL is not used and a system failure occurs, all mirrors of the volume must be restored to a consistent state by copying the full contents of the volume between its mirrors. This process can be lengthy and I/O intensive.

A log can be created when the volume is created or can be added later.

Caution: Although DRL makes sure that the mirror copies of the mirrored volumes are in sync following a system crash, it does not guarantee data integrity. The data integrity will be preserved by the file system, for example, NTFS.

When a dirty region log is created, a log subdisk is added to the volume. Multiple logs can be associated with a single mirrored volume as a fault-tolerant measure. Depending on the number of logs configured, this may result in degraded performance.

RAID-5 logging

The primary purpose of RAID-5 logging is to quickly reactivate a RAID-5 volume when a system is restarted following a crash. Without RAID-5 logging enabled, a time-consuming reactivation of the entire RAID-5 volume is necessary.

If a RAID-5 log is available, updates need to be made only to the data and parity portions of the volume that were in transit during a system crash. The entire volume does not have to be resynchronized.

A log can be created when the volume is created or can be added later.

When a RAID-5 log is created, a log subdisk is added to the volume. Multiple RAID-5 logs can be associated with a single RAID-5 volume as a fault-tolerant measure. Depending on the number of logs configured, this may result in degraded performance.

Add a log

This operation adds a log plex containing a log subdisk to a volume. For mirrored volumes, a dirty region log is added. For RAID-5 volumes, a RAID-5 log is added.

Note: Logs are used only for mirrored volumes or RAID-5 volumes.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support adding a log.

To add a log to a mirrored or RAID-5 volume

- 1 Right-click on the volume you wish to add the log to.
- 2 Select **Log>Add** from the context menu.
The Add Log dialog box appears.
- 3 Choose either the default setting **Auto assign destination disks** or the option to manually assign the destination disks. Click **OK** to create the log.

Auto assign destination disks

This option adds one log to the selected volume.

Manually assign destination disks

You can create multiple logs with this option.

Click the **Manually assign destination disks** radio button. Available disks appear in the left pane. To add destination disks for the logs, select them in the left pane and click the **Add** button. To add logs to all available disks, click the **Add All** button.

To remove destination disks, select them in the right pane and click the **Remove** button. To remove all of the destination disks, click the **Remove All** button.

Disable Track Alignment

This option disables track alignment for the logs being added.

Remove a log

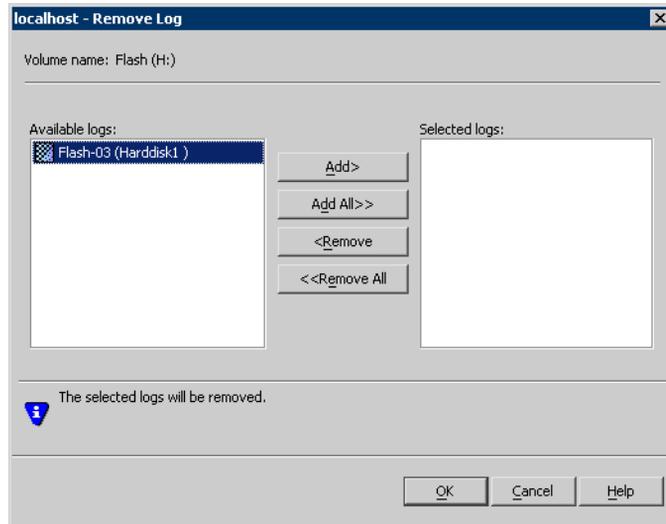
After a log is removed, the space formerly allocated to it reverts to free space.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support removing a log.

To remove a log

- 1 Right-click on the volume you wish to remove the log from.
- 2 Select **Log>Remove**.

The Remove Log dialog box will appear as shown in the sample screen below:



The name of the volume with the log appears in the upper left.

- 3 The available logs will appear in the left pane. Use the **Add** or **Add All** button to move the desired logs to the list of logs selected to be removed in the right pane. To move the logs from the **Selected logs** list to the **Available logs** list, select them in the right pane and click the **Remove** button. To move all the logs from the **Selected logs** list back to the **Available logs** list, click the **Remove All** button.
- 4 Click **OK** to remove the log or logs.
- 5 Click **Yes** at the message warning you that removing logs will potentially increase recovery time.

Dynamic relayout

Storage Foundation for Windows allows you to reconfigure the layout of a volume without taking it offline with the Dynamic Relayout feature.

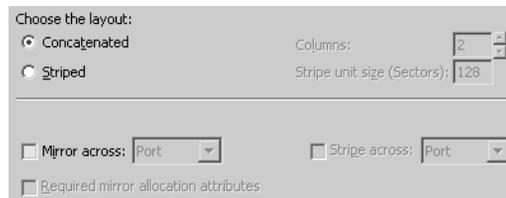
You can make the following dynamic volume layout changes:

Table 8-1 Dynamic Relayout Changes

Changed from	Changed to
Concatenated	Striped
Striped	Concatenated
Striped	Striped with changes in column size or stripe unit size

This feature is implemented through the Add Mirror window. That window has a section called “Choose the layout.”

Figure 8-1 Choose the layout section of add mirror window



The basic concept is that you select the features you want the volume layout to be changed to, and the program creates a mirror or plex of the original volume with the desired attributes of the new layout. If you no longer have a need for the original volume, you remove it with the **Remove Mirror** command.

Thus, the conversion or relayout is a two-step process. First, you select the desired attributes and create the mirror through the **Add Mirror** command. Second, you remove the original plex through the **Remove Mirror** command.

Examples of dynamic relayout

This section provides examples of the different layout types. The section that follows gives the step-by-step process for Dynamic Relayout.

■ **Concatenated to Striped**

For example, if you want to convert a concatenated volume on a single disk to a striped volume with two columns, you select striped and two columns in the Add Mirror window. The resulting volume will have two mirrors or plexes—one is the original plex, and the second is a copy of the original volume striped across two disks. Thus, the entire volume requires a total of three disks. The volume's type is designated as **Mixed**. At this point, you can remove the original plex by deleting it with the **Remove Mirror** command. Now you have a striped volume in place of the concatenated one that existed before.

■ **Striped to Concatenated**

Changing a striped volume to a concatenated volume probably won't be done very often. Assume the example of an existing two-column striped volume. If you open the Add Mirror window and select the concatenated layout, the resulting volume will involve three disks: the first two disks have the plex of the two-column striped original volume, and the third disk contains a concatenated plex of the volume. By removing the original plex, the volume now will now reside on one disk.

■ **Striped to Striped**

The purpose of converting a striped volume to another striped volume is to change the attributes of the volume (the stripe unit size and the number of columns) without having to recreate the volume.

For example, you can convert a two-column striped volume to a three-column striped volume. First, you would select three columns in the Add Mirror window. The resulting volume would involve five disks: two disks for the original two-column striped plex and three disks for the new three-column striped mirror. Again, you can remove the original plex by deleting it with the **Remove Mirror** command, leaving only a three-column striped volume.

Detailed steps for dynamic relayout

Dynamic Relayout allows you to change dynamic volume layout types while the volumes are still online. You use both the **Add Mirror** command and the **Remove Mirror** command to complete the Dynamic Relayout process.

- 1 Right-click the volume with the layout that will be converted. Choose **Mirror>Add** from the context menu that appears.
- 2 Set the number of mirrors setting to 1. If desired, you can manually select the disks by clicking the radio button to select the disks and use the **Add** or **Add All** button to move the disks you want to the **Selected disks** pane on the right side of the window. You may also check **Disable Track Alignment** to disable track alignment for the mirrors.
Click **Next** to continue.
- 3 Select the desired layout for the volume in the “Choose the layout” section of the window.
If you choose striped, make sure that you have the number of columns desired and the stripe unit size that you want.
Click **Next** to continue.
- 4 When you are satisfied with your settings, click **Finish**.
The program creates a mirror or plex of the original volume with the attributes of the new layout. If you no longer have a need for the original volume, you can remove it with the **Remove Mirror** command.
You may want to review the information on how the program implements the dynamic relayout for each of the possible layout types.
See “[Examples of dynamic relayout](#)” on page 278.
- 5 If you want to delete the original plex, right-click on it and select **Mirror>Remove** from the context menu. In the Remove Mirror window that appears, use the **Add** button to move the plex to be removed to the **Selected mirrors** pane on the right side of the window, and click **OK**.
The process for converting the layout type on the volume is now complete.

Command line interface

SFW commands available from the command line

This chapter describes the command line interface (CLI) commands available with Veritas Storage Foundation for Windows. The key SFW commands can be executed from the command line as well as from the GUI.

The utilities are available in the Veritas Storage Foundation for Windows installation directory, typically **C:\Program Files\Veritas\Veritas Volume Manager 5.1**. You can invoke the commands from any directory in the command prompt window.

Note: The CLI commands run only on the server. They will not run on the Veritas Storage Foundation for Windows client.

Note: For Windows Server 2008, all CLI commands must run in the command window in the "run as administrator" mode.

The available commands are the following:

- **vxvol**
Displays volume information, repairs a RAID-5 or mirrored volume, turns Fast Resynchronization on and off, and reactivates a volume.
- **vx dg**
Allows you to create a dynamic disk group and perform other functions related to dynamic disk groups.
- **vxclus**
Enables and disables the capability of forcing the import of a disk group on a cluster controlled by Microsoft Clustering. The command also has keywords that allow the cluster disk group to reside on the same bus as the cluster node's system and boot disk.

- [vxdisk](#)
Provides information on dynamic disks, allows you to reactivate a dynamic disk, and enables track alignment for the disk.
- [vxassist](#)
Allows you to create a dynamic volume and perform other operations related to dynamic volumes such as shrinking the size of the volume.
- [vxevac](#)
Evacuates (moves) subdisks from the disk specified to a specified destination disk.
- [vxunreloc](#)
Reverses the process of hot relocation.
- [vxsd](#)
Provides commands for moving and splitting a subdisk and joining two subdisks.
- [vxstat](#)
Provides commands for displaying statistics for disks, volumes, and subdisks.
- [vxtask](#)
Provides commands for displaying percentage completion information for tasks.
- [vxedit](#)
Provides commands to rename or add comments to a dynamic disk group, a disk, a volume, a plex, and a subdisk.
- [vxdmpadm](#)
Provides commands for Dynamic Multi-pathing (DMP DSMs).
- [vxcbr](#)
Provides commands for backing up and restore the Veritas Storage Foundation for Windows configuration information.
- [vxsnap](#)
Performs multiple snapshots simultaneously. The utility integrates with the Windows Volume Shadow Copy Service (VSS) as a VSS Requester. This allows for the simultaneous snapshot of all volumes associated with an Exchange Server database or an SQL Server 2005 database.
- [vxsnapsql](#)
Performs simultaneous snapshot of all volumes associated with an SQL Server 2000 or SQL Server 2005 database.
- [vxfsync](#)

Resynchronize a single file in a snapshotted volume back to the original volume. It is designed to restore one or more corrupt files in a database application that has volumes with multiple database files.

- **vxscrub**
Removes unneeded entries in the registry that are a result of adding and deleting volumes. The command is designed to shrink the size of the registry by purging the system hive.
- **vxverify**
Determines if there are any differences between plexes of mirrored volumes.
- **vxcache**
Enables a designated cache memory pool to improve performance for specific dynamic volumes.
- **vxprint**
Displays information about SFW and VVR objects.

Command line log

SFW provides support for a log that captures commands issued through the CLI. The command line log also captures the system response to each command. The log file, vxcli.log, is typically located at **C:\Program Files\Veritas\Veritas Volume Manager 5.1\logs**.

Each entry in the log is prefixed with the date and time of the command or system response, followed by the process identification and thread identification. Each CLI command is a separate entry in the log and each is identified by "----- Command : ". Each system response is also a separate entry in the log and follows the CLI command.

Note: Help messages are not recorded in the command line log.

As an example of a log's content, the following was recorded as a result of entering `vxdbg list`

```
03/28/06 22:59:37 [5376,2024] ----- Command : vxdbg
list
03/28/06 22:59:38 [5376,2024] Disk groups are...
03/28/06 22:59:38 [5376,2024] Name : BasicGroup
03/28/06 22:59:38 [5376,2024] Disk Group Type : Basic
```

```
03/28/06 22:59:38 [5376,2024] DiskGroup ID : No ID
03/28/06 22:59:38 [5376,2024] Status : Imported
03/28/06 23:00:08 [4212,5760] ----- Command : vxdisk
list
03/28/06 23:00:09 [4212,5760] Name MediaName Diskgroup
DiskStyle Size(MB) FreeSpace(MB) Status
03/28/06 23:00:09 [4212,5760] Harddisk0 BasicGroup MBR
117239 67240 Uninitialized
03/28/06 23:00:09 [4212,5760] Harddisk1 BasicGroup MBR
1019 917 Uninitialized
03/28/06 23:00:09 [4212,5760] Harddisk2 (No Signature)
BasicGroup MBR 10236 10236 Uninitialized
03/28/06 23:00:09 [4212,5760] Harddisk3 BasicGroup MBR
1019 917 Uninitialized
03/28/06 23:00:09 [4212,5760] Harddisk4 (No Signature)
BasicGroup MBR 10236 10236 Uninitialized
03/28/06 23:01:41 [1100,4728] ----- Command : vxdbg
-g dg1 init harddisk1
03/28/06 23:01:47 [1100,4728] Successfully created
dynamic disk group dg1
```

Conventions for command line syntax

This topic describes the typographical conventions used for the command line syntax in this CLI section.

The conventions are as follows:

- Any parameter that is optional for the command syntax has square brackets ([]) around it. For example:
`[-b]` or `[-o keepplex]`
- Required command words and parameters for the command do not have square brackets around them. For example:
`vxvol volinfo` or `<VolumeName>`
- Command words and parameters that are typed as shown in the command syntax are displayed in the Courier bold font. For example:
`vxvol volinfo` or `[-b]`
- Parameters that require the user to enter something in their place are displayed in Helvetica Italic font and have angle brackets around them. They are placeholders for information the user enters. For example:
`<VolumeName>`
If a parameter is enclosed by both angle brackets and square brackets, it is an optional parameter for the command. For example:
`[<DiskName>]`
- The | character is a separator that allows two or more choices for a given parameter. The user can use any one of the choices for the command. For example:
`<VolumeName | DriveLetter>`
`[volume|mirror|log]`
- Ellipses (...) after a parameter indicate more items. For example, the parameter `<DiskName>...` means to enter one or more disk names. The parameter `[DriveLetter={A|B|...|Z}]` means to enter `DriveLetter=` and a drive letter in the range of A to Z.
- The parameter `!<DiskName>` is used with three commands—`vxassist break`, `vxassist remove`, and `vxassist snapshot`. The exclamation mark is needed to make these commands consistent with the Volume Manager for UNIX versions of these commands.
- **About Volume Names**
 - **Assigning a Volume Name**
When you are creating a volume with `vxassist make`, the `<VolumeName>` parameter is a name you assign to the volume. A volume name is limited to 18 characters. It cannot contain spaces or

forward or backward slashes. Also, a period cannot be the first character in the name. The volume name you assign in either the command line or the GUI is the internal name of the volume. SFW will make that internal volume name into the operating system volume label. However, if you later change the volume label through the operating system, the internal SFW volume name will not change.

Note: The name you assign for the *<VolumeName>* parameter when creating a volume in the CLI is equivalent to the volume name that is specified in creating a volume with the **New Volume** command in the VEA GUI.

The internal volume name supplies an identifier for the volume that will stay the same. The operating system may reassign drive letters. A persistent name is especially important in scripts. If you want to use the internal volume name in the command line to refer to the volume, you must precede it with its disk group parameter, *-g<DynamicDiskGroupName>*, for example, *-gDG1 Salesvolume*. If you do not assign a volume name, SFW will assign the name, in the form of *volume1*, *volume2*, etc. The internal volume name is assigned by the program only to dynamic volumes.

■ **Other Ways to Designate a New Volume**

A basic or dynamic volume can also be indicated by a drive letter, *<DriveLetter>*. If the volume has been mounted at an NTFS folder, the volume name is indicated by the drive path parameter *<DrivePath>*, which is the path to the folder.

■ **Referring to an Existing Volume**

There are four methods for referring to an existing volume in the CLI:

1) The full path name of the volume, which has the following syntax:

```
\Device\HarddiskDmVolumes\<DynamicDiskGroupName>\<VolumeName>
```

For example:

```
\Device\HarddiskDmVolumes\DynDskGrp1\Volume1
```

2) With a drive letter, such as *D*:

3) With its internal volume name, which requires the disk group option

```
For example, -gDG1 Salesvolume or -gDG1 Volume1
```

4) With a *<DrivePath>* parameter if the volume is mounted on an NTFS folder, such as *D:\Sales*.

Note: In commands that involve existing volumes, the internal volume name is referred to as *<VmName>* in the command line syntax.

You can identify the internal volume name through the `vxvolinfo` command, or you can see the internal volume name in the right pane of the GUI when a volume is selected.

■ **About Disk Names**

A disk can be specified in the command line in four ways:

- 1) With the device name, such as `Harddisk2`
- 2) With a path name, such as `\Device\Harddisk2`
- 3) With the internal disk name assigned by the SFW program, such as `Disk2`
- 4) With `p#c#t#l#`, where the `#`s correspond to port, channel, target, and LUN

The internal disk name is a persistent name that remains even when the operating system changes the disk name, and thus it is useful in scripts. It requires a disk group parameter whenever it is used (for example, `-gDG1 Disk2`). You cannot assign this name. You can identify a disk's internal name by using the `vxdisk diskinfo` command. An internal disk name is assigned only to dynamic disks, not basic disks.

You can also see the device name and the internal disk name in the right pane of the GUI when a disk or disks are selected.

vxvol

The **vxvol** utility has commands relating to dynamic volumes. These are the keywords:

<code>volinfo</code>	Displays information on a dynamic volume.
<code>repair</code>	Repairs a RAID-5 volume.
<code>set fastresync=on off</code>	Turns Fast Resynchronization on and off.
<code>reactivate</code>	Reactivates the volume (restarts the volume).
<code>rdpol prefer</code>	Sets the volume read policy on a volume with multiple mirrors to designate one specific plex to be used whenever possible for reading from the volume.
<code>rdpol round</code>	Sets the volume read policy on a volume with multiple mirrors so that plexes are read sequentially in a “round-robin” fashion.
<code>growfs</code>	Grow the file system.
<code>access</code>	Sets the volume to read only or read/write access mode.
<code>reclaim</code>	Reclaim storage space from a volume. (Portion of volume must reside on a thin provisioned disk.)
<code>reclaimcancel</code>	Immediately cancels reclaim operation
<code>capacitymonitor</code>	Set threshold on dynamic volume so that when the used disk space on a volume reaches the specified threshold, an alert message is logged.
<code>autogrow</code>	Allows an individual volume to grow (increase capacity) automatically by a specified amount when the used disk space on the volume reaches a certain threshold. The threshold is set by Capacity Monitoring.

Each keyword is followed by the volume name or drive letter. Typing the following sequence for each keyword brings up a description of its syntax:

```
vxvol <Keyword> -?
```

Keywords or operands

```
vxvol volinfo
```

```
vxvol [-v] [-g<DynamicDiskGroupName>] volinfo <VolumeName|  
DriveLetter|VmName|DrivePath>
```

Returns information on the volume. The following attributes apply:

<code>[-v]</code>	The verbose option displays the size and offset of the subdisks as well as the other information provided by the main command.
<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1Volume1</code> .
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

The possible information categories are name, dynamic disk group name, size, volume type, whether it is a boot or system volume, whether it contains the page file (pagefile.sys), volume status, and access mode (read only or read/write access mode). If the volume is a dynamic volume, the command can return additional information on any mirror plexes or DCO volumes associated with the volume.

Example

```
vxvol volinfo E:
```

This returns a list with specified information as described above for volume E.

```
vxvol repair
```

```
vxvol [-o notrackalign] [-g<DynamicDiskGroupName>] repair  
<VolumeName| DriveLetter|<VmName|DrivePath>
```

Repairs a RAID-5 or mirrored volume if its status is Degraded and there is unallocated space on another dynamic disk. The command repairs the

damaged part of the volume by placing a functional replacement of that subdisk on another disk. The following attributes apply:

<code>-o notrackalign</code>	Disable track alignment on the destination disk.
<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1Volume1</code> .
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support track alignment.

Example

```
vxvol repair J:
```

This command repairs a RAID-5 volume (designated as J:) after a disk that belongs to the RAID set has failed.

```
vxvol set fastresync=on|off
```

```
vxvol [-o notrackalign] [-g<DynamicDiskGroupName>] set  
fastresync=on|off <VolumeName | DriveLetter |<VmName|DrivePath>
```

Turns FastResync on or off for the specified mirrored volume. The following attributes apply:

<code>-o notrackalign</code>	Disable track alignment on the disk where the log resides. Applicable when <code>fastresync=on</code> .
<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.

<i><VmName></i>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1Volume1</code> .
<i><DrivePath></i>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

FastResync is not supported on RAID-5 volumes. If you have initiated a snapshot operation on a volume, you cannot turn FastResync off for that volume. If you try to do so, the command line interface returns an error message.

When you turn FastResync on, a DCO (disk change object) log volume is created. When you turn FastResync off, the DCO log volume is deleted. You can perform a limited number of operations on a DCO log volume.

For more information, see the following topics:

- [“FastResync”](#) on page 570
- [“Disk change object \(DCO\) volume”](#) on page 572.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support track alignment.

Examples

```
vxvol set fastresync=on J:
```

This command turns on the FastResync feature on the volume with drive letter J.

```
vxvol set fastresync=on  
\Device\HarddiskDMVolumes\DynDskGrp1  
\Volume1
```

This command turns on the FastResync feature for Volume 1, which belongs to DynDskGrp1.

```
vxvol reactivate
```

```
vxvol [-g<DynamicDiskGroupName>] reactivate <VolumeName |  
DriveLetter |<VmName|DrivePath>
```

Manually restarts the volume. You need to rescan and then reactivate the disk before attempting to reactivate the volume.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxvol reactivate` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name parameter.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1.</code>
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1Volume1.</code>
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

For information on the CLI version of the **Rescan** command and the **Reactivate** (a disk) command, see the following topics:

- “[vxassist rescan](#)” on page 372
- “[vxdisk reactivate](#)” on page 334

Example

```
vxvol reactivate J:
```

This command reactivates the volume with drive letter J.

```
vxvol rdpol prefer
vxvol [-g<DynamicDiskGroupName>] rdpol prefer <VolumeName |
DriveLetter |<VmName|DrivePath> <PlexName>
```

Sets the volume read policy on a volume with multiple mirrors to designate a specific plex to be used for reads. This plex is referred to the “preferred plex.”

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxvol rdpol prefer` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name parameter.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1Volume1</code> .
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<code><PlexName></code>	Name or GUID of the desired preferred plex. A GUID is a unique internal number assigned to the plex. To determine the GUID for a given plex, use the command <code>vxvol volinfo</code> for the mirrored volume that contains the plex.

Designating a plex as preferred can improve your system’s read performance if the drive used for the target mirror is a high-performance drive or if the target mirror is located on a drive that is physically closer.

Note: When a preferred plex has an error, the read operation is completed by another plex. This happens automatically, as if there were no preferred plex.

Example

```
vxvol rdpol prefer J: Volume1-01
```

This command designates plex Volume1-01 as the preferred plex on mirrored volume J.

```
vxvol rdpol round  
vxvol [-g<DynamicDiskGroupName>] rdpol round <VolumeName |  
DriveLetter |<VmName|DrivePath>
```

Sets the volume read policy on a volume with multiple mirrors to read from each plex sequentially in a “round-robin” fashion. Sequential access causes only one plex to be accessed at a time. This takes advantage of the drive or controller read-ahead caching. The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name parameter.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1Volume1</code> .
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Example

```
vxvol rdpol round J:
```

This command sets up the mirrors of volume J to be read in a round-robin fashion.

vxvol growfs

```
vxvol [-g<DynamicDiskGroupName>] growfs <VolumeName |
DriveLetter | <VmName | DrivePath> [<length>]
```

Grows the file system if a volume is resized but the file system fails to resize correctly. If the optional parameter [<length>] is not used, the command would try to grow the file system size to the full volume size. The following attributes apply:

-g<DynamicDiskGroupName>	Needed only if you are using the internal volume name parameter.
<VolumeName>	The path name of the volume, such as \Device\HarddiskDmVolumes\DG1\Volume1.
<DriveLetter>	The drive letter of the volume.
<VmName>	Internal name of the volume; requires the use of the -g option, such as -gDG1Volume1.
<DrivePath>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<length>	Size of the volume in MB. If no size is indicated, the volume is grown to the maximum size.

Note: Any growth is limited to a maximum of 2 TB every time this command is run. The file system usable space is in general somewhat smaller than the raw volume size, since the file system itself occupies space. Only use this command when you see a large difference between the volume size and the file system capacity.

Example

```
vxvol growfs J: 1000
```

This command would grow the file system size of volume J by 1 GB.

```
vxvol growfs J:
```

This command would grow the file system size of volume J to the full volume size.

vxvol access

```
vxvol [-g<DynamicDiskGroupName>] [-f ]
access readonly|readwrite <VolumeName | DriveLetter
| <VmName| DrivePath>
```

Sets the read/write access mode of a volume. The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name parameter.
<code>[-f]</code>	The force option forces the volume to the specified access mode.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1Volume1</code> .
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Example

```
vxvol access readwrite E:
```

This command sets volume E to read/write access.

vxvol reclaim

```
vxvol [-g<DynamicDiskGroupName>] [-b]
reclaim<VolumeName|DriveLetter|VmName|DrivePath>
```

Reclaim storage space from a volume. (Portion of volume must reside on a thin provisioned disk.)

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Name of dynamic disk group. (Needed only if you are using the internal disk name of the volume.)
<code>-b</code>	Run the command in the background.
<code>VolumeName</code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code>
<code>DriveLetter</code>	Drive letter of the volume.

VmName	The internal disk name of the volume, which requires the -g option (for example, -gDG1 Volume2).
DrivePath	Drive path that the volume is mounted on. (Must be an empty folder on a local NTFS volume.)

Note: The operation to reclaim storage from thin provisioned disks is not supported for RAID-5 volumes.

Note: The reclaim storage operation is disabled during a shrink volume operation. The reclaim storage operation is enabled when the shrink volume operation has completed.

Example

```
vxvol -gDG1 reclaim Volume1
```

This command reclaims space from volume with internal name Volume1.

vxvol reclaimcancel

```
vxvol [-g<DynamicDiskGroupName>]
```

```
reclaimcancel<VolumeName|DriveLetter|VmName|DrivePath>
```

Immediately cancels the reclaim operation. Only a portion of the storage space of the volume may have been reclaimed.

The following attributes apply:

-g<DynamicDiskGroup upName>	Name of dynamic disk group. (Needed only if you are using the internal disk name of the volume.)
VolumeName	The path name of the volume, such as <pre>\Device\HarddiskDmVolumes\DG1\Volume1</pre>
DriveLetter	Drive letter of the volume.
VmName	The internal disk name of the volume, which requires the -g option (for example, -gDG1 Volume2).
DrivePath	Drive path that the volume is mounted on. (Must be an empty folder on a local NTFS volume.)

Example

```
vxvol reclaimcancel F:
```

This command immediately cancels the reclaim operation on volume associated with drive letter F:.

vxvol capacitymonitor

```
vxvol [-g<DynamicDiskGroupName>]
capacitymonitor<VolumeName|DriveLetter|VmName|DrivePath>
enable=<yes|no> [critical=<# of volume capacity>] [warning=<# of
volume capacity>] [pollinginterval=<# of seconds>]
[messageinterval=<# of seconds>] [email=<email address>] [-A
APPLYPOLICYTOFAILOVER]
```

Set threshold on dynamic volume so that when the used disk space on a volume reaches the specified threshold, an alert message is logged.

The following attributes apply:

-g<DynamicDiskGroup upName>	Name of dynamic disk group. (Needed only if you are using the internal disk name of the volume.)
VolumeName	The path name of the volume, such as \Device\HarddiskDmVolumes\DG1\Volume1
DriveLetter	Drive letter of the volume.
VmName	The internal disk name of the volume, which requires the -g option (for example, -gDG1 Volume2).
DrivePath	Drive path that the volume is mounted on. (Must be an empty folder on a local NTFS volume.)
Enable	Enable or disable capacity monitoring.
Critical	Critical threshold. The percentage of volume capacity when SFW reports an error. The default value is 90% of capacity.
Warning	Warning threshold. The percentage of volume capacity when SFW logs a warning alert
Email	Notification email address when volume capacity has reached warning/critical threshold.
PollingInterval	Polling interval for checking capacity. The polling interval is the interval of time, in seconds, at which Storage Foundation for Windows checks volume capacities. The default value is 20 seconds.

MessageInterval Minimum time between alerts. To keep the event log file from getting full, you can limit how often an alert message is generated after the warning threshold is reached for a volume. The default is 100 seconds between messages

-A Make capacity monitoring policy available to another cluster node after a failover.

APPLYPOLICYTOFAILOVER

vxvol autogrow

```
vxvol [-g<DynamicDiskGroupName>]
autogrow<VolumeName|DriveLetter|VmName|DrivePath> enable=<yes|no>
[growby=<length>] [-t tpdiskonly] [maxvolumesize=<#size>]
[email=<email address>] [<alloc_attributes...>]
[<diskname|p#c#t#l#>...] [-A APPLYPOLICYTOFAILOVER]
```

Allows an individual volume to grow (increase capacity) automatically by a specified amount when the used disk space on the volume reaches a certain threshold. The threshold is set by Capacity Monitoring.

The following attributes apply:

-g<DynamicDiskGroup upName>	Name of dynamic disk group. (Needed only if you are using the internal disk name of the volume.)
VolumeName	The path name of the volume, such as \\Device\HarddiskDmVolumes\DG1\Volume1
DriveLetter	Drive letter of the volume.
VmName	The internal disk name of the volume, which requires the -g option (for example, -gDG1 Volume2).
DrivePath	Drive path that the volume is mounted on. (Must be an empty folder on a local NTFS volume.)
Enable	Enable or disable automatic volume growth.
growby	Amount of space that volume is to be expanded each time the growth threshold is reached. Amount of space can be specified in terms of S for Sectors, K for KBs, M for MBs, G for GBs, T for TBs. The default unit of measurement is MBs.
-t tpdiskonly	Specify for only thin provisioned disks.

maxvolumesize	Maximum volume size. Limit volume growth to a maximum volume size. Maximum volume size can be specified in terms of S for Sectors, K for KBs, M for MBs, G for GBs, T for TBs. The default is unrestricted volume growth.
email	Notification email address when volume capacity has reached warning/critical threshold.
<alloc_attributes...>	Specify allocation attributes for mirror/striped volumes. Attributes are of the form: mirror={diskclass} wantmirror={diskclass} stripe={diskclass} wantstripe={diskclass} [!]{diskclass}:instance
Mirror	Specify the diskclass to use for mirroring.
WantMirror	Specify the diskclass to use for mirroring. This specification is ignored if allocations are not available.
Stripe	Specify that volumes are to be striped across instances of a diskclass.
WantStripe	Specify that volumes are to be striped across instances of a diskclass. This specification is ignored if allocations are not available.
diskclass	Type of disk grouping to be used for mirror/striped. Available types are channel, enclosure, port, or target.
instance	Specify (or exclude) a set of disks. Diskclass instance is a particular type of group of disks.
diskname	Name of the disk, e.g., Harddisk2; or internal disk name (requires use of -g option), e.g., -g MyDg Disk2
p#c#t#l#	Corresponds to the Port, Channel, Target, Lun of a disk.
-A	Make capacity monitoring policy available to another cluster
APPLYPOLICYTOFAILOVER	node after a failover.

vxdg

The `vxdg` utility performs operations relating to dynamic disk groups. The keywords are:

<code>list</code>	Displays a list of the dynamic disk groups on the computer.
<code>dginfo</code>	Displays information about a specified dynamic disk group.
<code>init</code>	Creates a dynamic disk group.
<code>adddisk</code>	Adds a basic disk to a dynamic disk group.
<code>rmdisk</code>	Removes a disk from a dynamic disk group and reverts it back to a basic disk.
<code>import</code>	Imports the specified dynamic disk group on the computer.
<code>deport</code>	Deports the specified dynamic disk group on the computer.
<code>destroy</code>	Deletes the specified dynamic disk group on the computer.
<code>protect</code>	Adds private dynamic disk group protection.
<code>release</code>	Removes private dynamic disk group protection.
<code>upgrade</code>	Upgrades the disk group version to the current version (the default) or the Volume Manager 3.0/3.1 version.
<code>repldisk</code>	Replaces the specified disk by moving all the subdisks to a spare disk.
<code>split</code>	Splits the specified dynamic disk group into two dynamic disk groups.
<code>recover</code>	Recovers a dynamic disk group that fails because of a system crash or other problem during a dynamic disk group split operation.
<code>join</code>	Joins two dynamic disk groups into one larger dynamic disk group.

latestart	Imports diskgroups after system start up to allow more time for storage to become available for applications.
reclaim	Reclaim storage space from thin provisioned disks in a dynamic disk group.
reclaimcancel	Immediately cancel reclaim operation

A dynamic disk group is identified by `-g<DynamicDiskGroupName>`, such as `DynDskGrp1` or by its dynamic disk group ID (DgID). The DgID is an internal number assigned to the disk group. It can be viewed through the `vxdg list` or `vxdg dginfo` command.

A disk that is being added or removed is identified by its `<DiskName>` or by `p#c#t#l#` (where the #s corresponds to the port, channel, target, and LUN of a disk).

In early releases of Volume Manager for Windows, using `vxdg adddisk` to add the first basic disk to a dynamic disk group automatically created the first dynamic disk group (known as the primary dynamic disk group). If you then used `vxdg adddisk` to specify adding a disk to a dynamic disk group with a new name, a secondary dynamic disk group was formed. Starting with Volume Manager 3.0 for Windows 2000, the `vxdg adddisk` command does not automatically create a dynamic disk group by adding a disk. You must use the `vxdg init` command to create a dynamic disk group. The `vxdg adddisk` command now only adds disks to dynamic disk groups that have already been created.

Note: In Volume Manager 3.0 and 3.1 and Veritas Storage Foundation for Windows, the primary dynamic disk group is the dynamic disk group that contains the boot or system disk. It is not necessarily the first dynamic disk group that is created.

Note: In Volume Manager 3.0 and 3.1, occasionally if volumes arrived after commands like `import`, `init`, `addisk`, and `join` are completed, subsequent commands like associating a drive letter might fail. In Veritas Storage Foundation for Windows, these commands will wait until the volumes are ready to be used. If the volumes take a very long time to arrive (a rare case), the command may timeout so that the script will not hang. Users can use `-o timeout=<n>` to override the default timeout.

Typing the following sequence for each keyword brings up a description of its syntax:

```
vxdg <keyword> -?
```

Keywords or operands

```
vxdg list
```

```
vxdg list
```

Returns a list of the dynamic disk groups that are on the current computer. The list includes the disk groups' names, their types, whether each disk group is imported or deported, and the DgID. The dynamic disk group ID (DgID) is an internal number assigned to the disk group. It can be used in place of the dynamic disk group name.

```
vxdg dginfo
```

```
vxdg -g<DynamicDiskGroupName> dginfo
```

Returns information about the dynamic disk group that is referenced in `-g<DynamicDiskGroupName>`. Gives the names and numbers of the volumes and the disks in the dynamic disk group. It also includes the dynamic disk group name, its state (either Imported or Deported), and its dynamic disk group ID. The dynamic disk group ID (DgID) is an internal number assigned to the disk group. It can be used in place of the dynamic disk group name.

Example

```
vxdg -gSalesDynDskGrp dginfo
```

Lists the names and numbers of the volumes and disks in the disk group named "SalesDynDskGrp."

```
vxdg init
```

```
vxdg -g<DynamicDiskGroupName> [-s|-R][-TLDM][-o timeout=<n>]
```

```
init [<medianame>=<DiskName>... | <p#c#t#l#>...
```

```
[basename=<seedname>]
```

Creates a new dynamic disk group with the specified disks.

`-g<DynamicDiskGroupName>` Identifies the dynamic disk group name. A dynamic disk group name is limited to 18 ASCII characters. It should not have any spaces.

`-s` Creates a cluster dynamic disk group.

-R	Creates a private dynamic disk group, that is a disk group with private dynamic disk group protection.
-TLDM	Type of dynamic disk group created is dependent on the version of Windows running on the system. <ul style="list-style-type: none">■ On Windows 2003: Creates a Windows Disk Management compatible dynamic disk group.■ On Windows 2008: Creates a Microsoft Disk Management Disk Group. <hr/> <p>Note: Windows 2008 allows only one Microsoft Disk Management Disk Group and automatically assigns the name of the disk group when it is created. Specifying the <code>-TLDM</code> option with the name of the disk group with the <code>-g <diskgroupname></code> attribute results in an error.</p> <hr/>
-o timeout=<n>	Allows the operation to timeout in <n> seconds.
<medianame>	Internal disk name specified by user. <p>Note: Only ASCII characters are allowed.</p>
<DiskName>...	The name of the disk or disks, which can be specified by the device name (such as <code>Harddisk2</code>).
<p#c#t#l#>...	Another way to indicate a disk name; the #s correspond to port, channel, target, and LUN of the disk.
<seedname>	A name that when appended with a system-generated number becomes the internal identifier of the disk. <p>Note: Only ASCII characters are allowed.</p>

There can be one or more disks in a dynamic disk group. Disks within a dynamic disk group share a common configuration. Dynamic volumes are

created within a dynamic disk group and are restricted to using disks within that group.

You can use this command to create a cluster dynamic disk group, a private dynamic disk group, a Windows Disk Management compatible dynamic disk group, or a Microsoft Disk Management Disk Group.

See “[About disk groups](#)” on page 194.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support cluster disk groups.

Examples

```
vxdg -gSharedDg1 init -s -TLDM Harddisk0 Harddisk1
```

On Windows 2003, this command creates a new cluster dynamic disk group called SharedDg1. The cluster dynamic disk group is Windows Disk Management compatible. The dynamic disk group includes Harddisk0 and Harddisk1.

```
vxdg -gProtectedDg init -R -TLDM Harddisk0 Harddisk1
```

This command creates a new private dynamic disk group called ProtectedDg.

- On Windows 2003, a Windows Disk Management compatible dynamic disk group is created. The dynamic disk group includes Harddisk0 and Harddisk1.
- On Windows 2008, an error occurs because the dynamic disk group is specified.

```
vxdg init -TLDM Harddisk5
```

On Windows 2008, this command creates a Microsoft Disk Management Disk Group. The dynamic disk group includes Harddisk5.

```
vxdg -gDG1 init mediaName1=Harddisk1  
mediaName2=Harddisk2 Harddisk3 Harddisk4
```

This command creates a new dynamic disk group called “DG1”. The dynamic disk group includes Harddisk1, Harddisk2, Harddisk3, And Harddisk4 and the names mediaName1 and mediaName2 area assigned to Harddisk1 and Harddisk2 respectively.

vxdg adddisk

```
vxdg -g<DynamicDiskGroupName> [-o timeout=<n>] adddisk
[<medianame>=<DiskName>... | <p#c#t#l#>...
[basename=<seedname>]
```

Adds one or more basic disks that are referenced in <DiskName>... | <p#c#t#l#>... to the dynamic disk group referenced in -g<DynamicDiskGroupName>. The following attributes apply:

-g<DynamicDiskGroupName>	The name of the disk group that the disk is being added to.
-o timeout=<n>	Allow the operation to timeout in <n> seconds.
<medianame>	Internal disk name specified by user. Note: Only ASCII characters are allowed.
<DiskName>...	The name of the disk or disks, which can be specified by the device name (such as Harddisk2).
<p#c#t#l#>...	Another way to indicate a disk name; the #s correspond to port, channel, target, and LUN of the disk.
<seedname>	A name that when appended with a system-generated number becomes the internal identifier of the disk. Note: Only ASCII characters are allowed.

The ellipses indicate that you can specify more than one disk.

You can no longer create a dynamic disk group implicitly by using a different dynamic disk group name. Dynamic disk group creation and all the options associated with the operation are now done through vxdg init instead.

Examples

```
vxdg -gSalesDynDskGrp adddisk Harddisk4
```

Adds Harddisk4 to SalesDynDskGrp.

```
vxdg -gclustr_dyndskgrp1 adddisk Harddisk5
```

Adds Harddisk5 to the cluster dynamic disk group clustr_dyndskgrp1.

vxdg rmdisk

```
vxdg [-g<DynamicDiskGroupName>] [-f] rmdisk <DiskName> |
p#c#t#l#>
```

Reverts a disk that is referenced in <DiskName> | <p#c#t#l#> from a dynamic disk to a basic disk. <DiskName> can be the disk name or path

name of the device, such as `Harddisk2` or `\Device\Harddisk2`. The disk must not contain any volumes when it is reverted. The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	The name of disk group that the disk is being removed from.
<code>-f</code>	Forces the command; use this option with caution.
<code><DiskName></code>	The disk name of the disk being reverted, which can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG2 Disk2</code>).
<code>p#c#t#l#</code>	Another way to indicate a disk name; the <code>#s</code> correspond to port, channel, target, and LUN of the disk.

Example

```
vxdg rmdisk Harddisk2
```

Reverts `Harddisk2` to a basic disk.

```
vxdg import
vxdg -g<DynamicDiskGroupName> [-n<NewDynamicDiskGroupName>]
[-s|-d] [-f] [-C] [-o timeout=<n>] import
Imports the dynamic disk group referenced in
-g<DynamicDiskGroupName> for use on this computer. You can use its
name from the original computer or rename it with
-n<NewDynamicDiskGroupName>.
```

Note: Microsoft Disk Management Disk Groups do not support the `vxdg import` command.

The following attributes apply:

- | | |
|--------------------------|---|
| -g<DynamicDiskGroupName> | The name of the disk group that is being imported. |
| -s | Imports the disk group as a cluster disk group. Using this command with the <code>-s</code> option is the only way you can convert a regular secondary disk group to a cluster disk group.

In VM 3.0 and 3.1, every time an import or deport command is used with a cluster disk group, it is necessary to use the <code>-s</code> option. With SFW, it is only required the first time you create the cluster disk group. |
| -d | Converts a cluster disk group to a regular disk group. |
| -f | Forces the command; use this option with caution. The <code>-f</code> option can be used to force the import of a cluster disk group when a minority of disks in the disk group are available.

See “Unable to bring a cluster disk group online when a minority of the disks in the disk group are available” on page 505. |
| -C | Clears the disk group’s host ID. See more about the host ID below. |
| -o timeout=<n> | The <code>-o timeout=<n></code> option will allow the operation to timeout in <code><n></code> seconds. This is useful for scripting purposes. |

About a Disk Group Host ID

When a dynamic disk group is created or imported, all disks in the dynamic disk group are stamped with the computer's host ID. Typically, a dynamic disk group cannot be imported if any of its disks are stamped with a non-matching host ID. This mechanism provides a check in cases when disks can be accessed from more than one host.

In Volume Manager 3.0 and 3.1 and Veritas Storage Foundation for Windows, if a dynamic disk group is in use by one machine when another machine attempts to import this dynamic disk group again, the import will fail because the host IDs of these two machines are different.

If a dynamic disk group is successfully deported, the host ID is cleared and the group can be safely imported to another machine. In Volume Manager 3.0 and 3.1, it was necessary to use the `-s` option with the import command for a cluster disk group to retain its status as a cluster disk group.

Otherwise, it became a regular disk group after it was imported. With SFW, you do not need the `-s` option. A cluster disk group remains a cluster disk group when it is imported. If you want to change a cluster disk group back to an ordinary disk group, you deport it and then import it with the `-d` option.

To move a dynamic disk group from one machine to another when the dynamic disk group was not cleanly deported (for example, if the host computer crashed), you must specify the `-C` option to clear the original host ID and stamp a new host ID onto the dynamic disk group.

Example

```
vxdg -gDynDskGrp1 -nAcctgDynDskGrp import
```

Imports the dynamic disk group previously known as "DynDskGrp1" and renames it "AcctgDynDskGrp."

```
vxdg deport
vxdg -g<DynamicDiskGroupName> [-f] deport
```

Deposits the dynamic disk group referenced in `-g<DynamicDiskGroupName>` in preparation for its being imported to another computer. Disks and volumes cannot be accessed until the dynamic disk group is imported. The `-f` option forces the deport of the disk group if one or more of its volumes are still in use. Veritas Storage Foundation for Windows does not allow you to deport a cluster disk group that is a VCS or Microsoft Clustering disk group resource.

Note: Microsoft Disk Management Disk Groups do not support the `vxdg deport` command.

Example

```
vxdg -gDynDskGrp1 deport
```

Deposits the dynamic disk group named “DynDskGrp1.”

```
vxdg destroy
vxdg -g<DynamicDiskGroupName> [-f] destroy
```

Deletes the dynamic disk group referenced in `-g<DynamicDiskGroupName>`. The `-f` option forces the delete of the disk group.

Example

```
vxdg -gDynDskGrp1 destroy
```

Deletes the dynamic disk group named “DynDskGrp1.”

```
vxdg protect
vxdg -g<DynamicDiskGroupName> protect
```

Adds private dynamic disk group protection to a secondary dynamic disk group on the current host. Private dynamic disk group protection allows administrators to partition storage and assign exclusive ownership in a SAN or shared disk array.

Note: Microsoft Disk Management Disk Groups do not support the `vxdg protect` command.

Private dynamic disk group protection uses hardware locking techniques to protect a secondary dynamic disk group located on shared storage from access by other hosts connected to the shared storage pool. The hardware locking is implemented by using a SCSI reservation thread to maintain a current reservation for each disk in a protected group.

If disks are being added to a dynamic disk group that has a SCSI reservation, they will get a reservation automatically.

As long as the dynamic disk group remains on the same host, the protection will be enabled, even through reboots. If the dynamic disk group is deported and imported on another host, the private dynamic disk group protection is removed and the command must be redone to restore the protection.

Also, if you uninstall Veritas Storage Foundation for Windows, the dynamic disk group protection information is removed. If you then reinstall Veritas Storage Foundation for Windows and want to restore the dynamic disk group protection, you must redo the command.

See [“Partitioned shared storage with private dynamic disk group protection”](#) on page 209.

Example

```
vxdg -gDynDskGrp2 protect
```

Adds private dynamic disk group protection to DynDskGrp2.

```
vxdg release
```

```
vxdg -g<DynamicDiskGroupName> release
```

Removes private dynamic disk group protection.

Note: Microsoft Disk Management Disk Groups do not support the `vxdg release` command.

Example

```
vxdg -gDynDskGrp2 release
```

Removes private dynamic disk group protection from DynDskGrp2.

```
vxdg upgrade
```

```
vxdg -g<DynamicDiskGroupName> [-T <version>] upgrade
```

Upgrades a dynamic disk group that was originally created on an earlier version of Volume Manager or its related programs to the current Veritas Storage Foundation for Windows dynamic disk group version. The optional `-T <version>` parameter allows you to upgrade a disk group created under Disk Management or earlier versions of Volume Manager for Windows to the Volume Manager 3.0/3.1 disk group version.

Note: Microsoft Disk Management Disk Groups do not support the `vxdg upgrade` command.

In most cases, you'll want to upgrade an existing disk group so that it can take advantage of the dynamic disk group capabilities of Veritas Storage Foundation for Windows.

If you don't plan to make changes to these existing disk groups, you do not have to upgrade them; upgrading them allows you to use additional features that affect a disk group, such as SFW's support for VSS, the Volume Shadow Copy Service feature. SFW incorporates VSS support into FlashSnap. If you plan to use the FlashSnap option with these existing disk groups, then you should upgrade them to the current disk group type.

Note: If you upgrade a disk group to SFW, you will not be able to import it on another server that is running Volume Manager 3.1 or any earlier version of Volume Manager or Disk Management. Once a disk group version is upgraded, it cannot be changed back to a earlier disk group version.

There are five disk group versions:

Version Number	Version Used In:
20	Microsoft Windows Disk Management, Volume Manager for Windows NT, Volume Manager 2.5 and 2.7 for Windows 2000
30	Volume Manager 3.0 and 3.1 for Windows 2000
40	Storage Foundation for Windows 4.0, 4.1, and 4.2
43	Storage Foundation for Windows 4.3
50	Storage Foundation for Windows 5.0 and 5.1

Note: SFW does not allow you to upgrade a dynamic disk group that contains a boot or system volume. It must remain at the Disk Management disk group version level to allow for the fact that the program could be uninstalled and that a system and boot disk group would become inaccessible if it were a higher disk group version.

Examples

```
vxdg -gDynDskGrp1 upgrade
```

Upgrades DynDskGrp1 to the Veritas Storage Foundation for Windows dynamic disk group version.

```
vxdg -gDynDskGrp2 -T30 upgrade
```

Upgrades DynDskGrp2 to the Volume Manager 3.0/3.1 disk group version. DynDskGrp2 has to have been created in Volume Manager 2.7 or an earlier

version of Volume Manager or its related products. You might want to do this if you plan to move a disk group to a server that is running the Volume Manager 3.0 or 3.1.

```
vxdg repldisk
```

```
vxdg [-g<DynamicDiskGroupName>] repldisk <"Missing Disk (disk#)" | DiskName |p#c#t#l#>=<SpareDiskName>
```

Replaces a missing disk specified by "Missing Disk (disk#)" | *DiskName* |p#c#t#l#> moving all the subdisks to the disk specified by <*SpareDiskName*>. The disk specified by <*SpareDiskName*> must be a basic blank disk.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxdg repldisk` command.

The following attributes apply:

- `-g<DynamicDiskGroupName>` This parameter is required only if the internal disk name is used to identify the missing disk.
- `"Missing Disk (disk#)"` Specifies the missing disk. This string represents how the missing disk is identified by the program. Because the string "Missing Disk (disk#)" has spaces, you must use quotation marks around it. The program specifies the (disk#), such as (disk2).
- DiskName* The internal disk name of the missing disk. Requires the use the `-g` option (for example, `-gDG1 Disk2`).
- `p#c#t#l#` Another way to indicate a disk name; the #s correspond to port, channel, target, and LUN.
- `<SpareDiskName>` The name of the replacement disk.

This command is listed under dynamic disk group commands because it applies only to dynamic disks.

Example

```
vxdg repldisk "Missing Disk (disk2)"=Harddisk3
```

This command moves the contents of a missing dynamic disk designated as "Missing Disk (disk2)" to a basic disk, which in this case is Harddisk3. In the process, Harddisk3 becomes a dynamic disk. Active redundant volumes (mirrored and RAID-5) on the replaced disk will be resynchronized automatically after disk replacement.

```
vxdg -gDG1 repldisk Disk2=Harddisk3
```

This is an example of the same command using the internal disk name parameter.

```
vxdg split
```

```
vxdg -g<SourceDynamicDiskGroupName>
```

```
-n<TargetDynamicDiskGroupName>
```

```
[-i] [-f] [-s|-d] [-y] [-v] split [<Object>...]
```

Splits a dynamic disk group into two dynamic disk groups. The disks and volumes that will be in the split-off disk group must be healthy. Also, the volumes that will be in the new disk group must be complete for the command to succeed.

Note: Microsoft Disk Management Disk Groups do not support the `vxdg split` command.

See [“Dynamic disk group split”](#) on page 600.

-g<SourceDynamicDiskGroupName>	Name of the current dynamic disk group.
-n<TargetDynamicDiskGroupName>	Name of the new dynamic disk group.
-i	Makes the new dynamic disk group to be in the Imported state.
-f	Forces the split. Use this command with care.
-s	Makes the new dynamic disk group a cluster dynamic disk group.
-d	Changes the target disk group from a cluster disk group to a regular disk group.
-y	Query for the split closure. See the first example below.
-v	Splits all disks in the dynamic disk group that contain snapshot volumes. Do not use the <Object> parameter when you use this option.

<Object>

Name of a disk or volume, or a drive letter. You can split by either disks or volumes. This option is not needed when using the `-v` option.

The internal volume and disk name can be used. The <DrivePath> parameter is supported for a volume name. Also, a disk can be indicated by the `p#c#t#l#` parameter; the `#s` correspond to port, channel, target, and LUN.

A primary dynamic disk group created in Volume Manager for Windows 3.0, 3.1, or Veritas Storage Foundation for Windows cannot be split because it contains a boot or system drive. If you have dynamic disk groups created in an early release of Volume Manager, you will need to upgrade them to be compatible with Volume Manager 3.0, 3.1, and Veritas Storage Foundation for Windows dynamic disk groups before you can use the `vxdg split` and `join` commands. To do this you use the `vxdg upgrade` command.

See “[vxdg upgrade](#)” on page 312.

By default, the new dynamic disk group is in the Deported state after the split. You can use the `-i` option to have it be in the Imported state. The source dynamic disk group remains in the Imported state.

With the GUI `split` command, if the source disk group is a cluster disk group or a disk group with private dynamic disk group protection, the resulting target disk group will be of the same disk group type. With a CLI `split` command for either of these two disk group types, you must use the `-i` switch. In a CLI `split` operation with either of these disk group types, the target disk group does not assume the disk group type of the source disk group until after the target disk group is imported.

See also “[Dynamic disk group split and join](#)” on page 597.

Note: In Volume Manager 3.0 and 3.1, it was necessary to designate the `-s` switch with every command involving a cluster disk group. Starting with SFW 4.0, you use the `-s` switch only the first time you designate a cluster disk group. The `-d` switch has been added to allow changing a cluster disk group to an ordinary disk group.

Before using dynamic disk group `split` and `join` commands with a cluster on shared storage, you should review the considerations for doing so.

See “[Using dynamic disk group split and join with a cluster on shared storage](#)” on page 609.

Examples

```
vxdg -gDynDskGrp1 -y -nDynDskGrp2 split Harddisk5
Harddisk7
```

This command makes a query to determine whether Harddisk5 and Harddisk7 in a dynamic disk group named “DynDskGrp1” comprise the total disks that are needed to have a dynamic disk group split where all the volumes in the split-off dynamic disk group are complete. Here is the output from the command:

Following is the Closure for the requested Split operation.

Names of the Disks are....

Harddisk7

Harddisk5

Harddisk6

Names of the Volumes are....

\Device\HarddiskDmVolumes\DynDskGrp1\Volume1

\Device\HarddiskDmVolumes\DynDskGrp1\Stripe1

The output indicates that in order to have a successful split, or what is called “split closure,” Harddisk6 must be added. The example of the command to perform the actual split is as follows:

```
vxdg -gDynDskGrp1 -i -nDynDskGrp2 split Harddisk5
Harddisk6 Harddisk7
```

This command results in successfully splitting the dynamic disk group DynDskGrp1 with the target dynamic disk group DynDskGrp2 in the Imported state. The new dynamic disk group has the disks Harddisk5, Harddisk6, and Harddisk7.

The example that follows designates the volumes to be included in a new target disk group. Note the path name that is needed for volumes.

```
vxdg -gDynDskGrp1 -i -nDynDskGrp2 split
```

```
\Device\HarddiskDmVolumes\DynDskGrp1\mirrorvol1
```

```
\Device\HarddiskDmVolumes\DynDskGrp1\mirrorvol2
```

This command results in successfully splitting the dynamic disk group DynDskGrp1 with the target dynamic disk group DynDskGrp2 in the Imported state. The new dynamic disk group contains the volumes

```
\Device\HarddiskDmVolumes
```

```
\DynDskGrp2\mirrorvol1 and \Device\HarddiskDmVolumes
```

```
\DynDskGrp2\mirrorvol2.
```

```
vxdg -gttest -nnew split p1c0t110 p1c0t210
```

This command performs the split operation. The name of the new disk group is “new.” This command shows an example of the use of the `p#c#t#l#` with the `<Object>` parameter.

```
vxdg -gtest -nnew split Disk1 Disk2
```

This command performs the split operation. This example shows the use of the internal disk name with the *<Object>* parameter.

```
vxdg -gtest -nnew split Volume1 Volume2
```

This command performs the split operation. This example shows the use of the internal volume name with the *<Object>* parameter.

```
vxdg -gtest -nnew split L:\Folder
```

This command performs the split operation. This example shows the use of *<DrivePath>* with the *<Object>* parameter.

```
vxdg -gtest -nnew split Volume1 Volume2 -f
```

This command performs the split operation. This example shows the use of the *-f* force option.

```
vxdg recover
```

```
vxdg -g<DynamicDiskGroupName> [-s|-d] recover
```

Recovers a dynamic disk group that fails because of a system crash or other problem during a dynamic disk group split operation. This command is used for manual recovery of a disk group when the disk group requires such recovery. The *-s* option recovers the disk group as a cluster disk group in the Imported state. The *-d* parameter is used to change a cluster disk group to a regular disk group.

More information is available about automatic and manual modes of recovery.

See “[Recovery for the split command](#)” on page 604.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support cluster disk groups.

Example

```
vxdg -gDynDskGrp2 recover
```

Recovers DynDskGrp2 after it failed because of a system crash during a dynamic disk group split operation.

```
vxdg join
vxdg -g<SourceDynamicDiskGroupName>
-n<TargetDynamicDiskGroupName> [-C] [-P] [-o timeout=<n>] join
```

Joins two dynamic disk groups together. If some disks are missing or are not functioning, the join command will fail.

Note: Microsoft Disk Management Disk Groups do not support the `vxdg join` command.

<code>-g<SourceDynamicDiskGroupName></code>	Name of the source dynamic disk group, the dynamic disk group that will be added to the target dynamic disk group. The source dynamic disk group ceases to exist after the join.
<code>-n<TargetDynamicDiskGroupName></code>	Name of the target dynamic disk group, the dynamic disk group that will exist after the join.
<code>-C</code>	Clear Host ID. This parameter should be used when you want to import a disk group from another node and that disk group was not properly deported. A host ID might not be cleared, for example, if the host computer became nonfunctional. When a host ID has not been cleared, SFW will not permit the join without the Clear Host ID override. Use this override with care.
<code>-P</code>	Allow Partial Join. See the explanation of the <code>PartialJoin</code> command: “About partial disk group join” on page 608
<code>-o timeout=<n></code>	Allow the operation to timeout in <code><n></code> seconds. This parameter is useful for scripting.

The disk group type after the join will be the type of the target disk group. For example, if the target disk group before the join had private dynamic disk group protection, the resulting disk group will have private dynamic

disk group protection after the join. Also, a cluster dynamic disk group will not be allowed to be the source group for a join command if the disk group is being monitored by cluster software, such as VCS or Microsoft Clustering (MSCS). However, a cluster disk group can be a target dynamic disk group in a join command.

See also “[Dynamic disk group split and join](#)” on page 597.

Example

```
vxdg -gDynDskGrp2 -nDynDskGrp1 join
```

This command will join DynDskGrp2 back into DynDskGrp1. You can also join dynamic disk groups together that were not originally split apart.

```
vxdg join -gddg -ncdg -o timeout=200 join
```

This command joins the dynamic disk group ddg to dynamic disk group cdg. The example shows the use of the `-o timeout=<n>` parameter.

vxdg reclaim

```
vxdg [-g<DynamicDiskGroupName>] [-b] reclaim
```

```
option=<volumes|freespaces|all>
```

Reclaim storage space from thin provisioned disks in a dynamic disk group.

The following attributes apply:

<code>-g<DynamicDiskGro</code>	Name of dynamic disk group.
<code>upName></code>	
<code>-b</code>	Run the command in the background.
<code>volumes</code>	Reclaim storage space from volumes.
<code>freespaces</code>	Reclaim freespace from disks.
<code>all</code>	Reclaim storage space from volumes and freespace from disks. (Default option.)

Note: The operation to reclaim storage from thin provisioned disks is not supported for RAID-5, DCO, or VVR DCM volumes.

Note: The reclaim storage operation is disabled during a shrink volume operation. The reclaim storage operation is enabled when the shrink volume operation has completed.

Example

```
vxdg -gDG1 reclaim option=freespaces
```

This command reclaims only the freespace of the thin provisioned disks in the DG1 dynamic disk group.

vxdg reclaimcancel

```
vxdg [-g<DynamicDiskGroupName>] reclaimcancel
```

```
option=<volumes|freespaces|all>
```

Immediately cancels the reclaim operation. Only a portion of the storage space of the dynamic disk group may have been reclaimed.

The following attributes apply:

<code>-g<DynamicDiskGroup</code>	Name of dynamic disk group.
<code>upName></code>	
<code>volumes</code>	Reclaim storage space from volumes.
<code>freespaces</code>	Reclaim freespace from disks.
<code>all</code>	Reclaim storage space from volumes and freespace from disks. (Default option.)

Example

```
vxdg -gDG1 reclaimcancel
```

This command immediately cancels the reclaim operation for volumes and freespace of the thin provisioned disks in the DG1 dynamic disk group. (No option is specified, so the default option of volumes and freespace is used.)

```
vxdg lateststart
```

```
vxdg -g<DynamicDiskGroupName> lateststart on|off
```

<code>-g<DynamicDiskGroupName></code>	Name of the dynamic disk group that is made available after system startup.
<code>on</code>	Enables the specified dynamic disk group to be imported after system startup.
<code>off</code>	Disables the specified dynamic disk group from being imported after system startup.

Generally, dynamic (non-cluster) disk groups are automatically imported during system startup. However, some types of storage are not available

during system startup which would cause the import to fail. In a clustered environment, disk groups are imported by the cluster application and do not need to have `vxdg lateststart` enabled.

Specifying `on` in the `vxdg lateststart` command enables the dynamic disk group that is referenced in `-g<DynamicDiskGroupName>` to be imported after system startup by the Veritas DG Delayed Import Service (VxDgDI). VxDgDI can import the dynamic disk group after it is made dependent on the service that controls the storage. This allows the required time for the storage to become available. Applications that rely on storage imported by the VxDgDI service may also need to be made dependent on VxDgDI so that they may proceed when their storage is available. Making the VxDGDI service startup type automatic allows the service to run every time the system is started.

Note: To configure a dependency for iSCSI, use VxDgDI to import the dynamic disk group after it is made dependent on the iSCSI service (MSiSCSI) that controls the storage.

As long as the dynamic disk group remains on the same host, `vxdg lateststart` is enabled, even through reboots. If the dynamic disk group is deported and imported on another host, `vxdg lateststart` must be reenabled on the new host.

Note: For SFW 5.1 or later release, newly created dynamic disk groups that contain iSCSI disks, or existing dynamic disk groups that have iSCSI disks added to them, are automatically configured to be imported after system startup. Using the `vxdg lateststart` command is not required for these dynamic disk groups.

To setup `vxdg lateststart`:

- 1 Edit the Windows registry to make VxDgDI dependent on the service that controls the storage.

Example: The following procedure for Windows Server 2003 makes the VxDgDI dependent on the service that controls the storage.

- a Open the Registry Editor (regedit) to edit the Windows registry.
- b Select the registry key
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VxDgDI`
- c Right-click the `DependOnService` value and select **Modify**.
If the `DependOnService` value does not exist, right-click in an empty space in the right pane of the Registry Editor to bring up a context

menu to create the value. Select **New > Multi-String Value** and name the new value DependOnService. Then right-click the DependOnService value and select **Modify**.

- d In the Edit String dialog that appears, enter the name of the service on a new line below the other entries that appear in the Value Data pane
- e Click **OK** and close the Registry Editor.

- 2 Enter the `vxdg lateststart` command at the command line.

For example

```
vxdg -gDynDskGrp2 lateststart on
```

enables the dynamic disk group “DynDskGrp2” to be imported after system startup.

- 3 Applications that rely on storage imported by the VxDgDI service will have their storage available automatically after the Veritas DG Delayed Import Service completes its startup process. However applications that start as a Windows service, such as Microsoft Exchange, need to be made dependent on the Veritas DG Delayed Import Service with the Windows Registry Editor before their storage is available.

Example: The following procedure for Windows Server 2003 makes the service for Microsoft Exchange (Microsoft Exchange Information Store service) dependent on VxDgDI.

- a Open the Registry Editor (regedit) to edit the Windows registry.
- b Select the registry key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\MSExchangeIS
- c Right-click the DependOnService value and select **Modify**.
If the DependOnService value does not exist, right-click in an empty space in the right pane of the Registry Editor to bring up a context menu to create the value. Select **New > Multi-String Value** and name the new value DependOnService. Then right-click the DependOnService value and select **Modify**.
- d In the Edit String dialog that appears, enter VxDgDI on a new line below the other entries that appear in the Value Data pane.
- e Click **OK** and close the Registry Editor.

vxclus

The `vxclus` utility makes it possible to bring a Microsoft Clustering disk group online on a node with a minority of the disks in the disk group. The `vxclus` utility creates an entry in the Registry that enables the cluster resource to be brought online. Once `vxclus enable` is executed, you can bring the resource online with the Windows Server 2003 Cluster Administrator or with Windows Server 2008 Failover Cluster Management.

With SFW, the `vxclus` utility has added keywords that allow a cluster disk group to reside on the same bus as the cluster node's system and boot disk. These keywords are necessary to support booting from a SAN. Also your hardware array must also have support for booting from a SAN. Refer to your hardware array manufacturer's instructions and the Microsoft web site for more information about booting from a SAN.

Note: The `vxclus` commands are needed only with Microsoft Clustering.

Bringing cluster disk groups online on a node with a minority of the disk group's disks is described in more detail in the following topic:

[“Unable to bring a cluster disk group online when a minority of the disks in the disk group are available”](#) on page 505

The `vxclus` keywords or operands are:

<code>enable</code>	Allows a cluster disk group to be brought online when a minority of disks in the disk group are available.
<code>disable</code>	Disables the capability to bring a cluster disk group online when a minority of disks in the disk group are available.
<code>cleanup</code>	Disables for all cluster disk groups on a node the capability to bring the disk group online when a minority of disks in the disk group are available. The cleanup option is not applicable to the <code>UseSystemBus ON OFF</code> support.
<code>UseSystemBus ON</code>	Sets up the conditions to allow a cluster disk group to be created that can reside on the same bus as the cluster node's system or boot disk.
<code>UseSystemBus OFF</code>	Removes the capability of a creating a cluster disk group that can reside on the same bus as the cluster node's system or boot disk.

Typing the following sequence for each keyword brings up a description of its syntax:

```
vxclus <Keyword> -?
```

Caution: To avoid possible data corruption, make sure that a majority of a disk group's disks do not become available and online on one node while another node with a minority of the disk group's disks also has the disk group online.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxclus` command.

Keywords or operands

```
vxclus enable
```

```
vxclus enable -g<DynamicDiskGroupName> [-p]
```

Enables a designated cluster disk group for force import so that it may be brought online when a minority of disks in the disk group are available. The `vxclus` utility creates an entry in the Windows registry that enables the cluster resource for force import. Once `vxclus enable` is executed, you can bring the resource online with the Windows Server 2003 Cluster Administrator or with Windows Server 2008 Failover Cluster Management. After the resource is brought online, the `vxclus` force import functionality is disabled. However if `-p` is specified, the entry made in the Windows registry is such that the `vxclus` force import functionality remains enabled. This allows persistent force import of the designated cluster disk group so that this resource can always be brought online with the Windows Server 2003 Cluster Administrator or with Windows Server 2008 Failover Cluster Management.

<code>-g<SourceDynamicDiskGroupName></code>	Name of the cluster disk group to be enabled for force import.
<code>-P</code>	Enables persistent force import of the cluster disk group.

Example

```
vxclus enable -gDG2 -p
```

Enables the DG2 cluster disk group to be brought online on a node when a minority of disks in the disk group are available. Also the DG2 clusterdisk group is enabled so that it is always ready to be brought online with the

Windows Server 2003 Cluster Administrator or with Windows Server 2008 Failover Cluster Management.

```
vxclus disable
```

```
vxclus disable -g<DynamicDiskGroupName>
```

Disables the capability to bring the designated cluster disk group online on a node when a minority of disks in the disk group are available. This command is necessary only if you have executed the `vxclus enable` command but have not yet brought the disk group online with the Windows Server 2003 Cluster Administrator or with Windows Server 2008 Failover Cluster Management, and then you decide that you do not want to bring the disk group online.

Example

```
vxclus disable -gDG2
```

Removes from the DG2 cluster disk group the capability to be brought online when a minority of disks in the disk group are available.

```
vxclus cleanup
```

```
vxclus cleanup
```

Disables for all cluster disk groups on a node the capability to bring a disk group online when a minority of disks in the disk group are available. This command is necessary only if you have executed the `vxclus enable` command on multiple cluster disk groups but you have not yet brought the cluster disk groups online with the Windows Server 2003 Cluster Administrator or with Windows Server 2008 Failover Cluster Management and you decide that you do not want to bring these disk groups online.

Example

```
vxclus cleanup
```

On the current cluster node, this command turns off the `vxclus` capability for any cluster disk groups that had this capability enabled.

```
vxclus UseSystemBus ON
```

```
vxclus UseSystemBus ON
```

This command makes the registry changes necessary to allow a dynamic cluster disk group to be created on the same bus as the cluster node's system or boot disk. In previous versions of Volume Manager, the program did not allow this to happen. The reason for making this command available is for users who want to have the boot or system disk and the cluster disk group located on a SAN in order to boot from the SAN.

Caution: If you decide that you want to have a cluster disk group on the same bus as the computer node's system or boot disk and you want to boot from a SAN, then you need to follow the specific instructions of your array manufacturer for booting from a SAN. See the Microsoft Windows Server Knowledge Base article 305547 for details of the considerations involved when booting from a SAN.

Example

```
vxclus UseSystemBus ON
```

Makes it possible to create a cluster disk group on the same bus as the cluster node's system or boot disk.

```
vxclus UseSystemBus OFF  
vxclus UseSystemBus OFF
```

Reverses the `vxclus UseSystemBus ON` command, removing the Registry changes that make it possible to create a cluster disk group that can reside on the same bus as the cluster node's system or boot disk.

Example

```
vxclus UseSystemBus OFF
```

Removes the capability of creating a cluster disk group on the same bus as the cluster node's system or boot disk.

vxdisk

The `vxdisk` utility has commands relating to disks. Its keywords or operands are:

<code>diskinfo</code>	Gives information about a disk.
<code>attach</code>	Connects the disk and enables access to the disk.
<code>detach</code>	Stops disk access and disconnects the disk.
<code>list</code>	Gives information about all disks on a managed server or on a specified disk group.
<code>merge</code>	Merges a foreign disk.
<code>reactivate</code>	Reactivates a disk (restarts a disk).
<code>sig</code>	Places a disk signature on a disk.
<code>convertdisk</code>	Converts the partitioning scheme of a disk to MBR or GPT.
<code>set track</code>	Sets track alignment offset for data storage.
<code>trackaligninfo</code>	Displays track alignment setting for host and track alignment offset and settings for all arrays.
<code>ping</code>	Identifies a physical disk.
<code>reclaim</code>	Reclaim storage space from a thin provisioned disk.
<code>reclaimcancel</code>	Immediately cancel reclaim operation

Each keyword is followed by `<DiskName>`, the name of the disk, which can be indicated by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` disk group option (for example, `-gDG1 Disk2`). Another way to specify a disk is with the `p#C#t#l#` parameter. The `#s` correspond to port, channel, target, and LUN of the disk.

Typing the following sequence for each keyword brings up a description of its syntax:

```
vxdisk <Keyword> -?
```

Keywords or operands

vxdisk diskinfo

```
vxdisk [-g<DynamicDiskGroupName>] diskinfo <DiskName>
```

Provides information on the disk referenced in <DiskName>. The information includes the disk name, the dynamic disk group with which the disk is associated, capacity (indicated as *Length*), disk partition style, free space, device type, port, channel, target ID, LUN, the disk signature, track alignment settings, Thin Provisioning type (ThinNoReclaim or ThinReclaim for thin provisioned disks), etc. If the disk has subdisks associated with it, they will be listed.

The `-g` option is needed only if you use the internal disk name to indicate the disk name (for example, `-gDG1 Disk2`).

Note: Not all manufacturers of thin provisioned disks enable the display of the current provisioned size.

Example

```
vxdisk diskinfo Harddisk2
```

Gives information on Harddisk2.

vxdisk attach

```
vxdisk [-g<DynamicDiskGroupName>] attach <DiskName |  
p#c#t#l# >
```

Attaches a disk that was detached.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxdisk attach` command.

The following attributes apply:

`-g<DynamicDiskGroupName>` This parameter is required only if the internal disk name is used.

`<DiskName>` The internal disk name of the missing disk, which requires the `-g` option (for example, `-gDG1 Disk2`).

`p#c#t#l#` Another way to indicate a disk; the `#s` correspond to port, channel, target and LUN of a disk.

Example

```
vxdisk -gDG1 attach Disk2
```

Attaches a disk, Disk2, to disk group DG1, that was previously detached.

```
vxdisk detach  
vxdisk [-g<DynamicDiskGroupName>] detach <DiskName |  
p#c#t#l#>  
Detaches a disk.
```

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxdisk detach` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	This parameter is required only if the internal disk name is used.
<code><DiskName></code>	The internal disk name of the missing disk, which requires the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
<code>p#c#t#l#</code>	Another way to indicate a disk; the <code>#s</code> correspond to port, channel, target and LUN of a disk.

Example

```
vxdisk -gDG1 detach Disk2  
Detaches a disk, -gDG1 Disk2, that was attached earlier.
```

```
vxdisk list  
vxdisk [-g<DynamicDiskGroupName>] [-v] list  
Lists device name, internal disk name, disk group, disk partition style, size, free space, LUN, status, serial number, ThinProvisioningType (ThinNoReclaim or ThinReclaim for thin provisioned disks), ProvisionedSize (current size of thin provisioned disks), etc. for all the disks on the managed server.  
The -g option limits the list of disks to the specified disk group. The -v (verbose) option displays signature, status, bus type, port, target, channel, LUN, track alignment offset, and track alignment setting information for the disks in the list.
```

Note: Not all manufacturers of thin provisioned disks enable the display of the current provisioned size.

Example

```
vxdisk -gDB1 -v list
```

Gives information on all the disks in the DB1 disk group. The `-v` option includes the signature, status, bus type, port, channel, target, and LUN information.

```
vxdisk merge  
vxdisk -g<DynamicDiskGroupName> merge <DiskName | p#c#t#l#>
```

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxdisk merge` command.

In the GUI, this command is called **Merge Foreign Disk**. If you remove a disk from the server and also remove it in Veritas Storage Foundation for Windows and then decide to reattach it to the server as a member of the same dynamic disk group, you will need to use this command. The command will reinstate the disk to its old status as a member of its former dynamic disk group on that server.

You will also need to use this command if you remove a disk without taking its disk group offline, move the disk to another server, and then attempt to reinstall it in the original server. The command is necessary in this case because the disk has the other server's disk group ID.

See "[Merge foreign disk command](#)" on page 487.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Name of the dynamic disk group.
<code><DiskName></code>	The designated hard disk, which can be specified by the device name (such as <code>Harddisk2</code>).
<code>p#c#t#l#</code>	The #s corresponds to the port, channel, target, and LUN of the disk.

Example

```
vxdisk -gDB1 merge Harddisk3
```

Merges `Harddisk3` back into its former disk group, `DB1`.

```
vxdisk reactivate
vxdisk [-g<DynamicDiskGroupName>] reactivate <"Missing
Disk (disk#)" | DiskName |p#c#t#l#>
Reactivates a disk that has gone offline.
```

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxdisk reactivate` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	This parameter is required only if the internal disk name is used.
<code>"Missing Disk (disk#)"</code>	Specifies the missing disk. This string represents how the missing disk is identified by the program. Because the string <code>"Missing Disk (disk#)"</code> has spaces, you must use quotation marks around it. The program specifies the <code>(disk#)</code> , such as <code>(disk2)</code> .
<code><DiskName></code>	The internal disk name of the missing disk, which requires the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
<code>p#c#t#l#</code>	Another way to indicate a disk; the <code>#s</code> correspond to port, channel, target and LUN of a disk.

Example

```
vxdisk reactivate "Missing Disk (disk2) "
```

Reactivates a disk shown as "Missing Disk (disk2)" that has gone offline. This assumes that the disk was offline and has now come back online.

```
vxdisk set hotreloc
vxdisk [-g<DynamicDiskGroupName>] set hotreloc
<mode=<enable|disable|on|off>>
|<usage=<preferred|secondary|nohotuse|reserved>
<diskname>>
Set hot relocation at the host or disk level.
```

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxdisk set hotreloc` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Specifies the dynamic disk group name.
<code>mode=<enable disable on off></code>	Specifies the mode to set the hot relocation. <ul style="list-style-type: none"> ■ enable: Enable hot relocation at the host level. ■ disable: Disable hot relocation at the host level. ■ on: Enable hot relocation at the disk level. ■ off: Disable hot relocation at the disk level.
<code>usage=<preferred secondary nohotuse reserved></code>	Hot relocation setting at the disk level. <ul style="list-style-type: none"> ■ preferred: Preferred target disk in case of I/O failure. ■ secondary: Target disk used in case of I/O failure if no preferred disk is specified, or no free space available on preferred disks. ■ nohotuse: Does not allow disk to be used for hot relocation. ■ reserved: Does not allow disk to be used for hot relocation or other automatic selection operations.
<code><DiskName></code>	Specifies disk name for hot relocation. (Requires the <code>-g</code> option; for example, <code>-gDG1 Disk2.</code>)

Example

```
vxdisk set hotreloc usage reserved disk2
```

Does not allow disk2 to be used for hot relocation.

```
vxdisk sig
    vxdisk sig "<DiskName> (no signature)"
                |p#c#t#l#> [diskstyle=<MBR|GPT>]
```

Adds a disk signature to a new disk. Because the string "`<DiskName> (no signature)`" has spaces, you must use quotation marks around it.

<code><DiskName></code>	The internal disk name of the disk.
<code>p#c#t#l#</code>	Another way to indicate a disk; the #s correspond to port, channel, target and LUN of a disk.
<code>diskstyle=<MBR GPT></code>	Specifies the disk partitioning scheme. The default is MBR <p>Note: GPT is only available on Windows Server 2003 and later 64-bit systems and on Windows Server 2003 SP1 and later 32-bit systems.</p>

Example

```
vxdisk sig "Harddisk5 (no signature)"
```

Adds a signature to Harddisk5 with a diskstyle of MBR.

```
vxdisk convertdisk
    vxdisk convertdisk <DiskName>
        |p#c#t#l#> [diskstyle=<MBR|GPT>]
```

Converts the disk partitioning scheme to MBR or GPT.

Note: vxdisk convertdisk is only available on Windows Server 2003 and later 64-bit systems and on Windows Server 2003 SP1 and later 32-bit systems.

Note: Only primary partitions are allowed on GPT disks.

<i><DiskName></i>	The internal disk name of the disk.
p#c#t#l#	Another way to indicate a disk; the #s correspond to port, channel, target and LUN of a disk.
diskstyle=<MBR GPT>	Specifies the disk partitioning scheme. If diskstyle is omitted, then a GPT disk is converted to an MBR disk or an MBR disk is converted to a GPT disk.

Example

```
vxdisk convertdisk Harddisk5 diskstyle=MBR
```

Converts the diskstyle of Harddisk5 to MBR.

```
vxdisk set track
    vxdisk [-g<DynamicDiskGroupName>]set track align= <enable
        | disable | yes | no> offset=offset# <[vid=<vendor id>
        pid=<product id>] | <DiskName> |<p#c#t#l#>>
```

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support track alignment.

Sets track alignment offset of data storage for disks connected to the host. When a disk is specified by name or by p#c#t#l#, the track alignment is set for all the disks that match the vendor ID and product ID of the disk. When the vendor ID and the product ID is specified, the track alignment is set for all the disks that match the specified vendor ID and product ID.

This command sets track alignment for all disks connected to the host if no disk or no vendor ID and product ID are specified.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	This parameter is required only if the internal disk name is used.
<code>align</code>	Enable or Disable track alignment. (Yes to enable or No to disable track alignment.)
<code>vid</code>	Vendor ID of storage device.
<code>pid</code>	Product ID of storage device.
<code>offset</code>	Track alignment offset of storage device (Range: 64 - 4096).
<code><DiskName></code>	Name of disk (for example, Harddisk2) or internal disk name (requires the <code>-g</code> option, for example, <code>-gDG1 Disk2</code>).
<code>p#c#t#l#</code>	Another way to indicate a disk; the <code>#s</code> correspond to port, channel, target and LUN of a disk.

Examples

```
vxdisk set track align=enable vid=DGC pid=EMC  
offset=128
```

Enables track alignment and sets offset to 128 for all disks connected to the host with vendor ID matching 'DGC' and product ID matching 'EMC'.

```
vxdisk set track align=enable vid=default pid=default  
offset=64
```

Enables track alignment and sets offset to 64 for all disks connected to the host with vendor ID matching 'default' and product ID matching 'default'. (The 'default' specification refers to those disks that are not explicitly supported by the track alignment feature of SFW. Use the `vxdisk trackaligninfo` command to display which disks are supported by SFW.)

```
vxdisk set track align=enable offset=67 harddisk6
```

Enables track alignment and sets offset to 67 for all disks connected to the host with vendor ID and product ID that match the vendor ID and product ID of `harddisk6`.

```
vxdisk -gdg1 set track align=enable offset=67 disk6
```

Enables track alignment and sets offset to 67 for all disks connected to the host with vendor ID and product ID that match the vendor ID and product ID of disk6 in diskgroup dg1.

```
vxdisk set track align=enable
```

Enables track alignment for all disks connected to the host.

```
vxdisk trackaligninfo
```

```
vxdisk trackaligninfo
```

Displays the track alignment setting for the host and track alignment offset and settings for all arrays (including VID and PID).

Examples

```
vxdisk trackaligninfo
```

Displays the track alignment settings at the host level. Also displays the track alignment offset and track alignment setting for all arrays (identified by vendor ID and product ID).

```
vxdisk ping
```

```
vxdisk [-g<DynamicDiskGroupName>] ping <DiskName | p#c#t#l#>
```

Identifies a physical disk. This command flashes the fault light until you stop the command.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxdisk ping` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	This parameter is required only if the internal disk name is used.
<code><DiskName></code>	The internal disk name of the disk, which requires the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
<code>p#c#t#l#</code>	Another way to indicate a disk; the <code>#</code> s correspond to port, channel, target and LUN of a disk.

Example

```
vxdisk ping -gDG1 Disk2
```

Identifies Disk2 that belongs to disk group DG1.

vxdisk reclaim

```
vxdisk [-g<DynamicDiskGroupName>] [-b] reclaim<DiskName | p#c#t#l#>
```

Reclaims storage space from a thin provisioned disk. The -b (background) option runs the reclaim operation in the background.

The following attributes apply:

-g<DynamicDiskGroupName>	Name of dynamic disk group. (Needed only if you are using the internal disk name of the disk.)
-b	Run the command in the background.
<DiskName>	The DiskName can be the external name or the internal name. <ul style="list-style-type: none"> ■ The external name of the disk (for example, Harddisk2). ■ The internal disk name of the disk, which requires the -g option (for example, -gDG1 Disk2).
p#c#t#l#	Another way to indicate a disk; the #s correspond to port, channel, target and LUN of a disk.

Note: The operation to reclaim storage from thin provisioned disks is not supported for RAID-5, DCO, or VVR DCM volumes.

Note: The reclaim storage operation is disabled during a shrink volume operation. The reclaim storage operation is enabled when the shrink volume operation has completed.

Example

```
vxdisk reclaim Harddisk2 Harddisk3
```

This command reclaims space on the disks with the external names of Harddisk2 and Harddisk3.

vxdisk reclaimcancel

```
vxdisk [-g<DynamicDiskGroupName>] reclaimcancel<DiskName | p#c#t#l#>
```

Immediately cancels the reclaim operation. Only a portion of the storage space of the disk may have been reclaimed.

The following attributes apply:

-g<DynamicDiskGroup Name>	Name of dynamic disk group. (Needed only if you are using the internal disk name of the disk.)
<DiskName>	The DiskName can be the external name or the internal name. <ul style="list-style-type: none">■ The external name of the disk (for example, Harddisk2).■ The internal disk name of the disk, which requires the -g option (for example, -gDG1 Disk2).
p#c#t#l#	Another way to indicate a disk; the #s correspond to port, channel, target and LUN of a disk.

Example

```
vxdisk reclaimcancel Harddisk2 Harddisk3
```

This command immediately cancels the reclaim operation on the disks with the external names of Harddisk2 and Harddisk3.

vxassist

The `vxassist` utility has keywords or operands for creating and changing a volume and for doing operations related to a volume. The keywords are:

<code>make</code>	Creates a dynamic volume.
<code>growby</code>	Extends an NTFS dynamic volume or an unformatted dynamic volume.
<code>shrinkby</code>	Decreases the size of an NTFS dynamic volume or an unformatted dynamic volume.
<code>shrinkabort</code>	Abort the shrink volume before it completes.
<code>mirror</code>	Adds a mirror to an existing volume.
<code>break</code>	Breaks a mirror from an existing volume.
<code>remove</code>	Removes a volume, a mirror, or a log.
<code>delete</code>	Deletes a partition or volume.
<code>shred</code>	Shreds and deletes a volume.
<code>addlog</code>	Adds a log plex to a volume.
<code>prepare</code>	Prepares a volume for a snapshot by adding a mirror to the volume. Note: Either the <code>prepare</code> or <code>snapstart</code> keyword may be used in the CLI, however <code>prepare</code> is recommended.
<code>snapshot</code>	Creates a separate volume from the snapshot mirror.
<code>snapback</code>	Joins the snapshot mirror back to the original volume.
<code>snapclear</code>	Clears the association between the original volume and the snapshot volume, making them separate volumes.
<code>snapabort</code>	Aborts the operation to prepare the snapshot on the original volume.
<code>rescan</code>	Rescans all the storage objects on the computer.
<code>refresh</code>	Refreshes volume, drive letter, and system information.

resetbus	Performs a SCSI bus reset on all SCSI buses.
version	Displays installed version of SFW and the build number.

Windows-Specific Commands

assign	Assigns or changes a drive letter or drive path.
unassign	Removes a drive letter or drive path.
create_part	Creates a primary partition.
create_ext	Creates an extended partition.
create_driv	Creates a logical drive.
e	
delete_ext	Deletes an extended partition.

Typing the following sequence for each keyword brings up a description of its syntax.

```
vxassist <Keyword> -?
```

Keywords or operands

```
vxassist make
  vxassist [-b] [-o notrackalign] -g<DynamicDiskGroupName>
  make [<VolumeName>] <Length> [type={mirror|raid5|stripe}
  [, log]] [<alloc_attributes...>] [Column=<n>] [StripeUnit=<Width>]
  [DriveLetter={A|B|...|Z}|DrivePath=<DrivePath>]
  [[!]<DiskName>...]
```

Creates a volume. The following attributes apply:

-b	Option to run the command in the background. This option is useful for operations that take an extended amount of time, such as adding a mirror or extending a volume.
-o notrackalign	Disable track alignment on the disk where the volume resides.
-g<DynamicDiskGroupName>	Name of the dynamic disk group.

<code><VolumeName></code>	Name of the volume. This is a Veritas Storage Foundation for Windows-specific name that is used for internal processing. The name is limited to 18 ASCII characters. It cannot contain spaces or forward or backward slashes. A period cannot be the first character in the name.
<code><Length></code>	Size of the volume; megabytes is the default. To indicate KB, add K to the number (500K); similarly, add G for GB and T for TB.
<code>type={mirror raid5 stripe}[, log]</code>	Type of volume to be created. Default is a spanned volume. The [, log] argument in <code>type</code> will add a RAID-5 log for a RAID-5 volume or a dirty region logging (DRL) log for a mirrored volume during volume creation.
<code><alloc_attributes></code>	Allocation attributes for mirroring and striping volumes. Attributes are: <ul style="list-style-type: none">■ <code>Mirror=n</code>, {diskclass {[!]diskclass:instance}}■ <code>Wantmirror={diskclass {[!]diskclass:instance}}</code>■ <code>Stripe={diskclass {[!]diskclass:instance}}</code>■ <code>Wantstripe={diskclass {[!]diskclass:instance}}</code>
<code>Mirror=<n></code> or <code>Mirror=<n>, diskclass</code>	Number of mirrors to be created for mirrored volumes. (Default is 2.) Optionally specify a diskclass to use in mirroring. For example, <code>Mirror=2, target</code> specifies that volumes are mirrored between SCSI target addresses. Each mirror can contain disks from any number of instances of the diskclass, but different mirrors cannot use disks from the same instance of the diskclass.
<code>Stripe=diskclass</code>	Volumes are striped across instances of a particular diskclass. For example, <code>Stripe=target</code> specifies that volumes are striped between SCSI target addresses. Each column stripe can contain disks from any number of instances of the diskclass, but different columns cannot use disks from the same instance of the diskclass.

<code>Wantmirror=diskclass</code>	Specifies a diskclass to use in mirroring. However this constraint is ignored if the requested allocation cannot be satisfied.
<code>Wantstripe=diskclass</code>	Volumes are striped across instances of a particular disk class. However this constraint is ignored if the requested allocation cannot be satisfied.
<code>diskclass</code> { [!]diskclass:instance }	Diskclass specifies (or excludes) a particular type of disk grouping. For example, <code>port</code> specifies a group of disks on a port. Instance specifies which grouping. For example, <code>p1</code> specifies a particular grouping of disks. Each type of diskclass has a particular format for specifying instances of the class. Multiple diskclass instances can be specified separated by a space. Diskclass can be one of the following: <ul style="list-style-type: none">- <code>target</code> or <code>t</code> Specifies disks that have the same SCSI target address of the same port. The target is specified in the form <code>p#t#</code>- <code>enclr</code>, <code>e</code>, or <code>enclosure</code> Specifies disks belonging to a particular enclosure.- <code>port</code> or <code>p</code> Specifies disks connected to a particular port.- <code>channel</code> or <code>ch</code> Specifies disks connected to a particular channel.
<code>Column=<N></code>	Number of columns. Required for RAID-5 and striped volumes.
<code>StripeUnit=<Width></code>	Stripe width of RAID-5/striped volumes in blocks (512 Kbytes). Allows the user to specify the stripe unit for RAID-5 and striped volumes.
<code>DriveLetter={A B ... Z}</code>	The default is no assignment of a drive letter to the volume.

<code>DrivePath=<DrivePath></code>	Used when you want to mount the new volume at a folder on a local NTFS volume. You can use this attribute as an alternative to the drive letter.
<code>[!]<DiskName>...</code>	<p>Name of a disk or disks to include or exclude, such as Harddisk2. Parameters will be used to specify disks for volume creation, mirroring, and extension.</p> <p>The disk name can also be indicated by the internal disk name or by <code>p#c#t#l#</code>, where the <code>#s</code> correspond to port, channel, target, and LUN of a disk.</p> <p>If disks are not specified, SFW will select the disks automatically within the specified disk group.</p> <p>Note: This attribute is required when working with a Microsoft Disk Management Disk Group.</p>

Note: The default volume type is a concatenated volume. The created volume is not formatted (no file system is created on the volume). You need to use the operating system **format** command to format the volume.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support track alignment.

Examples

```
vxassist -gDG2 make 100 DriveLetter=E Harddisk1
```

The above command line sequence creates a simple 100-MB volume in dynamic disk group DG2. The volume's drive letter is E. The volume would be created on Harddisk1.

```
vxassist -gDG2 make 100 type=mirror,log DriveLetter=F
```

The above command line sequence makes a mirrored 100-MB volume with a DRL log. The volume is assigned the drive letter F.

```
vxassist -gDG2 make 120 type=raid5 DriveLetter=X  
Column=3 Harddisk2 Harddisk3 Harddisk5
```

The above command line sequence creates a 120-MB RAID-5 volume with the drive letter X. The volume is striped across Harddisk2, Harddisk3, and Harddisk5. All RAID-5 volumes require at least three columns. If you do not indicate a column number for a RAID-5 volume, the command will fail.

```
vxassist -b -gDG2 make 100 type=stripe DriveLetter=X
Column=3
```

The above command line sequence makes a striped volume that is assigned drive letter X. The `-b` option allows the command to run in the background.

```
vxassist -gDG2 make DbVolume 100
```

The resulting path name for the volume is:

```
\Device\HarddiskDmVolumes\DG2\DbVolume.
```

```
vxassist -gDG2 make Vol1 100m mirror=2, port
```

The above command line sequence makes a two mirrored 100-MB volumes connected to the same port.

```
vxassist -gDG2 make Vol1 100m mirror=2, port port:p2
port:p3
```

The above command line sequence makes two mirrored 100-MB volumes connected to port:p2 and port:p3.

```
vxassist growby
```

```
vxassist [-b] [-o notrackalign] [-g<DynamicDiskGroupName>]
growby <VolumeName| DriveLetter|VmName|DrivePath> <Length>
[<alloc_attributes...>] [[!]<DiskName>|p#c#t#1#>]...
```

Extends the usable space of an NTFS or unformatted volume by the amount specified in `<Length>`. The following attributes apply:

<code>-b</code>	Runs the command in the background.
<code>-o notrackalign</code>	Disable track alignment on the disk where the volume resides.
<code>-g<DynamicDiskGroupName></code>	Required only if the internal volume name or internal disk name is used.
<code><VolumeName></code>	the path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1.</code>
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1 Volume1.</code>
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<code><Length></code>	The size of the volume; megabytes is the default. To indicate KB, add K to the number (500K); similarly, add G for GB and T for TB.

<code><alloc_attributes></code>	Allocation attributes for mirroring and striping volumes.
	<p>Attributes are:</p> <ul style="list-style-type: none"> ■ Mirror={diskclass {[]diskclass:instance}} ■ Wantmirror={diskclass {[]diskclass:instance}} ■ Stripe={diskclass {[]diskclass:instance}} ■ Wantstripe={diskclass {[]diskclass:instance}}
<code>Mirror=diskclass</code>	Specifies a diskclass to use in mirroring. For example, <code>Mirror=target</code> specifies that volumes are mirrored between SCSI target addresses. Each mirror can contain disks from any number of instances of the diskclass, but different mirrors cannot use disks from the same instance of the diskclass.
<code>Stripe=diskclass</code>	Volumes are striped across instances of a particular diskclass. For example, <code>Stripe=target</code> specifies that volumes are striped between SCSI target addresses. Each column stripe can contain disks from any number of instances of the diskclass, but different columns cannot use disks from the same instance of the diskclass.
<code>Wantmirror=diskclass</code>	Specifies a diskclass to use in mirroring. However this constraint is ignored if the requested allocation cannot be satisfied.
<code>Wantstripe=diskclass</code>	Volumes are striped across instances of a particular disk class. However this constraint is ignored if the requested allocation cannot be satisfied.

<pre>diskclass {[!]diskclass:instance}</pre>	<p>Diskclass specifies (or excludes) a particular type of disk grouping. For example, <code>port</code> specifies a group of disks on a port.</p> <p>Instance specifies which grouping. For example, <code>p1</code> specifies a particular grouping of disks.</p> <p>Each type of diskclass has a particular format for specifying instances of the class. Multiple diskclass instances can be specified separated by a space.</p>
	<p>Diskclass can be one of the following:</p> <ul style="list-style-type: none"> - <code>target</code> or <code>t</code> <p>Specifies disks that have the same SCSI target address of the same port. The target is specified in the form <code>p#t#</code></p> <ul style="list-style-type: none"> - <code>enclr</code>, <code>e</code>, or <code>enclosure</code> <p>Specifies disks belonging to a particular enclosure.</p> <ul style="list-style-type: none"> - <code>port</code> or <code>p</code> <p>Specifies disks connected to a particular port.</p> <ul style="list-style-type: none"> - <code>channel</code> or <code>ch</code> <p>Specifies disks connected to a particular channel.</p>
<pre>Column=<N></pre>	<p>Number of columns. Required for RAID-5 and striped volumes.</p>
<pre>StripeUnit=<Width></pre>	<p>Stripe width of RAID-5/striped volumes in blocks (512 Kbytes). Allows the user to specify the stripe unit for RAID-5 and striped volumes.</p>
<pre>[!]<DiskName>...</pre>	<p>The name of the disk or disks to include or exclude on which the volume will be extended. The disk name can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).</p>
<pre>[!]<p#c#t#l#></pre>	<p>Another way to indicate a disk to include or exclude; the <code>#s</code> correspond to port, channel, target, and LUN of the disk.</p>

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support track alignment.

Examples

```
vxassist growby J: 100
```

The above command extends volume J by 100 MB. Only NTFS or unformatted volumes can be extended. An unformatted volume's file system type is shown as "RAW."

```
vxassist -g mydg growby vol1 100M port:p3 !Harddisk2
```

The above command extends vol1 by 100 MB on disks connected to port p3 excluding Harddisk2.

```
vxassist shrinkby
```

```
vxassist [-b] [-g<DynamicDiskGroupName>] shrinkby  
<VolumeName | DriveLetter | VmName | DrivePath> <Length>
```

Decreases an NTFS or unformatted volume (RAW) by the amount specified in <Length>. The volume must also be unmounted or offline. NTFS volumes greater than 2TB are not supported.

The following attributes apply:

-b	Runs the command in the background.
-g<DynamicDiskGroupName>	Required only if the internal volume name or internal disk name is used.
<VolumeName>	the path name of the volume, such as \\Device\HarddiskDmVolumes\DG1\Volume1.
<DriveLetter>	The drive letter of the volume.
<VmName>	Internal name of the volume; requires the use of the -g option, such as -gDG1 Volume1.
<DrivePath>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<Length>	The amount that the volume decreases; megabytes is the default. To indicate KB, add K to the number (500K); similarly, add G for GB and T for TB.

Note: The shrink volume operation is disabled during a reclaim storage operation for thin provisioned disks. The shrink volume operation is enabled when the reclaim storage operation has completed.

Examples

```
vxassist shrinkby J: 100
```

The above command shrinks volume J by 100 MB. Only NTFS or unformatted volumes are supported by this command. An unformatted volume's file system type is shown as "RAW."

```
vxassist shrinkabort
```

```
vxassist [-g<DynamicDiskGroupName>] shrinkabort  
<VolumeName | DriveLetter | VmName | DrivePath>
```

Aborts a shrink volume operation before it completes. The size of the volume as a result of being cancelled can range from the original size of the volume to the specified smaller volume size. The file system on the volume is preserved even though the shrink volume operation was cancelled.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Required only if the internal volume name or internal disk name is used.
<code><VolumeName></code>	the path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1 Volume1</code> .
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Examples

```
vxassist shrinkabort J:
```

The above command aborts the shrink volume operation on volume J.

```
vxassist mirror
```

```
vxassist [-b][-o notrackalign] [-g<DynamicDiskGroupName>]  
mirror <VolumeName | DriveLetter | VmName | DrivePath> [Type=stripe]  
[<alloc_attributes...>] [Column=<n>] [StripeUnit=<Width>]  
[[!]<DiskName | p##t##l#>...]
```

Adds a mirror to an existing volume. The following attributes apply:

<code>-b</code>	Runs the command in the background.
<code>-o notrackalign</code>	Disable track alignment on the disk where the volume resides.
<code>-g<DynamicDiskGroupName></code>	Required only if the internal volume name or internal disk name is used.
<code><VolumeName></code>	the path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option (for example, <code>-gDG1Volume1</code>).
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<code>Type=<Type></code>	Type of volume layout. Types are: - Stripe - Spanned (Spanned is the default.)
<code><alloc_attributes></code>	Allocation attributes for mirroring and striping volumes. Attributes are: ■ <code>Mirror=n[, {diskclass {[!]<i>diskclass:instance</i>}]</code> ■ <code>Wantmirror={diskclass {[!]<i>diskclass:instance</i>}}</code> ■ <code>Stripe={diskclass {[!]<i>diskclass:instance</i>}}</code> ■ <code>Wantstripe={diskclass {[!]<i>diskclass:instance</i>}}</code>
<code>Mirror=<n></code> or <code>Mirror=<n>, diskclass</code>	Number of mirrors to be created for mirrored volumes. (Default is 2.) Optionally specify a diskclass to use in mirroring. For example, <code>Mirror=2, target</code> specifies that volumes are mirrored between SCSI target addresses. Each mirror can contain disks from any number of instances of the diskclass, but different mirrors cannot use disks from the same instance of the diskclass.

Stripe=diskclass	Volumes are striped across instances of a particular diskclass. For example, Stripe=target specifies that volumes are striped between SCSI target addresses. Each column stripe can contain disks from any number of instances of the diskclass, but different columns cannot use disks from the same instance of the diskclass.
Wantmirror=diskclass	Specifies a diskclass to use in mirroring. However this constraint is ignored if the requested allocation cannot be satisfied.
Wantstripe=diskclass	Volumes are striped across instances of a particular disk class. However this constraint is ignored if the requested allocation cannot be satisfied.
diskclass {[!]diskclass:instance}	<p>Diskclass specifies (or excludes) a particular type of disk grouping. For example, port specifies a group of disks on a port.</p> <p>Instance specifies which grouping. For example, p1 specifies a particular grouping of disks.</p> <p>Each type of diskclass has a particular format for specifying instances of the class. Multiple diskclass instances can be specified separated by a space.</p> <p>Diskclass can be one of the following:</p> <ul style="list-style-type: none"> - target or t Specifies disks that have the same SCSI target address of the same port. The target is specified in the form p#t# - enclr, e, or enclosure Specifies disks belonging to a particular enclosure. - port or p Specifies disks connected to a particular port. - channel or ch Specifies disks connected to a particular channel.

Column=< <i>N</i> >	Number of columns. Required for RAID-5 and striped volumes.
StripeUnit=< <i>Width</i> >	Stripe width of RAID-5/striped volumes in blocks (512 Kbytes). Allows the user to specify the stripe unit for RAID-5 and striped volumes.
[!]< <i>DiskName</i> >...	The name of the disk or disks (such as <code>Harddisk2</code>) on which the mirror or mirrors are to be created. The disk name can also be indicated by the internal disk name, which requires the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
[!]<p#c#t#l#>	Another way to indicate a disk; the #s correspond to port, channel, target, and LUN of a disk.

Caution: Adding mirrors to a volume involves a certain amount of time for mirror resynchronization. Take care not to perform actions on the volume until the command is complete. Also, if you inadvertently shut down the server or deport the disk group containing the volume before mirror resynchronization completes, any mirrors that were being added to the volume will be deleted when the disk group with the volume comes online again.

Note: The SmartMove feature can help reduce mirror resynchronization time. See “[SmartMove](#)” on page 130.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support track alignment.

Example

```
vxassist mirror -b Z: Mirror=2 Harddisk4 Harddisk5
```

The above command line sequence adds two mirrors to volume Z. Harddisk4 and Harddisk5 will be used to create the mirrors. The process of adding the two mirrors will run in the background. Instead of using the drive letter Z, you could provide a path name, such as:

```
\Device\HarddiskDmVolumes\DynDskGrp1\Volume1
```

vxassist break

```
vxassist [-g<DynamicDiskGroupName>] break <VolumeName>
[DriveLetter> <plex=PlexName>|<! Diskname>|!p#c#t#l#>]
[DriveLetter={A|B|...|Z}|DrivePath=<DrivePath>]
```

Breaks a mirror from an existing volume. When a mirror is broken, it becomes a separate volume and you will lose the fault tolerance that mirroring provides.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Required only if the internal volume name or internal disk name is used.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option (for example, <code>-gDG1 Volume1</code>).
<code>plex=<PlexName></code>	The mirror or plex to be broken off. It can be the plex name (such as <code>Volume2-01</code>) or the GUID of the mirror plex. A GUID is a unique internal number assigned to the plex. To determine the GUID for a given plex, use the command <code>vxvol volinfo</code> for the mirrored volume that contains the plex. If you are using a script and have multiple snapshot plexes, then the GUID can distinguish the different snapshot plexes.
<code><! DiskName></code>	The name of the disk, such as <code>Harddisk2</code> , or the internal disk name, which requires the use of the <code>-g</code> option (for example, <code>!-gDG1 Disk2</code>). You can use this attribute as an alternative to the plex name. See the note on the exclamation mark that follows this table.
<code><!p#c#t#l#></code>	Another way to indicate a disk; the <code>#s</code> correspond to port, channel, target, and LUN of the disk. It also requires the <code>!</code> .
<code>DriveLetter={A B ... Z}</code>	Used to assign a specific drive letter to the new volume that is created from the broken-off plex. The drive letter is not automatically assigned.

`DrivePath=<DrivePath>` Used when you want to mount the new volume that is created from the broken-off plex at a folder on a local NTFS volume. You can use this attribute as an alternative to the drive letter.

Note: The exclamation mark in front of the *DiskName* attribute is necessary to make the command compatible with the Volume Manager for UNIX version of the command.

If you do not remember the plex name, you can determine what it is by using the `vxvol volinfo` command. Alternatively, if you know which disk the plex resides on, you can use the `<! DiskName>` syntax, for example, `!Harddisk2`, to specify the plex.

Note: If you want to delete the mirror instead of breaking it off, see the `vxremove` command in the section.

Examples

```
vxassist break H: plex=Volume1-01 DriveLetter=Z
```

The above command line sequence breaks a mirror from a volume that has been assigned the drive letter H. The specified plex becomes a new volume and receives the drive letter Z. The drive letter H is retained by the original volume.

```
vxassist break
\Device\HarddiskDmVolumes\DynDskGrp1\Volume1
plex=Volume1-01 DriveLetter=Z
```

The above command line sequence is the same as the previous command sequence except that a path name, instead of a drive letter, is used to indicate the volume from which the mirror will be broken.

```
vxassist break L: !Harddisk3 DriveLetter=M
```

This breaks off the mirror that resides on Harddisk3 from volume L and assign drive letter M to the newly created volume.

```
vxassist remove
vxassist [-f][-g<DynamicDiskGroupName>] remove
[volume[mirror|log] <VolumeName | DriveLetter | VmName|DrivePath>
[LogType=<DRL|DCM|DCO>] [nlog=<#>]
[plex=<PlexName>|<! Diskname |!p#c#t#l#>]
```

Removes (deletes) either a volume, a mirror from an existing volume, or a DRL or RAID-5 log from an existing volume. When you specify removing a volume, the command works the same as `vxassist delete`. If no volume, mirror, or log is specified, the command assumes a mirror plex for

backward compatibility because the command formerly removed only a mirror plex.

The following attributes apply:

<code>-f</code>	Force the operation.
<code>-g<DynamicDiskGroupName></code>	Required only if the internal volume name or internal disk name is used.
<code>volume[mirror log]</code>	Specifies what is to be removed from an existing volume. If you do not use this parameter, a mirror will be removed. If you want to remove a volume or a log, you will have to put the <code>volume</code> or <code>log</code> keyword in.
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume to be operated on.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option (for example, <code>-gDG1Volume1</code>).
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<code>LogType</code>	Specify the type of log when removing a log (DCM, DRL or DCO type).
<code>nlog=<n></code>	Specify the number of logs when removing a log. Number of logs. (n>0)
<code>plex=<PlexName></code>	The mirror or plex to be removed. It can be the plex name (such as <code>Volume2-01</code>) or the GUID of the mirror plex. A GUID is a unique internal number assigned to the plex. To determine the GUID for a given plex, use the command <code>vxvol volinfo</code> for the mirrored volume that contains the plex. If you are using a script and have multiple snapshot plexes, then the GUID can distinguish the different snapshot plexes.

<! <i>DiskName</i> >	The name of the disk, such as <code>Harddisk2</code> , or the internal disk name, which requires the use of the <code>-g</code> option (for example, <code>!-gDG1 Disk2</code>). You can use this attribute as an alternative to the plex name. See the note on the exclamation mark that follows this table. If there is more than one mirror or log associated with the volume, you need to indicate either the mirror plex name or log plex name or the disk name.
<!p#c#t#l#>	Another way to indicate a disk; the #s correspond to port, channel, target, and LUN of the disk. It also requires the !.

Note: The exclamation mark in front of the *DiskName* attribute is necessary to make the command compatible with the Volume Manager for UNIX version of the command.

If you do not remember the plex name, you can determine what it is by using the `vxvol volinfo` command. Alternatively, if you know which disk the plex resides on, you can use the `<! DiskName>` syntax, for example, `!Harddisk2`, to specify the plex.

The logs can be either DRL or RAID-5 logs. If you have more than one log, you will need to identify the log plex. You cannot remove a DCO log with this command. A DCO log is added with the command `vxvol set fastresync=on` and deleted with the command `vxvol set fastresync=off`.

See “[vxvol](#)” on page 288 .

Examples

```
vxassist remove Z: plex=Volume1-01
```

The above command line sequence removes a mirror from volume Z. The data on the specified plex will be destroyed and is not recoverable.

```
vxassist remove volume F:
```

The above command line sequence removes volume F. The data on the volume will be destroyed and is not recoverable.

```
vxassist remove log H:
```

The above command line sequence removes a log from volume H.

```
vxassist delete
vxassist [-f] [-g<DynamicDiskGroupName>] delete
<VolumeName | DriveLetter | VmName | DrivePath>
```

Deletes a volume or partition. The following attributes apply:

-f	Force the operation.
-g<DynamicDiskGroupName>	Required only if the <VmName> parameter is used.
>	
<VolumeName>	The path name of the volume, such as \Device\HarddiskDmVolumes\DG1\Volume1.
<DriveLetter>	The drive letter of the volume to be operated on.
<VmName>	Internal name of the volume; requires the use of the -g option (for example, -gDG1Volume1).
<DrivePath>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Examples

```
vxassist delete J:
```

The above command deletes volume J. The command will destroy all data on the volume.

```
vxassist delete
\Device\HarddiskDmVolumes\DynDskGrp1\volume1
```

The above command deletes a volume with the path name:

```
\Device\HarddiskDmVolumes\DynDskGrp1\volume1.
```

```
vxassist shred
vxassist [-f] [-g<DynamicDiskGroupName>] shred
[shredtype=<0|1|2>] <VolumeName | DriveLetter | VmName|DrivePath>
```

Overwrites the entire volume with zeroes and then deletes the volume.
SFW provides the following methods for overwriting the volume.

- 1 Pass algorithm
Overwrites the volume with a pattern of zeroes.
Specified by `shredtype=0`.
- 3 Pass algorithm
The volume is overwritten a total of 3 times. The volume is first overwritten with a pre-selected digital pattern, then overwritten with the binary complement of the pattern. In the last pass, the volume is overwritten with a randomly selected digital pattern. This 3 pass approach is based on the specifications in the US Department of Defense standard 5220.22-M (3).
Specified by `shredtype=1`.
- 7 Pass algorithm
The volume is overwritten a total of 7 times. Each pass consists of overwriting the volume with a randomly selected digital pattern or with the binary complement of the previous pattern. This 7 pass approach is based on the specifications in the US Department of Defense standard 5200.28-STD (7).
Specified by `shredtype=2`.

SFW defaults to the 1 Pass algorithm when `shredtype` is not specified.

Caution: All data in the volume will be lost when you shred it. Make sure that the information has been backed up onto another storage medium and verified, or that it is no longer needed.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxassist shred` command.

The following attributes apply:

- | | |
|---|---|
| <code>-f</code> | Force the operation. |
| <code>-g<DynamicDiskGroupName></code> | Required only if the <code><VmName></code> parameter is used. |
| <code>></code> | |

<code>-shredtype=<0 1 2></code>	Specifies the method to overwrite the volume. <ul style="list-style-type: none"> ■ 0 specifies the 1 Pass algorithm ■ 1 specifies the 3 Pass algorithm ■ 2 specifies the 7 Pass algorithm
<code><VolumeName></code>	The path name of the volume, such as <code>\Device\HarddiskDmVolumes\DG1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume to be operated on.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option (for example, <code>-gDG1Volume1</code>).
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Examples

```
vxassist shred J:
```

The above command shreds volume J.

```
vxassist shred
\Device\HarddiskDmVolumes\DynDskGrp1\volume1
```

The above command shreds a volume with the path name:

```
\Device\HarddiskDmVolumes\DynDskGrp1\volume1.
```

```
vxassist addlog
vxassist [-o notrackalign] [-g<DynamicDiskGroupName>]
addlog
<VolumeName|DriveLetter|VmName|DrivePath>
[LogType=<DRL|DCM|DCO>] [nlog=<n>] [[!]diskclass:instance]
[[!]<DiskName|p#c#t#l#>...]
Adds a DRL, DCM, DCO, or RAID-5 log plex to the volume.
```

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxassist addlog` command.

The following attributes apply:

<code>-o notrackalign</code>	Disable track alignment on the disk where the log resides.
<code>-g<DynamicDiskGroupName></code>	Required only if the internal volume name or internal disk name is used.

<code><VolumeName></code>	The path name of the volume, such as \Device\HarddiskDmVolumes\DG1\Volume1.
<code><DriveLetter></code>	The drive letter of the volume to be operated on.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option (for example, <code>-gDG1Volume1</code>).
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<code>LogType</code>	Type of log to add (DCM, DRL or DCO type).
<code>nlog=<n></code>	Number of logs to add.
<code>[!]diskclass:instance</code>	Specify (or exclude) a set of disks. Diskclass specifies a particular type of disk grouping. For example, <code>port</code> specifies a group of disks on a port. Instance specifies which grouping. For example, <code>p1</code> specifies a particular grouping of disks. Each type of diskclass has a particular format for specifying instances of the class. Multiple diskclass instances can be specified separated by a space.
<code>diskclass</code>	Diskclass can be one of the following: - <code>target</code> or <code>t</code> Specifies disks that have the same SCSI target address of the same port. The target is specified in the form <code>p#t#</code> - <code>enclr</code> , <code>e</code> , or <code>enclosure</code> Specifies disks belonging to a particular enclosure. - <code>port</code> or <code>p</code> Specifies disks connected to a particular port. - <code>channel</code> or <code>ch</code> Specifies disks connected to a particular channel.

[!]<DiskName>...	Specifies the disk or disks to include or exclude. If you do not use this parameter, the program selects the disks. The <i>DiskName</i> parameter can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
[!]<p#c#t#l#>	Another way to indicate a disk; the #s correspond to port, channel, target, and LUN of a disk.

For descriptions of the advanced features of DRL and RAID-5 logging, see the following topic:

[“Dirty region logging \(DRL\) and RAID-5 logging”](#) on page 274.

Example

```
vxassist -g mydg addlog vol1 logtype=DRL port:p2  
!harddisk3
```

Adds a DRL log to vol1 on a disk that is not harddisk3 and is connected to port p2.

```
vxassist prepare
vxassist [-b] [-o notrackalign] [-g<DynamicDiskGroupName>]
prepare <VolumeName| DriveLetter|VmName|DrivePath> [Type=stripe]
[<alloc_attributes...>] [Column=<n>] [StripeUnit=<Width>]
[Plex=<MirrorPlexName> |!]<Diskname> |p#c#t#l#> ...]
```

Adds a snapshot mirror to the volume. It is a mirrored plex of the original volume that is broken off in the snapshot process. You can either add a new snapshot mirror or convert a mirror of the volume that already exists. A snapshot mirror is also referred to as a “snap plex.”

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxassist prepare` command.

The following attributes apply:

Note: Either the `prepare` or `snapstart` keyword may be used in the CLI, however `prepare` is recommended.

<code>-b</code>	Runs the command in the background.
<code>-o notrackalign</code>	Disable track alignment on the disk where the mirror resides.
<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name or internal disk name.
<code><VolumeName></code>	The path name of the volume, such as \Device\HarddiskDmVolumes\DynDskGrp1\ Volume1.
<code><DriveLetter></code>	The drive letter of the existing volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option (for example, <code>-gDG1 Volume1</code>).
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<code>Type=<Type></code>	Type of volume layout. Types are: - Stripe - Spanned (Spanned is the default.)

<code><alloc_attributes></code>	Allocation attributes for mirroring and striping volumes. Attributes are: <ul style="list-style-type: none">■ <code>Mirror={diskclass [!]diskclass:instance}</code>■ <code>Wantmirror={diskclass [!]diskclass:instance}</code>■ <code>Stripe={diskclass [!]diskclass:instance}</code>■ <code>Wantstripe={diskclass [!]diskclass:instance}</code>
<code>Mirror=diskclass</code>	Specifies a diskclass to use in mirroring. For example, <code>Mirror=target</code> specifies that volumes are mirrored between SCSI target addresses. Each mirror can contain disks from any number of instances of the diskclass, but different mirrors cannot use disks from the same instance of the diskclass.
<code>Stripe=diskclass</code>	Volumes are striped across instances of a particular diskclass. For example, <code>Stripe=target</code> specifies that volumes are striped between SCSI target addresses. Each column stripe can contain disks from any number of instances of the diskclass, but different columns cannot use disks from the same instance of the diskclass.
<code>Wantmirror=diskclass</code>	Specifies a diskclass to use in mirroring. However this constraint is ignored if the requested allocation cannot be satisfied.
<code>Wantstripe=diskclass</code>	Volumes are striped across instances of a particular disk class. However this constraint is ignored if the requested allocation cannot be satisfied.

<code>diskclass</code> { <code>!</code> } <code>diskclass:instance</code> }	<p>Diskclass specifies (or excludes) a particular type of disk grouping. For example, <code>port</code> specifies a group of disks on a port.</p> <p>Instance specifies which grouping. For example, <code>p1</code> specifies a particular grouping of disks.</p> <p>Each type of diskclass has a particular format for specifying instances of the class. Multiple diskclass instances can be specified separated by a space.</p> <p>Diskclass can be one of the following:</p> <ul style="list-style-type: none">- <code>target</code> or <code>t</code> Specifies disks that have the same SCSI target address of the same port. The target is specified in the form <code>p##</code>- <code>enclr</code>, <code>e</code>, or <code>enclosure</code> Specifies disks belonging to a particular enclosure.- <code>port</code> or <code>p</code> Specifies disks connected to a particular port.- <code>channel</code> or <code>ch</code> Specifies disks connected to a particular channel.
<code>Column=<N></code>	Number of columns. Required for RAID-5 and striped volumes.
<code>StripeUnit=<Width></code>	Stripe width of RAID-5/striped volumes in blocks (512 Kbytes). Allows the user to specify the stripe unit for RAID-5 and striped volumes.
<code>plex=<MirrorPlexName></code>	Converts a specified mirror plex to a snap plex. It can be the plex name (such as <code>Volume1-01</code>) or the GUID of the mirror plex. A GUID is a unique internal number assigned to the plex. To determine the GUID for a given plex, use the command <code>vxvol -v volinfo</code> for the mirrored volume that contains the plex.

[!]<DiskName>	The designated hard disk to include or exclude, which can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
[!]<p#c#t#l#>	Another way to indicate a disk; the <code>#s</code> correspond to port, channel, target, and LUN of a disk.

If you do not remember the plex name, you can determine what it is by using the `vxvol volinfo` command.

When the snapshot mirror is synchronized with the volume, its state changes to Snap Ready and the prepare the volume for snapshot task exits. For more information on the snap commands, see “[Snapshot commands](#)” on page 577.

Examples

```
vxassist -b prepare E:
```

Runs the prepare the volume for snapshot process on volume E in the background.

```
vxassist prepare E: plex=Volume2-01
```

Runs the prepare the volume for snapshot process on volume E, converting the existing mirror plex, Volume2-01, to a snap plex.

```
vxassist prepare e: plex=volume1-02
```

This command converts the plex named “volume1-02” from a regular mirror to a snapshot plex.

```
vxassist prepare e: harddisk2 harddisk3
```

This command creates a new snap plex on harddisk2 and/or harddisk3. You can indicate more than one disk to be used for the snap plex.

```
vxassist prepare d:\mount1
```

This command adds a snap plex to the volume that is mounted on folder `d:\mount1`.

Note: Either the `prepare` or `snapstart` keyword may be used in the CLI, however `prepare` is recommended.

Note: You should not use the `vxassist break` command to break off a snapshot mirror from its associated volume or the `vxassist remove` command to delete a snapshot mirror. Instead use `vxassist snapshot` to break off a snapshot mirror from the associated volume or use `vxassist snapabort` to delete it.

```
vxassist snapshot
vxassist [-g<DynamicDiskGroupName>] snapshot
<VolumeName|DriveLetter|VmName|DrivePath...>
[plex=<SnapPlexName>|<! DiskName |!p#c#t#l# >]
[access=readonly]
[DriveLetter={A|B|...|Z}]|DrivePath=<DrivePath>]
[<NewVolumeName>]
```

Detaches the snapshot mirror (also called the “snap plex”) and creates a separate volume that is associated with the snapshot mirror.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxassist snapshot` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName ></code>	Needed only if you are using the internal volume name or internal disk name parameter.
<code><VolumeName></code>	The path name of the original volume, such as <code>\Device\HarddiskDmVolumes\DynDskGrp1\Volume1</code> .
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option (for example, <code>-gDG1Volume1</code>).
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<code>plex=<SnapPlexName></code>	Name of the snapshot mirror. It can be the plex name (such as <code>Volume1-01</code>) or the GUID of the mirror plex. A GUID is a unique internal number assigned to the plex. To determine the GUID for a given plex, use the command <code>vxvol -v volinfo</code> for the mirrored volume that contains the plex. You need to specify this attribute only when there is more than one snap plex.

<code><! <i>DiskName</i>></code>	The name of the disk, such as <code>Harddisk2</code> , or the internal disk name, which requires the use of the <code>-g</code> option (for example, <code>!-gDG1 Disk2</code>). See the note below this table on the exclamation mark. You can use <code>! <i>DiskName</i></code> as an alternative to the plex name.
<code><!p#c#t#l#></code>	Another way to indicate a disk; the <code>#s</code> correspond to port, channel, target, and LUN of the disk. It also requires the <code>!</code> .
<code>access=readonly</code>	Sets the new volume to read only access.
<code>DriveLetter={A B ... Z}</code>	Used to assign a specific drive letter to the new volume.
<code>DrivePath=<<i>DrivePath</i>></code>	Used to assign a drive path to the new volume.
<code><<i>NewVolumeName</i>></code>	The name of the volume that is created when the snapshot mirror is broken off. This is also referred to as the <i>SnapVolumeName</i> parameter.

Examples

`vxassist snapshot E: access=readonly DriveLetter=H`
This command detaches a snapshot mirror from volume E. The snapshot volume will be volume H with read only access.

`vxassist snapshot E: plex=volume1-02 DrivePath=C:\ABC BackupVolume`

This command detaches the snapshot mirror, `volume1-02`, from volume E, and mounts the new volume called “BackupVolume” to an empty folder called “ABC” on the C drive. The device path of the new volume is:

`\Device\HarddiskDMVolumes\DynDskGrp1\BackupVolume.`

`vxassist snapshot d:\mp1 snap`

This will snapshot the volume which is mounted at the `d:\mp1` folder and assigns the “snap” name to the snapshot.

`vxassist snapback`

`vxassist [-o resyncfromreplica] [-b] [-f] [-g<DynamicDiskGroupName>] snapback <SnapVolumeName | DriveLetter | VmName | DrivePath>`

Joins the broken plex back to the original volume and resynchronizes the two volumes. By default, the synchronization is done from the original volume to the snapshot mirror.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxassist snapback` command.

The following attributes apply:

<code>-o resyncfromreplica</code>	Reverses the resynchronization, copying data from the snapshot mirror to the original volume
<code>-b</code>	Performs the command in the background.
<code>-f</code>	Forces the snapback. Use this option with care. Make sure the volume is not in use.
<code>-g<DynamicDiskGroupName></code>	Needed only if you are using an internal volume name.
<code><SnapVolumeName></code>	The name of the volume associated with the snapshot plex.
<code><DriveLetter></code>	The drive letter of the snapshot volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1 Volume1</code> .
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Example

```
vxassist snapback H:
```

This command joins the snapshot volume H back to the original volume.

```
vxassist snapback d:\mount1
```

This command will snapback the plex associated with the volume that is mounted on the `d:\mount1` folder.

```
vxassist snapclear
```

```
vxassist -g<DynamicDiskGroupName> snapclear  
<VolumeName | SnapVolumeName | DriveLetter | VmName | DrivePath>  
[plex=<SnapPlexName>] [<SnapshotName>]
```

Clears the association between the original volume and the snapshot volume and makes the snapshot volume and original volume two independent volumes. The `vxassist snapclear` command can be specified only after the `vxassist snapshot` command has been issued. After the `vxassist snapclear` command runs, the snapshot volume becomes an ordinary volume and cannot be snapped back to the original volume.

With SFW, it is possible to do a snapclear operation on the original volume. You might want to clear the original volume in two situations: 1) A snapshot volume is deported to a second host and then deleted on that host, and 2) A snapclear is done on the snap volume but the original volume is offline and later this volume comes online.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxassist snapclear` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Needed if you are using the internal volume name or original volume name.
<code><VolumeName></code>	The name of the original volume.
<code><SnapVolumeName></code>	The name of the volume associated with the snapshot plex, the volume that is broken off through the <code>vxassist snapshot</code> command.
<code><DriveLetter></code>	The drive letter of the snapshot volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1 Volume1</code> .
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.
<code>plex=<SnapPlexName></code>	Name or GUID of the mirror plex.
<code><SnapshotName></code>	Optional name assigned to the snapshot volume.

Examples

```
vxassist snapclear H:
```

This command clears the association between the snapshot volume H and the original volume.

```
vxassist snapclear e: plex=volume1-01
```

This will clear the association of e: (the snapshot volume) with its master volume.

```
vxassist snapclear F: snapvolume01
```

This command will clear the association of master volume (F:) with its snapshot volume named "snapvolume01."

Note: When you are using the `snapback` command to clear the association of the master volume, you must use the `<SnapPlexName>` or the `<Snapshot name>` when referring to the snapshot volume.

```
vxassist snapabort  
vxassist [-o keepplex] [-g<DynamicDiskGroupName>] snapabort  
<VolumeName | DriveLetter> | VmName | DrivePath  
[plex=<SnapPlexName>]
```

Aborts a snapshot mirror plex that has been attached to a volume through a prepare the volume for snapshot operation or a snapback operation by either deleting it or converting it to an ordinary mirror. In cases where the deleted snap plex is the last snap plex and the resulting volume is simple or striped, the `vxassist snapabort` command deletes the DCO log volume also.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxassist snapabort` command.

The following attributes apply:

<code>[-o keepplex]</code>	Converts the snap plex to a mirror plex instead of deleting it.
<code>-g<DynamicDiskGroupName></code>	Needed only if you are using the internal volume name.
<code><VolumeName></code>	The path name of the original volume, such as <code>\Device\HarddiskDmVolumes\DynDskGrp1\ volume1.</code>
<code><DriveLetter></code>	The drive letter of the volume.
<code><VmName></code>	Internal name of the volume; requires the use of the <code>-g</code> option (for example, <code>-gDG1Volume1</code>).
<code><DrivePath></code>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

`plex=<SnapPlexName>` Name of a mirror plex that was created when a prepare the volume for snapshot process began. You would need this only if you already prepared the volume for snapshot previously and you prepare the volume for snapshot again, and thus you have multiple snap plexes and want to abort one of them. A `<SnapPlexName>` can be the plex name (such as `Volume2-01`) or the GUID of the mirror plex. A GUID is a unique internal number assigned to the plex. To determine the GUID for a given plex, use the command `vxvol -v volinfo` for the mirrored volume that contains the plex.

Examples

```
vxassist snapabort E:
```

This command aborts the prepare the volume for snapshot operation on volume E.

```
vxassist -o keepplex snapabort H: plex=Concatvol1-03
```

This command aborts the prepare the volume for snapshot operation on volume H, but it converts the plex `Concatvol1-03` to a volume of the same type as the original volume. The reason the *SnapPlexName* had to be specified is that there were two snap plexes, because the `vxassist prepare` command had been invoked twice on volume H.

```
vxassist snapabort E: plex=volume1-0
```

This command aborts the prepare the volume for snapshot operation on volume E with the designated plex.

```
vxassist rescan
vxassist [-b] rescan
```

Rescans all the storage system objects on the computer, including disks, volumes, and file systems. The `-b` option runs the command in the background.

```
vxassist refresh
vxassist [-b] refresh
```

Refreshes volume, drive letter, and system information. The `-b` option runs the command in the background.

```
vxassist resetbus
vxassist resetbus
```

Performs a SCSI bus reset on all SCSI buses.

```
vxassist version
vxassist version
```

Displays installed version of SFW and the build number.

Windows-specific vxassist commands

```
vxassist assign
vxassist [-f] [-g<DynamicDiskGroupName>] assign <VolumeName
| DriveLetter|VmName|DrivePath>
DriveLetter={A|B|...|Z}|DrivePath=<DrivePath>
```

Assigns or changes a drive letter or drive path for a volume. In the command line interface, if you want a drive letter, you must always assign it. The following attributes are assigned:

-f	Forces the command. Use this option with caution.
-g<DynamicDiskGroupName>	Required only if the internal volume name or the internal disk name is used.
<VolumeName>	The path name of the original volume, such as \Device\HarddiskDmVolumes\DynDskGrp1\Volume1.
<DriveLetter>	The current drive letter of the volume.
<VmName>	Internal name of the volume; requires the use of the -g option (for example, -gDG1Volume1).
<DrivePath>	Existing drive path for the volume.
DriveLetter={A B ... Z}	The drive letter to be assigned.
DrivePath=<DrivePath>	The drive path to be assigned.

For more information on assigning a drive letter or drive path, see the following topics:

- [“Add, change, or remove a drive letter or path”](#) on page 167
- [“Mount a volume at an empty folder \(Drive path\)”](#) on page 170

If the volume already has a drive letter, assigning a drive letter will replace the existing drive letter. In addition, if you assign a drive path to a volume that already has an existing drive letter, the existing drive letter will remain.

Example

```
vxassist assign \Device\HarddiskDmVolumes\DynDskGrp2\
volumel DriveLetter=E:
```

This command assigns drive letter E to \Device\HarddiskDmVolumes\
\DynDskGrp2\volume1.

```
vxassist unassign
vxassist [-f] [-g<DynamicDiskGroupName>] unassign
<VolumeName | DriveLetter | VmName> [DrivePath=<DrivePath>]
```

Removes a drive letter or drive path for a volume. The following attributes apply:

-f	Forces the command. Use this option with caution.
-g<DynamicDiskGroupName>	Required only if the internal volume name is used.
<VolumeName>	The path name of the original volume, such as \Device\HarddiskDmVolumes\ DynDskGrp1\ Volume1.
<DriveLetter>	The current drive letter of the volume.
<VmName>	Internal name of the volume; requires the use of the -g option (for example, -gDG1 Volume1).

DrivePath=<DrivePath> The drive path to be unassigned.

More information on unassigning a drive letter or drive path is available in the following topics:

- [“Add, change, or remove a drive letter or path”](#) on page 167
- [“Mount a volume at an empty folder \(Drive path\)”](#) on page 170.

If a drive path and a drive letter are not specified, the command will remove the drive letter. If you want to remove the drive path, you must specify it.

Example

```
vxassist unassign E:
```

This command removes drive letter E from the volume.

```
vxassist create_part
vxassist create_part <DiskName |p#c#t#l#> <Length>
[DriveLetter={A|B|...|Z}]DrivePath=<DrivePath>]
```

Creates a primary partition of <Length> megabytes on <DiskName> and optionally assigns either a drive letter or drive path to it. To specify the partition size in KB, add K to the number (500K); similarly, add G for GB and T for TB.

See also [“Create primary and extended partitions”](#) on page 184.

The disk name can also be replaced by the `p#c#t#l#` parameter, where the `#s` correspond to port, channel, target, and LUN of the disk. Note that there is no internal disk name for a basic disk.

Example

```
vxassist create_part Harddisk0 100 DriveLetter=E
```

Creates a primary partition of 100 MB with drive letter E on Harddisk0.

```
vxassist create_ext
```

```
vxassist create_ext <DiskName|p#c#t#l#> <Length>
```

Creates an extended partition of `<Length>` megabytes on `<DiskName>`. To specify the extended partition size in KB, add K to the number (500K); similarly, add G for GB and T for TB. The disk name can be replaced by the `p#c#t#l#` parameter, where the `#s` correspond to port, channel, target, and LUN of the disk.

Example

```
vxassist create_ext Harddisk0 100
```

Creates an extended partition of 100 MB on Harddisk0.

```
vxassist delete_ext
```

```
vxassist delete_ext <DiskName|p#c#t#l#>
```

Deletes the extended partition on `<DiskName>`. In addition, the disk name can be replaced by the `p#c#t#l#` parameter, where the `#s` correspond to port, channel, target, and LUN of the disk.

Example

```
vxassist delete_ext Harddisk0
```

Deletes the extended partition on Harddisk0.

```
vxassist create_drive
```

```
vxassist create_drive <DiskName|p#c#t#l#> <Length>  
[DriveLetter={A|B|...|Z}]
```

Creates a logical drive of `<Length>` megabytes in the extended partition on `<DiskName>`. To specify the logical drive size in KB, add K to the number (500K); similarly, add G for GB and T for TB. The extended partition must have been created first.

See also “[New logical drives](#)” on page 189.

The disk name can also be replaced by the `p#c#t#l#` parameter, where the `#s` correspond to port, channel, target, and LUN of the disk.

Example

```
vxassist create_drive Harddisk0 100 DriveLetter=E
```

Creates a logical drive of 100 MB on Harddisk0. The logical drive has the drive letter E.

There is no separate `delete_part` command. The `vxassist delete` command, which removes a volume, can be used to delete primary partitions or logical drives. The `delete_ext` command is needed since an extended partition does not have a name to be used in the `vxassist delete` command.

vxevac

```
vxevac [-o notrackalign] [-g<DynamicDiskGroupName>]  
<DiskName [p#c#t#l#] [<NewDiskName>]
```

The vxevac utility moves subdisks from the disk specified by <DiskName> to one specified destination disk <NewDiskName>. If no <NewDiskName> argument is specified, any nonvolatile, nonreserved disk in the same dynamic disk group can be used as a destination disk. The destination disk must be in the same dynamic disk group.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the vxevac command.

The following attributes apply:

-o notrackalign	Disable track alignment when moving to destination disk.
-g<DynamicDiskGroupName>	Required only if the internal disk name is used.
<DiskName>	The name of the disk, which can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
p#c#t#l#	Another way to indicate a disk; the #s correspond to port, channel, target, and LUN of the disk.
<i>NewDiskName</i>	Name of the disk to which the subdisks will be moved.

Example

```
vxevac Harddisk0 Harddisk3
```

Moves all the subdisks from Harddisk0 to Harddisk3.

vxunreloc

```
vxunreloc [-g<DynamicDiskGroupName>] [-f] [-n<NewDiskName>]
<DiskName | p#c#t#l#>
```

Reverses the process of hot relocation or evacuation and moves the hot-relocated subdisks back onto the disk that was replaced after a disk failure or onto a new disk.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxunreloc` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Required only if the internal disk name is used.
<code>-f</code>	Unrelocates a subdisk to a different offset if unrelocating to the original offset is not possible.
<i>DiskName</i>	Name of the disk where the hot-relocated subdisks currently reside. The <i>DiskName</i> parameter can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
<code>p#c#t#l#</code>	Another way to indicate a disk name; the <code>#s</code> correspond to port, channel, target, and LUN of the disk.
<code>-n<NewDiskName></code>	Specifies a new disk to unrelocate to. All the subdisks belonging to <code><DiskName></code> will be unrelocated to <code><NewDiskName></code> .

All disks involved in the process must be in the same dynamic disk group.

Example

```
vxunreloc Harddisk0
```

This command unrelocates `Harddisk0`, which had been previously relocated to another hard disk.

See also “[Hot relocation](#)” on page 268.

vxsd

These are commands for moving, splitting, and joining a subdisk.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxsd` command.

The keywords are:

<code>mv</code>	Moves a subdisk.
<code>split</code>	Splits a subdisk.
<code>join</code>	Joins a subdisk.

Typing the following sequence for each keyword brings up a description of its syntax.

```
vxsd <Keyword> -?
```

Use `vxvol volinfo` to display the subdisk names. Use `vxvol -v volinfo` to display the size and offset of the subdisks. The `-g<DynamicDiskGroupName>` option needs to be specified since `<SubDiskName>` is not distinct among different dynamic disk groups.

```
vxsd mv
```

```
vxsd [-o notrackalign] -g<DynamicDiskGroupName> [-f] [-b] mv  
<SubDiskName> [<DiskName | p#c#t#l#>]
```

This command moves the named subdisk to the disk specified by `<DiskName | p#c#t#l#>`. If a disk is not specified, the move operation tries to find free space within the dynamic disk group. The Move Subdisk function can be used for load balancing by moving a subdisk from a heavily accessed disk to a more lightly loaded one.

This command can also be used to move the part of a volume that is on a failed or missing disk to a healthy one. Moving a subdisk for redundant volumes (mirrored or RAID-5) will use the redundant data to recreate the subdisk on the healthy disk. However, for nonredundant volumes (concatenated or striped), the data cannot be recreated and doing a subdisk move will therefore lose data, which could be recovered if the disk can be repaired. Because of this possibility of data loss, Veritas Storage Foundation for Windows normally does not allow you to move the subdisk for nonredundant volumes.

You can disable track alignment for the operation by using the `-o notrackalign` option. You can also force the operation by using the `-f` option if you don't need the data any more or you can no longer recover the

data. By doing so, you will retain the volume structure, but there is no guarantee that the data will be recoverable. The `-b` option performs the command in the background.

Note: Moving a subdisk from one disk to another involves a certain amount of time. The SmartMove feature can help reduce the time for this operation. See “[SmartMove](#)” on page 130.

Example

```
vxsd -gDynDskGrp1 mv Disk1-01 Harddisk2
```

This command moves subdisk Disk1-01 to Harddisk2 (belonging to the DynDskGrp1 dynamic disk group).

```
vxsd -gDynDskGrp1 -f mv Disk1-01
```

This command forces the move of subdisk Disk1-01 (which is on a failed disk) to another disk with enough free space.

```
vxsd split
```

```
vxsd -g<DynamicDiskGroupName> -s<Size> split <SubDiskName>
```

Splits a subdisk into two separate subdisks.

The `-s` option is required to specify the `<Size>` in MB of the first of the two subdisks to be created. The second subdisk occupies the remaining space used by the original subdisk.

Example

```
vxsd -gDynDskGrp1 -s100 split Disk3-03
```

This command will split subdisk Disk3-03 into two subdisks, the first of which is 100 MB.

```
vxsd join
```

```
vxsd -g<DynamicDiskGroupName> join <SubDiskName>...
```

Combines two or more existing subdisks into one subdisk. To join subdisks, the subdisks must be contiguous on the same disk.

Example

```
vxsd -gDynDskGrp1 join Disk3-03 Disk3-04
```

In this example, the command joins the two subdisks Disk3-03 and Disk3-04 into a new subdisk called Disk3-05.

vxstat

The `vxstat` utility has keywords and operands for displaying statistics for dynamic disks, dynamic volumes, and subdisks of dynamic volumes. It can also display statistics at specified intervals and for specified numbers of times.

Typing the following sequence brings up a description of its syntax:

```
vxstat <Keyword> -?
```

Keywords or operands

```
vxstat [-g<DynamicDiskGroupName>] [-s] [-d] [-v] [-i<Interval>]
[-c<Count>] [<Object>...]
```

The following attributes apply:

`-g<DynamicDiskGroupName>` Name of the dynamic disk group from which the records will be selected. For example, `-gDynDskGrp1`.

`<Object>...` An object can be a disk or a volume (specified by the volume name or drive letter). If no object is specified, the statistics apply to all the volumes on the managed server. Multiple objects are separated by a space.

`[-s]` Displays statistics for subdisks on the objects specified. If the object specified is a disk, all subdisks on that disk will be selected. If the object specified is a volume, all subdisks on that volume will be selected.

`[-d]` Displays statistics for disks on the objects specified.

`[-v]` Displays statistics for volumes on the objects specified.

`[-i<Interval>]` Displays statistics every `<Interval>` seconds. The default and minimum interval is 5 seconds between instances that the statistics are displayed.

`[-c<Count>]` Stops displaying interval statistics after `<Count>` times.

If the `-i<Interval>` option is specified without the `-c<Count>` option, the statistics will run continuously with the interval specified. If neither the `-i<Interval>` option nor the `-c<Count>` option is specified, the statistics display once.

Summary statistics for each object are displayed in one-line output records, preceded by two header lines. The output line consists of blank-separated fields for the object type and object name.

Statistics Types

The statistics types are as follows:

- **Read Requests/Second**
The number of read requests per second for selected storage objects.
- **Write Requests/Second**
The number of write requests per second for selected storage objects.
- **Read Blocks/Second**
The amount of read request data (in blocks per second) that is processed for selected storage objects. It is the throughput on the read requests made.
- **Write Blocks/Second**
The amount of write request data (in blocks per second) that is processed for selected storage objects. It is the throughput on the write requests made.
- **Average Time/Read Block**
The average time in microseconds that it takes to process a read block from the time a request is made until the data is returned.
- **Average Time/Write Block**
The average time in microseconds that it takes to process a write block from the time a request is made until the data is returned.
- **Queue Depth**
The current number of read and write requests in the queue for selected disks. It does not apply to volumes and subdisks.

You can use these statistics to improve performance on your system.

See “[Statistics overview](#)” on page 519.

Examples

```
vxstat -s
```

Displays statistics for all subdisks on a managed server.

```
vxstat -d Harddisk5 Harddisk6
```

Displays statistics for Harddisk5 and Harddisk6

```
vxstat -s E:
```

Displays statistics for the subdisks of volume E.

```
vxstat -i 10 -c 5 -d
```

Displays 5 sets of statistics at 10-second intervals for all the disks on the managed server.

```
vxstat -d F:
```

Displays statistics for the disks that are associated with volume F.

```
vxstat -v Harddisk5
```

Displays statistics for the volumes that are associated with Harddisk5.

```
vxstat -gDynDskGrp1 -v
```

Displays statistics for all volumes in DynDskGrp1.

```
vxstat -s F: G: H: Harddisk7
```

Displays subdisk statistics for volumes F, G, H, and for Harddisk7.

vxtask

The `vxtask` utility has keywords and operands to give percentage completion information on a task running on a managed server. Disk group and volume options allow you to specify a disk group or volume.

Typing the following sequence brings up a description of its syntax:

```
vxtask <Keyword> -?
```

Keywords or operands

```
vxtask [-g<DynamicDiskGroupName>] [-v<VolumeName | Driveletter |  
VmName>] list
```

The following attributes can apply:

`-g<DynamicDiskGroupName>` Name of the dynamic disk group for which the task information will be displayed. For example, `-gDynDskGrp1`.

`[-v<VolumeName | Driveletter | VmName>]` Displays task information for the specified volume. The `<VolumeName>` is the path name of the volume. The `<VmName>` parameter requires the use of the `-g` option, such as `-gDG1 Volume1`.

By default the information on all the tasks running on the managed server will be displayed unless the `-g` or `-v` options is specified.

Examples

```
vxtask list
```

Displays percentage completion information on all the tasks running on a managed server.

```
vxtask -gDynDskGrp1 list
```

Displays percentage completion information on the tasks relating to the disk group `DynDskGrp1`.

vxedit

The `vxedit` command has keywords to associate a comment with a dynamic diskgroup, disk, volume, plex, or subdisk, or to set an alias for an enclosure. The keywords are:

<code>set comment</code>	Associates a comment with a dynamic diskgroup, disk, volume, plex, or subdisk.
<code>set alias</code>	Set alias for an enclosure.
<code>rename</code>	Changes the name of a volume, plex, or disk media.

Typing the following sequence brings up a description of its syntax:

```
vxedit <Keyword> -?
```

Keywords or operands

```
vxedit [-g<DynamicDiskGroupName>] set comment=<comment>  
[<Object>]
```

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxedit set comment` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Name of the dynamic disk group for which the task information will be displayed. For example, <code>-gDynDskGrp1</code> .
<code><comment></code>	The comment text. The maximum size of comment is 40 bytes.
<code><Object></code>	Can be a dynamic volume, disk, plex, disk media, subdisk, or enclosure. Plex and subdisk require use of the <code>-g</code> option. If no object is specified, the command defaults to dynamic disk group (requires use of the <code>-g</code> option).

This command allows the user to add comments to any dynamic disk group, disk, volume, plex, or subdisk.

Example

```
vxedit set comment=BootDisk Harddisk0
Set the comment field of Harddisk0 to "BootDisk."
```

```
vxedit [-g<DynamicDiskGroupName>]
set alias=<EnclosureNewAlias> <EnclosureName | EnclosureOldAlias>
The following attributes apply:
```

<code>-g<DynamicDiskGroupName></code>	Name of the dynamic disk group for which the task information will be displayed. For example, <code>-gDynDskGrp1</code> .
<code>></code>	
<code><EnclosureNewAlias></code>	New alias name for enclosure.
<code><EnclosureName EnclosureOldAlias></code>	Name of enclosure or old alias of enclosure.

This command allows the user to set an alias for an enclosure.

Example

```
vxedit set alias=ABC1 DEC0
Set the alias for enclosure DEC0 to ABC1.
```

```
vxedit [-g<DynamicDiskGroupName>] rename <OldVolumeName>
<NewVolumeName> [-f] | <OldPlexName> <NewPlexName> |
<OldDMName> <NewDMName>
```

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxedit rename` command.

The following attributes apply:

<code>-g<DynamicDiskGroupName></code>	Name of the dynamic disk group for which the task information will be displayed. For example, <code>-gDynDskGrp1</code> .
<code>></code>	
<code><OldVolumeName></code>	Old name for volume.
<code><NewVolumeName></code>	New name for volume.
<code>-f</code>	Forces the rename of the volume.
<code><OldPlexName></code>	Old name for plex.

<i><NewPlexName></i>	New name for plex.
<i><OldDMName></i>	Old name for disk media.
<i><NewDMName></i>	New name for disk media.

This command allows the user to change the name of a volume, plex, or disk media to a new name.

Example

```
vxedit rename Volume1 VolumeABC  
Rename Volume1 to VolumeABC.
```

vxdmadm

The `vxdmadm` utility provides commands for Dynamic Multi-pathing (DMP DSMs).

The keywords are:

<code>dsminfo</code>	Displays information about the DSM.
<code>arrayinfo</code>	Displays information about an array.
<code>deviceinfo</code>	Displays information about a device (that is, a hard disk in an array).
<code>pathinfo</code>	Provides information about a path.
<code>arrayperf</code>	Displays performance statistics about an array.
<code>deviceperf</code>	Displays performance statistics about a device.
<code>pathperf</code>	Displays performance statistics about the paths connected to a device.
<code>allperf</code>	Displays performance statistics for all paths for all devices.
<code>iostat</code>	Displays I/O statistics for a single disk or for all disks in an array.
<code>cleardeviceperf</code>	Resets the performance I/O statistics of a device.
<code>cleararrayperf</code>	Resets the performance I/O statistics of an array that contains the specified disk.
<code>clearallperf</code>	Resets the performance I/O statistics of all arrays under the control of the DMP DSMs that the specified disk belongs to.
<code>setdsmscsi3</code>	Enables or disables SCSI3 support for the DMP DSMs that controls the specified disk.
<code>setarrayscsi3</code>	Enables or disables SCSI3 support in the registry of the array that contains the specified disk.
<code>setattr dsm</code>	Sets DSM attributes.

setattr array	Sets array attributes.
setattr device	Sets device attributes.
setattr path	Sets path attributes.

For a full explanation of the DMP DSMs software and commands, see the following topic:

- [“Dynamic multi-pathing software”](#) on page 717

Each keyword is followed by the volume name or drive letter. Typing the following sequence for each keyword brings up a description of its syntax:

```
vxdmpadm <Keyword> -?
```

Keywords or operands

```
vxdmpadm dsminfo
vxdmpadm [-g<DynamicDiskGroupName>] dsminfo <DiskName> |
p#c#t#l#>
```

This command displays the DSM name, arrays in the DSM, and the array load balance policy. The *DiskName* parameter can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG1 Disk2`). The `#s` in the `p#c#t#l#` parameter correspond to the port, channel, target, and LUN of a disk.

Example

```
vxdmpadm dsminfo Harddisk5
```

Displays the DSM information in which `Harddisk5` participates.

```
vxdmpadm arrayinfo
vxdmpadm [-g<DynamicDiskGroupName>] arrayinfo <DiskName> |
p#c#t#l#>
```

This command displays the array name, the devices in the array, and the array load balance policy. It also displays the tunable parameters (control timer settings) that affect the testing and failover of paths. The *DiskName* parameter can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG1 Disk2`). The `#s` in the `p#c#t#l#` parameter correspond to the port, channel, target, and LUN of a disk.

Example

```
vxdmpadm arrayinfo Harddisk5
```

Displays the array information for the array in which Harddisk5 participates.

```
vxdmpadm deviceinfo
```

```
vxdmpadm [-g<DynamicDiskGroupName>] deviceinfo <DiskName> |  
p#c#t#l#>...
```

This command displays the device name, the internal disk name, number of paths, status, and load balance policy. The *DiskName* parameter can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG1 Disk2`). The `p#c#t#l#` parameter corresponds to the port, channel, target, and LUN of a disk.

Example

```
vxdmpadm deviceinfo Harddisk5 Harddisk6
```

Displays DMP DSMs related information about Harddisk5 and Harddisk 6.

```
vxdmpadm pathinfo
```

```
vxdmpadm [-g<DynamicDiskGroupName>] pathinfo <DiskName> |  
p#c#t#l#>...
```

This command displays path status, load balance policy, port, target, and LUN along with device name, internal disk name, and number of paths. The *DiskName* parameter can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG1 Disk2`). The `p#c#t#l#` parameter corresponds to the port, channel, target, and LUN of a disk.

Example

```
vxdmpadm pathinfo Harddisk5 Harddisk6
```

Displays path information for Hardisk5 and Harddisk6.

```
vxdmpadm arrayperf
```

```
vxdmpadm [-g<DynamicDiskGroupName>] arrayperf <DiskName> |  
p#c#t#l#>
```

This command displays the date and time of the performance statistics, the array name, all the devices in the array, the paths for each device, and the performance statistics of all the devices in the array. The statistics are grouped by each path that is connected to a device. The *DiskName* parameter can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG1 Disk2`). The `#s` in the `p#c#t#l#` parameter correspond to the port, channel, target, and LUN of a disk.

The performance statistics represent the aggregate workload of the array and include the number of:

- Reads
- Writes
- Bytes read
- Bytes written

Example

```
vxdmpadm arrayperf Harddisk5
```

Displays the performance statistics of the devices in the array in which Harddisk5 participates.

```
vxdmpadm deviceperf
```

```
vxdmpadm [-g<DynamicDiskGroupName>] deviceperf <DiskName> |  
p#c#t#l#>...
```

This command displays the date and time of the performance statistics, the device name, the paths for the device, and the performance statistics of the device. The statistics are grouped by each path connected to the device. The *DiskName* parameter can be specified by the device name (such as Harddisk2) or the internal disk name (such as Disk2). The internal disk name must be preceded by the `-g` option (for example, `-gDG1 Disk2`). The `p#c#t#l#` parameter corresponds to the port, channel, target, and LUN of a disk.

The performance statistics represent the aggregate workload of the device and include the number of:

- Reads
- Writes
- Bytes read
- Bytes written

Example

```
vxdmpadm deviceperf Harddisk6
```

Displays the performance statistics of Harddisk6.

```
vxdmpadm pathperf
```

```
vxdmpadm [-g<DynamicDiskGroupName>] pathperf <DiskName> |  
p#c#t#l#>...
```

This command displays the date and time of the performance statistics, the device name, and the performance statistics of the device. The statistics are grouped by each path connected to the device. The *DiskName* parameter

can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG1 Disk2`). The `p#c#t#l#` parameter corresponds to the port, channel, target, and LUN of a disk.

The performance statistics represent the workload of the paths connected to the device and include the number of:

- Reads
- Writes
- Bytes read
- Bytes written

Example

```
vxdmpadm pathperf Harddisk6
```

Displays the performance statistics of `Harddisk6`.

```
vxdmpadm allperf
```

```
vxdmpadm allperf
```

This command displays performance information of the paths for all devices.

For devices, this includes the following:

- Name of the counter
- Path name
- Device name
- Array name
- Counter value

For path summaries, this includes the following:

- Name of the counter
- Path name
- Array name
- Counter value

```
vxdmpadm iostat  
vxdmpadm [-g<DynamicDiskGroupName>] iostat  
[showdevice|showarray] [interval=#] [count=#]  
<DiskName> | p#c#t#l#>
```

This command displays the I/O statistics for a single disk or for all disks in an array. The statistics can be displayed after a specified number of seconds and for a specified number of times.

The following attributes apply:

showdevice|showarray Display I/O statistics:

- showdevice specifies paths of the disk. (Default is showdevice.)
- showarray specifies all the paths of the array that contains the disk.

interval=# # specifies the amount of time (seconds) between displays of the I/O statistics. (Default value is 5 seconds between displays.)

count=# # specifies the number of times the I/O statistics are displayed. (Default is infinite number of displays.)

<DiskName> The designated disk, which can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG2 Disk1`).

p#c#t#l# The #s correspond to the port, channel, target, and LUN of a disk.

```
vxdmpadm cleardeviceperf  
vxdmpadm [-g<DynamicDiskGroupName>] cleardeviceperf  
<DiskName> | p#c#t#l#>
```

This command resets the performance I/O statistics of a device.
The following attributes apply:

<DiskName> The designated disk, which can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG2 Disk1`).

p#c#t#l# The #s correspond to the port, channel, target, and LUN of a disk.

```
vxdmpadm cleararrayperf  
vxdmpadm [-g<DynamicDiskGroupName>] cleararrayperf  
<DiskName> | p#c#t#l#>
```

This command resets the performance I/O statistics of an array that contains the specified disk.

The following attributes apply:

<DiskName> The designated disk, which can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG2 Disk1`).

p#c#t#l# The #s correspond to the port, channel, target, and LUN of a disk.

```
vxdmpadm clearallperf
vxdmpadm [-g<DynamicDiskGroupName>] clearallperf
<DiskName> | p#c#t#l#>
```

This command resets the performance I/O statistics of all arrays under the control of the DMP DSMs that the specified disk belongs to.

The following attributes apply:

<i><DiskName></i>	The designated disk, which can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG2 Disk1</code>).
<i>p#c#t#l#</i>	The #s correspond to the port, channel, target, and LUN of a disk.

```
vxdmpadm setdsmscsi3
vxdmpadm [-g<DynamicDiskGroupName>] setdsmscsi3
scsi3support=0|1 <DiskName> | p#c#t#l#>
```

This command enables or disables SCSI3 support in the registry of the DMP DSMs that controls the specified disk.

The following attributes apply:

<i>scsi3support=0 1</i>	<ul style="list-style-type: none"> ■ 0 disables SCSI3 support in the DMP DSMs ■ 1 enables SCSI3 support in the DMP DSMs
<i><DiskName></i>	The designated disk, which can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG2 Disk1</code>).
<i>p#c#t#l#</i>	The #s correspond to the port, channel, target, and LUN of a disk.

```
vxdmpadm setarrayscsi3  
vxdmpadm [-g<DynamicDiskGroupName>] setarrayscsi3  
scsi3support=0|1 <DiskName> | p#c#t#l#>
```

This command enables or disables SCSI3 support in the registry of the array that contains the specified disk.

The following attributes apply:

- | | |
|-------------------------------|---|
| <code>scsi3support=0 1</code> | <ul style="list-style-type: none">■ 0 disables SCSI3 support in the DMP DSMs■ 1 enables SCSI3 support in the DMP DSMs |
| <code><DiskName></code> | The designated disk, which can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG2 Disk1</code>). |
| <code>p#c#t#l#</code> | The #s correspond to the port, channel, target, and LUN of a disk. |

```
vxdmpadm setattr dsm
vxdmpadm [-g<DynamicDiskGroupName>] setattr dsm
[loadbalancepolicy=FO|RR|LQ|LB|BP [blockshift=#]]
[primarypath=#]
[testpathretrycount=# scsicmdtimeout=#
kernalsleeptime=# failoverretrycount=#]
<DiskName> | p#c#t#l#>
```

This command sets the load balance policy and primary path of the DSM to which the designated disk belongs. It also allows you to set tunable parameters (control timer settings) that affect the testing and failover of the paths. The following attributes apply:

loadbalancepolicy=FO RR LQ LB BP	Specifies the load balance policy for the DSM where: <ul style="list-style-type: none"> ■ FO specifies Fail Over Only (Active/Passive) ■ RR specifies Round Robin (Active/Active) ■ LQ specifies Dynamic Least Queue Depth ■ LB specifies Least Blocks ■ BP specifies Balanced Path
blockshift=#	# specifies the number of contiguous I/O blocks that are sent along a path to an Active/Active array before switching to the next available path. (Default value is 2048 blocks.)
primarypath=#	# specifies the primary path of the DSM. For example, primarypath=1-1-1 sets path 1-1-1 as the primary path of the DSM.
testpathretrycount=#	# specifies the number of times the testpath routine will retry to test the health of the path. Range: 0 ~ 50 times. Default: 0.
scsicmdtimeout=#	# specifies the amount of time a SCSI command waits for a device to respond to a SCSI command. Default is 30 seconds. Maximum is 120 seconds.

`kernalsleeptime=#` # specifies the interval of time the DMP DSMs kernal waits between attempts to recover a path from an error condition. Default is 200 milliseconds. Maximum is 10000 milliseconds.

`failoverretrycount=#` # specifies the number of times DMP DSMs attempts a failover to another path when the current path fails. Default is 0. Maximum is 50 times.

Note: For DMP DSMs, Failover Retry Count does not apply to the EMC Symmetrix array.

`<DiskName>` The designated disk, which can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG2 Disk1`).

`p#c#t#l#` The #s correspond to the port, channel, target, and LUN of a disk.

Example

```
vxddmpadm setattr dsm loadbalancepolicy=FO
primarypath=1-1-0 scsicmdtimeout=34 Harddisk6
```

Sets the load balance policy of the DSM to Fail Over Only (Active/Passive), the primary path to path 1-1-0, the scsicmdtimeout to 34 seconds.

```
vxddmpadm setattr array
vxddmpadm [-g<DynamicDiskGroupName>] setattr array
[loadbalancepolicy=FO|RR|RS [path#=state#]
|LQ|WP [path#=weight#]|LB|BP [blockshift=#]]
[primarypath=#]
[testpathretrycount=#scsicmdtimeout=#
kernalsleeptime=#failoverretrycount=#]
<DiskName> | p#c#t#l#>
```

This command sets the load balance policy and primary path of the array to which the designated disk belongs. It also allows you to set tunable

parameters (control timer settings) that affect the testing and failover of the paths. The following attributes apply:

<code>loadbalancepolicy=FO</code> <code> RR RS LQ WP LB BP</code>	<p>Specifies the load balance policy for the array where:</p> <ul style="list-style-type: none">■ FO specifies Fail Over Only (Active/Passive)■ RR specifies Round Robin (Active/Active)■ RS specifies Round Robin with Subset■ LQ specifies Dynamic Least Queue Depth■ WP specifies Weighted Paths■ LB specifies Least Blocks■ BP specifies Balanced Path
<code>path#=state#</code>	<p><code>state#</code> specifies either standby (0) or active (1) state of the specified <code>path#</code>. For example, 1-1-1=0 means that path 1-1-1 is assigned a state of standby.</p> <p>(Default state of a path is active (1).)</p>
<code>path#=weight#</code>	<p><code>weight#</code> specifies the weight assigned to the specified <code>path#</code>. For example, 1-1-1=10 means that path 1-1-1 is assigned a weight of 10. The path with the lowest weight indicates the most-favored path for I/O.</p> <p>(Range of values for <code>weight#</code>: 0 - 255.)</p>
<code>blockshift=#</code>	<p><code>#</code> specifies the number of contiguous I/O blocks that are sent along a path to an Active/Active array before switching to the next available path.</p> <p>(Default value is 2048 blocks.)</p>
<code>primarypath=#</code>	<p><code>#</code> specifies the primary path of the array. For example, <code>primarypath=1-1-1</code> sets path 1-1-1 as the primary path of the array.</p>
<code>testpathretrycount=#</code>	<p><code>#</code> specifies the number of times the <code>testpath</code> routine will retry to test the health of the path.</p> <p>Range: 0 ~ 50 times. Default: 0.</p>

`scsicmdtimeout=#` # specifies the amount of time a SCSI command waits for a device to respond to a SCSI command. Range: 30 ~ 120 seconds. Default is 30 seconds.

`kernalsleeptime=#` # specifies the interval of time the DMP DSMs kernal waits between attempts to recover a path from an error condition. Range: 200 ~ 10000 milliseconds. Default is 200 milliseconds.

`failoverretrycount=#` # specifies the number of times the failover routine will retry to failover the path. Range: 0 ~ 50 times. Default: 0.

Note: For DMP DSMs, Failover Retry Count does not apply to the EMC Symmetrix array.

`<DiskName>` The designated disk, which can be specified by the device name (such as `Harddisk2`) or the internal disk name (such as `Disk2`). The internal disk name must be preceded by the `-g` option (for example, `-gDG2 Disk1`).

`p#c#t#l#` The #s correspond to the port, channel, target, and LUN of a disk.

Examples

```
vxddmpadm setattr array loadbalancepolicy=FO
primarypath=2-1-0 testpathretrycount=4 Harddisk6
```

Sets the load balance policy of the array to Fail Over Only (Active/Passive), the primary path to path 2-1-0, the testpathretrycount to 4 times.

```
vxddmpadm setattr array loadbalancepolicy=RR Harddisk6
```

Sets the load balance policy of the array to Round Robin (Active/Active).

```
vxddmpadm setattr device
vxddmpadm [-g<DynamicDiskGroupName>] setattr device
[loadbalancepolicy=FO|RR|RS [path#=state#]
|LQ|WP [path#=weight#]|LB|BP [blockshift=#]]
[primarypath=#] <DiskName> | p#c#t#l#>
```

This command sets the load balance policy and primary path of the device to which the designated disk belongs. The following attributes apply:

<code>loadbalancepolicy=FO</code> <code> RR RS LQ WP LB</code>	<p>Specifies the load balance policy for the device where:</p> <ul style="list-style-type: none">■ FO specifies Fail Over Only (Active/Passive)■ RR specifies Round Robin (Active/Active)■ RS specifies Round Robin with Subset■ LQ specifies Dynamic Least Queue Depth■ WP specifies Weighted Paths■ LB specifies Least Blocks■ BP specifies Balanced Path
<code>path#=state#</code>	<p><code>state#</code> specifies either standby (0) or active (1) state of the specified <code>path#</code>. For example, 1-1-1=0 means that path 1-1-1 is assigned a state of standby. (Default state of a path is active (1).)</p>
<code>path#=weight#</code>	<p><code>weight#</code> specifies the weight assigned to the specified <code>path#</code>. For example, 1-1-1=10 means that path 1-1-1 is assigned a weight of 10. The path with the lowest weight indicates the most-favored path for I/O. (Range of values for <code>weight#</code>: 0 - 255.)</p>
<code>blockshift=#</code>	<p><code>#</code> specifies the number of contiguous I/O blocks that are sent along a path to an Active/Active array before switching to the next available path. (Default value is 2048 blocks.)</p>
<code>primarypath=#</code>	<p><code>#</code> specifies the primary path of the device. For example, <code>primarypath=1-1-1</code> sets path 1-1-1 as the primary path of the device.</p>
<code><DiskName></code>	<p>The designated disk, which can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).</p>
<code>p#c#t#l#</code>	<p>The <code>#s</code> correspond to the port, channel, target, and LUN of a disk.</p>

Example

```
vxdmpadm setattr device loadbalancepolicy=FO
primarypath=1-1-0 Harddisk6
```

Sets the load balance policy of the device to Fail Over Only (Active/Passive) and the primary path to path 1-1-0 for Harddisk6.

```
vxdmpadm setattr path
vxdmpadm [-g<DynamicDiskGroupName>] setattr path
[loadbalancepolicy=FO|RR|RS [path#=state#]
|LQ|WP [path#=weight#]|LB|BP [blockshift=#]]
[primarypath=#] <DiskName> | p#c#t#l#>...
```

This command sets the load balance policy and primary path of the designated disk. The following attributes apply:

loadbalancepolicy=FO |RR|RS|LQ|WP|LB Specifies the load balance policy for the device where:

- FO specifies Fail Over Only (Active/Passive)
- RR specifies Round Robin (Active/Active)
- RS specifies Round Robin with Subset
- LQ specifies Dynamic Least Queue Depth
- WP specifies Weighted Paths
- LB specifies Least Blocks
- BP specifies Balanced Path

path#=state# state# specifies either standby (0) or active (1) state of the specified path#. For example, 1-1-1=0 means that path 1-1-1 is assigned a state of standby.
(Default state of a path is active (1).)

path#=weight# weight# specifies the weight assigned to the specified path#. For example, 1-1-1=10 means that path 1-1-1 is assigned a weight of 10. The path with the lowest weight indicates the most-favored path for I/O.
(Range of values for weight#: 0 - 255.)

blockshift=# # specifies the number of contiguous I/O blocks that are sent along a path to an Active/Active array before switching to the next available path.
(Default value is 2048 blocks.)

<code>primarypath=#</code>	# specifies the primary path of the device. For example, <code>primarypath=1-1-1</code> sets path 1-1-1 as the primary path of the device.
<code><DiskName></code>	The designated disk, which can be specified by the device name (such as <code>Harddisk2</code>) or the internal disk name (such as <code>Disk2</code>). The internal disk name must be preceded by the <code>-g</code> option (for example, <code>-gDG1 Disk2</code>).
<code>p#c#t#l#</code>	The #s correspond to the port, channel, target, and LUN of a disk.

Example

```
vxdkpadm setattr path loadbalancepolicy=FO  
primarypath=1-1-0 Harddisk6
```

Sets the load balance policy of the device to Fail Over Only (Active/Passive) and the primary path to path 1-1-0 for Harddisk6.

vxcbr

The `vxcbr` utility provides the ability for users to back up and restore their Veritas Storage Foundation configuration. This utility does not back up and restore data, only the Veritas Storage Foundation configuration—that is, the disk group and logical volume layout on a server.

These are the keywords:

<code>backup</code>	Backs up the Veritas Storage Foundation configuration.
<code>restore</code>	Restores the Veritas Storage Foundation configuration.
<code>write_signature</code>	Manually writes a signature to a disk.

Typing the following sequence for each keyword brings up a description of its syntax:

```
vxcbr <Keyword> -?
```

Note: The `vxcbr` utility does not support Microsoft Disk Management Disk Groups. To back up the configuration of a Microsoft Disk Management Disk Group, use the Windows Server Backup feature of Windows.

Keywords or operands

```
vxcbr backup  
vxcbr [-a] [-p<Path>] backup [<DynamicDiskGroupName>...]  
Backs up the configuration to the directory where the Veritas Storage  
Foundation for Windows software is installed (normally C:\Program  
Files\VERITAS\Volume Manager 5.1) or to a directory indicated in the  
-p<Path> parameter. The configuration files take about one megabyte of  
space per disk group. The vxcbr utility will only back up the configurations  
of disk groups that are ONLINE. Any offline or deported disk groups will be  
skipped by this utility for backup purposes. The following attributes apply:
```

<code>[-a]</code>	Indicates that all disk groups on the server will be backed up. This option is recommended.
-------------------	---

<code>-p<Path></code>	Specifies the path to the directory where the configuration information will be archived. The default path is %ALLUSERSPROFILE%\Application Data\VERITAS\VXCBR\ManualCBR.
<code><DynamicDiskGroupName>...</code>	Limits the configuration to the disk group or disk groups indicated.

You must specify valid target disk groups.

Example

```
vxcbr -a backup
```

This backs up configuration of all online SFW disk groups on the managed server.

```
vxcbr restore
```

```
vxcbr [-i] [-p<Path>] restore [<DynamicDiskGroupName>...]
```

Restores the configuration. This restore command can only restore disk group configurations to their original disks; that is, the program assumes that you have not changed or replaced any of the ORIGINAL disks. However, if a disk is missing, you can specify the `-i` parameter to restore a configuration of an incomplete disk group. Probably, the only reason you might want to do an incomplete restore is to be able to access existing disks. An incomplete restore of the configuration is not recommended. The following attributes apply:

<code>-i</code>	Indicates that you want to restore an incomplete configuration—that is, one of the disks in the configuration is missing. It is a forced restore of an incomplete disk group.
<code>-p<Path>></code>	The path to where configuration information is saved.
<code><DynamicDiskGroupName>...</code>	Restores the disk group or groups specified.

Example

```
vxcbr restore Dg01 Dg02
```

Restores disk group configurations for Dg01 and Dg02.

```
vxcbr write_signature  
vxcbr [-f<FileName>] write_signature  
[<<DiskName>=<DiskSignature>>...]
```

If the signature on a disk is no longer readable, you must manually add the signature back to the disk, so that the configuration information can be restored to the disk. You can find the signature information from a backup of the disk. If you have one or two disks, you can indicate the disk names and signatures in the command line. However, if you have multiple disks, you may find it easier to create a separate file with the disk names and the corresponding disk signatures. The utility will read the information from a specified file.

The following attributes apply:

<code>[-f<FileName>]</code>	Name of the file that has disk names and signatures for each disk you want the write signature to be applied to. Use the format <code>DiskName>=<DiskSignature></code> . For example, <code>Harddisk3=0x1234</code> <code>Harddisk4=0xABCD</code> .
<code>[<<DiskName>=<DiskSignature>>...]</code>	Format for indicating the disk name and signature. See the example below.

Example

```
vxcbr write_signature Harddisk3=0x1234  
Harddisk4=0xABCD
```

Manually adds the 0x1234 signature to Harddisk3 and 0xABCD signature to Harddisk4.

vxsnap

The `vxsnap` CLI utility allows you to perform multiple snapshots at the same time. To use `vxsnap`, you must have the SFW FlashSnap option license installed.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxsnap` command.

The `vxsnap` CLI utility makes use of both FlashSnap and Volume Shadow Copy Service (VSS) technology to create high-quality snapshots that can be done when application files are open. VSS can quiesce the application for the moment when the snapshot is created and then resume the application immediately after the snapshot; but a VSS-aware application must be used, such as Microsoft Exchange or Microsoft SQL. The `vxsnap` CLI utility acts as a VSS requestor, which allows you to use SFW to initiate VSS snapshots at any time.

See “[Volume Shadow Copy Service \(VSS\)](#)” on page 617.

The `vxsnap` utility is designed to create and restore multiple snapshot sets. The `vxsnap` CLI utility allows you to name the snapshot volume. You must create the mirror for the volume before using the `vxsnap` CLI utility. The `vxsnap prepare` command can be used to create the mirror for the volume.

Note: Either the `prepare` or `start` keyword may be used in the CLI, however `prepare` is recommended.

Note: For step-by-step examples using `vxsnap`, see the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange* or the *Veritas Storage Foundation and High Availability Solutions Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft SQL*.

Note: To use `vxsnap`, the disk group must be a Storage Foundation for Windows 4.0 or later version. You must upgrade the disk groups created with an earlier version of Volume Manager for Windows before using the `vxsnap` utility.

Note: The `vxsnap` commands must be invoked on a local system.

vxsnap has the following keywords:

prepare	<p>Creates snapshot mirrors of the volumes in the specified component. The snapshot mirrors remain attached to and synchronized with the original volumes</p> <p>Note: Either the <code>prepare</code> or <code>start</code> keyword may be used in the CLI, however <code>prepare</code> is recommended.</p>
create	<p>Creates simultaneous snapshots of all volumes in the specified component, providing a point-in-time snapshot set.</p>
reattach	<p>Reattaches and resynchronizes an existing snapshot set to the original database volumes.</p>
restore	<p>Restores a volume or database from a snapshot set. For Exchange, restores an Exchange storage group (component) or a single database (subcomponent) from a snapshot set. Exchange storage group recovery can be either a point-in-time restore or a roll-forward recovery to the point of failure. Database recovery must be a roll-forward recovery to the point of failure.</p> <p>Exchange 2007 only: Restore to a recovery storage group (RSG) rather than the production store.</p> <p>Note: COWsnapshots are not supported when restoring to a recovery storage group (RSG).</p>
refresh	<p>Refreshes all VSS Writers and component objects. (Exchange, SQL, Enterprise Vault, Sharepoint, and COW operations)</p>
diffarea	<p>Manages shadow storage area for COW snapshots. For example, the management of shadow storage area creation, size, and removal.</p>
delete	<p>Deletes COW snapshots corresponding to the information in the specified snapshot set.</p>

Type the following sequence to view a description of the command syntax:

```
vxsnap <Keyword> -?
```

Keywords or operands

```
vxsnap prepare
```

For Exchange and volume operations:

```
vxsnap prepare  
component=<ComponentName>/writer=<WriterName>  
[-b] [source=<Volume>/harddisk=<Harddisk>...]
```

Creates snapshot mirrors of the volumes in the specified component and eliminates the need for multiple `vxassist prepare` commands. The snapshot mirrors remain attached to and synchronized with the original volumes.

Note: Either the `prepare` or `start` keyword may be used in the CLI, however `prepare` is recommended.

The following attributes apply:

<code>component=<ComponentName></code>	Name of the component; for Exchange, this is the storage group name found in the Exchange System Manager, for example, "First Storage Group".
<code>></code>	
<code>writer=<WriterName></code>	Unique ID of the VSS writer, for example, "Microsoft Exchange Writer".
<code>-b</code>	Run the process as a background process.
<code>source=<Volume></code>	Indicates the source volume for the snapshot mirror specified by a drive letter, drive path (mount point), or volume name of the form "\\?\Volume{GUID}\".
<code>harddisk=<Harddisk></code>	Name of the disk where the snapshot mirror is created, for example, <code>harddisk2</code> .

Example

```
vxsnap prepare component=SG2/writer="Microsoft  
Exchange Writer" source=L:/harddisk=harddisk2  
source=M:/harddisk=harddisk3
```

This command creates snapshot mirrors of all the volumes contained in the Exchange storage group (component) SG2. The snapshot mirror of the volume mounted on L: is created on disk 2 and the snapshot mirror of the volume mounted on M: is created on disk 3.

For Sharepoint operations:

```
vxsnap prepare writer=<WriterName> component=<ComponentName>
```

Creates snapshot mirrors of the volumes in the specified component. The snapshot mirrors remain attached to and synchronized with the original volumes.

Note: Either the prepare or start keyword may be used in the CLI, however prepare is recommended.

The following attributes apply:

component=<ComponentName>	Name of the database or index. The command prepares mirrors for both the database and log volumes or for the index.
writer=WriterName>	Unique ID of the VSS writer, for example, Sharepoint Services Writer or the GUID for the writer. Required if you specify the component.

Note: Any text string that contains spaces must be enclosed in quotation marks.

Example

```
vxsnap prepare writer="Sharepoint Services Writer"  
component=wss_content
```

This command will create snapshot mirrors of all the volumes contained in the component.

For Enterprise Vault operations:

```
vxsnap prepare [-b] writer=<WriterName>
```

```
[site=<SiteName>[/VSG=<VSGName>[/VS=<VSName>]]  
[[/]/component=<ComponentName>]
```

Creates snapshot mirrors of the volumes in the specified site, vault store group, vault store, or component. The snapshot mirrors remain attached to and synchronized with the original volumes.

Note: Note: Either the prepare or start keyword may be used in the CLI, however prepare is recommended.

The following attributes apply:

-b	Run the process as a background process.
writer=<WriterName> >	Unique ID of the VSS writer, for example, EnterpriseVault. Required if you specify the component.
site=<SiteName>	Name of the Enterprise Vault Site.
VSG=<VSGName>	Name of the Enterprise Vault Vault Store Group
VS=<VSName>	Name of the Enterprise Vault Vault Store
component=<ComponentName>	Name of the Enterprise Vault component. For example, VaultStore database, Fingerprint database, or Volume Component, such as index, partitions, etc.

Note: Any text string that contains spaces must be enclosed in quotation marks.

Additional information about the prepare operation for Enterprise Vault:

- Specifying only the writer attribute (as in vxsnap prepare writer=EnterpriseVault), results in the preparation of the components of the entire Enterprise Vault farm. This would include the Enterprise Vault directory database, monitoring database, audit database, and reporting database.
- Specifying the site attribute (as in vxsnap prepare writer=EnterpriseVault Site=Site1), results in the preparation of the components at the Enterprise Vault site level. This prepares the directory database and all the components (SQL and volume) in the specified site.

- Specifying the vault store group attribute (as in `vxsnap prepare writer=EnterpriseVault Site=Site1/VSG=VSG1`), results in the preparation of the fingerprint database and all the components in all vault stores in the specified vault storage group.
- Specifying the vault store attribute (as in `vxsnap prepare writer=EnterpriseVault Site=Site1/VSG=VSG1/VS=VS1`), results in the preparation of the vault store database and all the partitions in the specified vault store.
- Specifying the component attribute (as in `vxsnap prepare writer=EnterpriseVault Site=Site1/VSG=VSG1/VS=VS1 Component=<Component Name>`), results in the preparation of the specified component. The component can be an Enterprise Vault SQL database or a volume component (eg.vault store database, fingerprint database, directory database, monitoring database, reporting database, audit database, partition, index volume, etc.).
 - For vault store components:When the vault store database component is specified, the open partition in the vault store is also prepared.
 - For vault store components: When the open partition component is specified, the vault store database in the vault store is also prepared.
 - For different components: When different components reside on a common volume, the volume is prepared only once.
- Upon completion of the operation, the status (success/failure) of the selected components is recorded in a log, `%VMPATH%\logs\EVStatus.log`. The log contains information about the success or failure of the operation for the components. In the event that the prepare of a volume for a component fails, the operation continues to prepare the remaining volumes of the component and any other requested components. If the operation succeeds for all the volumes of a component, then the status of the component is logged as a success. If the operation fails for any one of the volumes of the component, then the status of the component is logged as a failure along with the cause of failure.

Example

```
vxsnap prepare writer=ev site=site1/vsg=vsg1/vs=vs1  
site=site2 component="Index Location (V:)"  
component="Directory DB"
```

The command prepares all the volumes for a snapshot for the Enterprise Vault Store vs1 of site1/vsg1 , Index Location (V:) of site2 and Directory DB.

For SQL operations:

```
vxsnap prepare
component=<ComponentName>/writer=<WriterName>
[server=<ServerName>] [instance=<InstanceName>] [-b]
[source=<Volume>/harddisk=<Hardisk>...]
```

Creates snapshot mirrors of the volumes in the specified component. The snapshot mirrors remain attached to and synchronized with the original volumes.

Note: Either the `prepare` or `start` keyword may be used in the CLI, however `prepare` is recommended.

The following attributes apply:

<code>component=<ComponentName></code>	Name of the database. The command prepares mirrors for both the database and log volumes of the SQL database.
<code>writer=<WriterName></code>	Unique ID of the VSS writer, for example, <code>SQLServerWriter</code> or the GUID for the writer. Required if you specify the component.
<code>server=ServerName</code>	SQL Server server name.
<code>instance=InstanceName</code>	SQL Server instance name.
<code>-b</code>	Run the process as a background process.
<code>source=<Volume></code>	Indicates the source volume for the snapshot mirror specified by a drive letter, drive path (mount point), or volume name of the form <code>"\\?\Volume{GUID}\"</code> .
<code>harddisk=<Harddisk></code>	Name of the disk where the snapshot mirror is created, for example, <code>harddisk2</code> .

Note: Any text string that contains spaces must be enclosed in quotation marks.

Example

```
vxsnap prepare
component=billing_DB/writer=SQLServerWriter
```

```
source=L:/harddisk=harddisk3
source=M:/harddisk=harddisk3
```

This command will create snapshot mirrors of all the volumes contained in the billing_DB database. The snapshot mirror of the volume mounted on L: will be created on harddisk 3 and the snapshot mirror of the volume mounted on M: will also be created on harddisk 3.

```
vxsnap create
```

For Exchange operations:

```
vxsnap -x <Filename> create source=<Volume>
[/DriveLetter=<DriveLetter>] [/DrivePath=<DrivePath>]
[/Newvol=<NewVolName>] [/Plex=<PlexName>] ...
[writer=<WriterName>] [component=<ComponentName>]
[backuptype=<Backuptype>] [-E] [-o]
[secHosts=<SecondaryHosts>]
```

Creates snapshot(s) of the specified volume(s) or storage group (component). Allows volumes to be snapshotted simultaneously.

Copy on Write (COW) snapshot may be specified.

Separate source volumes and attributes with forward slashes, not spaces.

Source and snapshot volume attributes are paired. You must specify the source volume if you choose to specify the snapshot volume plex, drive letter, drive path, label, or volume name.

In a 64-bit Exchange 2007 environment, you may also create snapshots of a Microsoft Exchange Writer Replica by specifying the writer to be the replica store writer. (See example below.)

The following attributes apply:

-x <Filename>

Indicates the name to be assigned to the XML metadata file that will be created with the command. The file name must include the ".xml" extension. The default path to the file is

```
C:\Documents and Settings\All
Users\Application
Data\Veritas\VSSXML\Exchange. If
you wish to place the file in another
directory, specify a full path before the
file name, for example
J:\XML\Image1.xml.
```

<code>source=<Volume></code>	Indicates the source volume for the split-mirror snapshot specified by a drive letter, drive path (mount point), or volume name of the form "\\?\Volume{GUID}\". Repeat this parameter for each volume associated with the specified component (for example, Exchange storage group).
<code>[/plex=<PlexName>]</code>	Specifies the name of the mirror or plex that is to be detached. Use this parameter if there are multiple snapplexes available to be snapshotted.
<code>[/DriveLetter=<DriveLetter>]</code>	The drive letter to be assigned to the new snapshot volume.
<code>[/DrivePath=<DrivePath>]</code>	The drive path to be assigned to the new snapshot volume. The drive path must reference an empty local NTFS folder, which was created beforehand. The path must include the drive letter and folder to be mounted, for example, C:\DB1VOL.
<code>[/Newvol=<NewVolName>]</code>	Specifies the name of the new snapshot volume that is created. If the name is not specified using this option, the form "SnapVolume01" is created. The full device path becomes: \\Device\HarddiskDmVolumes\ <DiskGroupName>\<NewVolName>
<code>writer=<WriterName></code>	Unique ID of the VSS writer, for example, "Microsoft Exchange Writer" or "Microsoft Exchange Writer Replica". If you plan to be able to do a roll-forward recovery to the point of failure, you must specify the writer.
<code>component=<ComponentName></code>	Name of the component; for Exchange, this is the storage group name found in the Exchange System Manager, for example, "First Storage Group". If you plan to be able to do a roll-forward recovery to the point of failure, you must use this component.

backuptype=< <i>Backuptype</i> >	Specifies the type of backup, either a Full or Copy. If no option is specified then Copy is the default. Copy backup creates a copy of the database and transaction logs volumes. Full backup creates a copy of the database and transaction logs volumes, runs Eseutil to check for consistency, and if consistent, truncates the transaction logs.
-E	Runs the Eseutil consistency check for database and log files. Eseutil is run automatically with a full backup, but must be optionally specified for a copy backup.
-o	Allows an existing XML file of the same name to be overwritten. If -O is not specified the vxsnap create command does not overwrite an existing XML file of the same name and the operation fails.
-c	<p>Specifies a COW snapshot.</p> <p>In preparation for a COW snapshot, the vxsnap diffarea command must be used to create the shadow storage volume. The following vxsnap attributes are not compatible with COW snapshots and result in an error:</p> <ul style="list-style-type: none"> ■ /DriveLetter=<driveLetter> ■ /DrivePath=<drivePath> ■ /Newvol=<newVolName> ■ /Plex=<plexName> ■ secHosts=<secondary hosts>
sechosts=< <i>SecondaryHosts</i> >	Applies to Veritas Volume Replicator (VVR) environment only. Comma separated list of secondary hosts on which a synchronized snapshot is to be taken.

Note: Any text string that contains spaces must be enclosed in quotation marks.

Example

```
vxsnap -x backupdoc.xml create  
writer="Microsoft Exchange Writer"  
component="First Storage Group"  
source=L:/DriveLetter=O source=M:/DriveLetter=P  
source=N:/DriveLetter=Q backuptype=full
```

This example creates a snapshot set based on the component "First Storage Group," which contains volume L, the log volume, and volumes M and N, two database volumes. The snapshots are assigned drive letters O, P, and Q, respectively. The XML file backupdoc.xml is used to store the VSS metadata as well as the snapshot volume names. The Full backup creates the copy of the database and transaction logs volumes, runs Eseutil to check for consistency, and then truncates the transaction logs.

```
vxsnap -x snapdata.xml create writer="Microsoft  
Exchange Writer Replica" component=SG1 backupType=COPY  
-E -O
```

This example creates a snapshot of the replica of the component SG1. It specifies that the VSS Writer, Microsoft Exchange Writer Replica, is used for the snapshot.

```
vxsnap -x snapdata.xml create  
-C writer="Microsoft Exchange Writer"  
component=mb1 backuptype=COPY -E
```

Creates a COW snapshot of component mb1 of Exchange server. A copy backup is created and a Eseutil consistency check is performed on the snapshot volumes.

For Sharepoint operations:

```
vxsnap -x <Filename> create  
[writer=<WriterName>] [component=<ComponentName>]...  
[backuptype=FULL|COPY]
```

Creates snapshot(s) of the specified volume(s) or Sharepoint components. Allows volumes to be snapshotted simultaneously. Separate attributes with forward slashes, not spaces. The following attributes apply:

- `-x <Filename>` Indicates the name to be assigned to the XML metadata file that will be created with the command. The file name must include the ".xml" extension. To specify a location other than the default location for the file, you must enter the full path for the file (eg. J:\XML\Image1.xml).
- `writer=<WriterName >` Unique ID of the VSS writer, for example, SharePoint Services Writer or the GUID for the writer. Required if you specify the component.
- `component=<ComponentName>` Name of the component. The command creates mirrors for both the database and log volumes, or the index, of the Sharepoint component. Multiple components can be specified.
- `backuptype=FULL|COPY` Specifies the type of backup, either a Full or Copy. If no option is specified then Copy is the default. To back up logs in Sharepoint so that you can restore the database using log replay, at least one Full backup must have been created earlier.

Note: Note: Any text string that contains spaces must be enclosed in quotation marks.

Note: Note: To enable the restore of a single SharePoint component from a snapshot, components should be configured to reside on individual volumes so that a snapshot of a volume contains a single component

Note: Note: When taking a snapshot of the Osearch component, Symantec recommends that the database and index of these components be snapshotted at the same time. Restoring only the database or only the index of these components from a snapshot may cause the component's database not to be synchronized. Restoring an Osearch component from a snapshot that contains both database and index would avoid this issue.

Example

```
vxsnap -x test.xml create  
writer="SharePoint Services Writer" component=wss_component1  
component=wss_component2
```

This example creates a snapshot based on the component wss_component1 and wss_component2. The XML file, test.xml, is used to store the VSS metadata that identifies the snapshot. This file is used in the command to reattach the snapshot to resynchronize it and in the command to recover the database using the snapshot.

For Enterprise Vault operations:

```
vxsnap -x <Filename> create writer=<WriterName>
[site=<SiteName>[/VSG=<VSGName>[VS=<VSName>]]]
[[/]component=<ComponentName>[backuptype=FULL|COPY] [-o]
```

Creates snapshot(s) of the Enterprise Vault components. Allows volumes to be snapshotted simultaneously.

The following attributes apply:

-x<Filename>	Indicates the name to be assigned to the XML metadata file that will be created with the command. The file name must include the ".xml" extension. To specify a location other than the default location for the file, you must enter the full path for the file (eg. J:\XML\Image1.xml).
writer=<WriterName> >	Unique ID of the VSS writer, for example, EnterpriseVault. Required if you specify the component.
site=<SiteName>	Name of the Enterprise Vault site.
VSG=<VSGName>	Name of the Enterprise Vault Vault Store Group.
VS=<VSName>	Name of the Enterprise Vault Vault Store.
component=<ComponentName>	Name of the Enterprise vault component. For example, Vault Store database, Fingerprint database, or Volume component, such as index, partitions, etc.
backuptype=FULL COPY	Specifies the type of backup, either a Full or Copy. If no option is specified then Copy is the default.
-o	Allows an existing XML file of the same name to be overwritten. If -o is not specified the vxsnap create command does not overwrite an existing XML file of the same name and the operation fails.

Note: Any text string that contains spaces must be enclosed in quotation marks.

Additional information about the create operation for Enterprise Vault:

- Specifying only the writer attribute (as in `vxsnap -x xmlfile create writer=EnterpriseVault`), results in the snapshot of the components of the entire Enterprise Vault farm. This would include the Enterprise Vault directory database, monitoring database, audit database, and reporting database.
- Specifying the site attribute (as in `vxsnap -x xmlfile create writer=EnterpriseVault Site=Site1`), results in the snapshot of the components at the Enterprise Vault site level. This prepares the directory database and all the components (SQL and volume) in the specified site.
- Specifying the vault store group attribute (as in `vxsnap -x xmlfile create writer=EnterpriseVault Site=Site1/VSG=VSG1`), results in the snapshot of the fingerprint database and all the components in all vault stores in the specified vault storage group.
- Specifying the vault store attribute (as in `vxsnap -x xmlfile create writer=EnterpriseVault Site=Site1/VSG=VSG1/VS=VS1`), results in the snapshot of the vault store database and all the partitions in the specified vault store.
- Specifying the component attribute (as in `vxsnap -x xmlfile create writer=EnterpriseVault Site=Site1/VSG=VSG1/VS=VS1 Component=<Component Name>`), results in the snapshot of the specified component. The component can be an Enterprise Vault SQL database or a volume component (eg.vault store database, fingerprint database, directory database, monitoring database, reporting database, audit database, partition, index volume, etc.).
 - For vault store components: When the vault store database component is specified, the open partition in the vault store is also snapshotted.
 - For vault store components: When the open partition component is specified, the vault store database in the vault store is also snapshotted.
 - For different components: When different components reside on a common volume, the volume is snapshotted only once.
- Upon completion of the operation, the status (success/failure) of the selected components is recorded in a log, `%VMPATH%\logs\EVStatus.log`. The log contains information about the success or failure of the operation for the components. In the event that the snapshot of a volume for a component fails, the operation does not snapshot the remaining volumes of

the component nor any other requested components that are remaining. If the operation succeeds for all the volumes of a component, then the status of the component is logged as SUCCESS. If the operation fails for any one of the volumes of the component, then the status of all the components of that EnterpriseVault server is logged as FAILED along with the cause of the failure. The status of all components that had been already snapshotted earlier before the failed component are logged as SUCCESS, and the status of the remaining components that had not been snapshotted are logged as SKIPPED.

Examples

```
vxsnap -x snapdata.xml create writer=EnterpriseVault  
site=site1/vsg=vsg1/vs=vs1  
site=site2 component="Index Location (V:)" component="Directory DB"
```

This example makes a snapshot of vault store "vs1" of site1/vsg1, "Index Location (V:)" of site2 and component "Directory DB".

```
vxsnap -x snapdata.xml create writer=EnterpriseVault site=site1
```

This example makes a complete snapshot of site1 (including the directory database).

For SQL operations:

```
vxsnap -x <Filename> create source=<Volume>  
[/DriveLetter=<DriveLetter>] [/DrivePath=<DrivePath>]  
[/Newvol=<NewVolName>] [/Plex=<PlexName>]...  
[writer=<WriterName>] [component=<ComponentName>]  
[server=ServerName] [instance=InstanceName]  
[backuptype=FULL|COPY] [-o] [secHosts=<SecondaryHosts>]
```

Creates snapshot(s) of the specified volume(s) or SQL database. Allows volumes to be snapshotted simultaneously.

Separate source volumes and attributes with forward slashes, not spaces. Source and snapshot volume attributes are paired. You must specify the source volume if you choose to specify the snapshot volume plex, drive letter, drive path, label, or volume name.

COW snapshot may be specified.

The following attributes apply:

<code>-x <Filename></code>	<p>Indicates the name to be assigned to the XML metadata file that will be created with the command. The file name must include the ".xml" extension. The default path to the file is C:\Documents and Settings\All Users\Application Data\Veritas\VSSXML\SQL. If you wish to place the file in another directory, specify a full path before the file name, for example J:\XML\Image1.xml.</p>
<code>source=<Volume></code>	<p>Indicates the source volume for the split-mirror snapshot specified by a drive letter, drive path (mount point), or volume name of the form "\\?\Volume{GUID}\". Repeat this parameter for each volume associated with the specified component.</p>
<code>[/plex=<PlexName>]</code>	<p>Specifies the name of the mirror or plex that is to be detached. Use this parameter if there are multiple snapplexes available to be snapshotted.</p>
<code>[/DriveLetter=<DriveLetter>]</code>	<p>The drive letter to be assigned to the new snapshot volume.</p>
<code>[/DrivePath=<DrivePath>]</code>	<p>The drive path to be assigned to the new snapshot volume. The drive path must reference an empty local NTFS folder, which was created beforehand. The path must include the drive letter and folder to be mounted, for example, C:\DB1VOL.</p>
<code>[/Newvol=<NewVolName>]</code>	<p>Specifies the name of the new snapshot volume that is created. If the name is not specified using this option, the form "SnapVolume01" is created. The full device path becomes: \Device\HarddiskDmVolumes\ <DiskGroupName>\<NewVolName></p>

<code>writer=<WriterName></code>	Unique ID of the VSS writer, for example, SQLServerWriter or the GUID for the writer. Required if you specify the component.
<code>component=<ComponentName></code>	Name of the database. The command prepares mirrors for both the database and log volumes of the SQL database.
<code>server=ServerName</code>	SQL Server server name.
<code>instance=InstanceName</code>	SQL Server instance name.
<code>backuptype=FULL COPY</code>	Specifies the type of backup, either a Full or Copy. If no option is specified then Copy is the default. To back up logs in SQL Server so that you can restore the database using SQL log replay, at least one Full backup must have been created earlier.
<code>-o</code>	Allows an existing XML file of the same name to be overwritten. If <code>-o</code> is not specified the <code>vxsnap create</code> command does not overwrite an existing XML file of the same name and the operation fails.
<code>-c</code>	Specifies a COW snapshot. In preparation for a COW snapshot, the <code>vxsnap diffarea</code> command must be used to create the shadow storage volume. The following <code>vxsnap</code> attributes are not compatible with COW snapshots and result in an error: <ul style="list-style-type: none">■ <code>/DriveLetter=<driveLetter></code>■ <code>/DrivePath=<drivePath></code>■ <code>/Newvol=<newVolName></code>■ <code>/Plex=<plexName></code>■ <code>secHosts=<secondary hosts></code>
<code>sechosts=<SecondaryHosts></code>	Applies to Veritas Volume Replicator (VVR) environment only. Comma separated list of secondary hosts on which a synchronized snapshot is to be taken.

Note: Any text string that contains spaces must be enclosed in quotation marks.

Example

```
vxsnap -x billing_DB.xml create
source=G:/Newvol=billing_data
source=H:/Newvol=billing_log
writer=SQLServerWriter component=billing_DB
backuptype=full
```

This example creates a snapshot set based on the component `billing_DB` which contains volume G, the database volume, and volume H, the log volume. The snapshot volumes are named `billing_data` and `billing_log`, respectively. The XML file, `billing_DB.xml`, is used to store the VSS metadata that identifies the snapshot set. This file is used in the command to reattach the snapshot set to resynchronize it and in the command to recover the database using the snapshot set.

```
vxsnap -x snapdata.xml create
-C writer=sqlserverwriter
component=testDB server=localhost
```

Creates a COW snapshot of SQL database `testDB` used in the default instance of the localhost.

For volume operations:

```
vxsnap -x <Filename> create source=<Volume>
[/DriveLetter=<DriveLetter>] [/DrivePath=<DrivePath>]
[/Newvol=<NewVolName>] [/Plex=<PlexName>] ... [-o]
```

Creates snapshot(s) of the specified volume(s). Allows volumes to be snapshotted simultaneously.

Separate source volumes and attributes with forward slashes, not spaces. Source and snapshot volume attributes are paired. You must specify the source volume if you choose to specify the snapshot volume plex, drive letter, drive path, label, or volume name.

COW snapshot may be specified.

The following attributes apply:

<code>-x <Filename></code>	Indicates the name to be assigned to the XML metadata file that will be created with the command. The file name must include the ".xml" extension.
----------------------------------	--

<code>source=<Volume></code>	Indicates the source volume for the split-mirror snapshot specified by a drive letter, drive path (mount point), or volume name of the form "\\?\Volume{GUID}\". Repeat this parameter for each volume associated with the specified component.
<code>[/plex=<PlexName>]</code>	Specifies the name of the mirror or plex that is to be detached. Use this parameter if there are multiple snapplexes available to be snapshotted.
<code>[/DriveLetter=<DriveLetter>]</code>	The drive letter to be assigned to the new snapshot volume.
<code>[/DrivePath=<DrivePath>]</code>	The drive path to be assigned to the new snapshot volume. The drive path must reference an empty local NTFS folder, which was created beforehand. The path must include the drive letter and folder to be mounted, for example, C:\DB1VOL.
<code>[/Newvol=<NewVolName>]</code>	Specifies the name of the new snapshot volume that is created. If the name is not specified using this option, the form "SnapVolume01" is created. The full device path becomes: \\Device\HarddiskDmVolumes\ <DiskGroupName>\<NewVolName>
<code>-o</code>	Allows an existing XML file of the same name to be overwritten. If <code>-o</code> is not specified the <code>vxsnap create</code> command does not overwrite an existing XML file of the same name and the operation fails.

- c Specifies a COW snapshot.
- In preparation for a COW snapshot, the vxsnap diffarea command must be used to create the shadow storage volume. The following vxsnap attributes are not compatible with COW snapshots and result in an error:
- /DriveLetter=<driveLetter>
 - /DrivePath=<drivePath>
 - /Newvol=<newVolName>
 - /Plex=<plexName>
 - secHosts=<secondary hosts>

Note: Any text string that contains spaces must be enclosed in quotation marks.

Example

```
vxsnap -x snapdata.xml create  
source=E:\Data\DB1/DrivePath=E:\Backup\DB1  
source=E:\Data\DB2/DrivePath=E:\Backup\DB2
```

This command does not specify a specific storage group (component) but rather creates snapshots from the volumes mounted on E:\Data\DB1 and E:\Data\DB2. The resulting snapshot volumes are assigned mount points E:\Backup\DB1 and E:\Backup\DB2, respectively. The metadata involved in this operation is stored in snapdata.xml.

```
vxsnap -x snapdata.xml create  
-C source=D:  
Creates a COW snapshot of volume D:
```

```
vxsnap reattach
```

For Exchange operations:

```
vxsnap -x <Filename> [-f] [-b] reattach  
[writer=<WriterName>] [secHosts=<SecondaryHosts>]
```

This command reattaches and resynchronizes the snapshot volumes in the snapshot set to the original database volumes.

The following attributes apply:

<code>-x <Filename></code>	The file created by the <code>vxsnap create</code> command. Each snapshot set must have a unique name for the metadata file. Note: This file is deleted after the reattach operation has completed successfully.
<code>-f</code>	Forces the reattach. Make sure the volume is not in use by another application before using this command. Use this option with care.
<code>-b</code>	Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete.
<code>writer=<WriterName></code>	Unique ID of the VSS writer, for example, "Microsoft Exchange Writer".
<code>sechosts=<SecondaryHosts></code>	Applies to Veritas Volume Replicator (VVR) environment only. Comma separated list of secondary hosts on which a synchronized snapshot is to be taken.

Note: Make sure that the snapshot volumes are not in use before using this command.

Example

```
vxsnap -x snapdata.xml reattach
```

This command uses the information in the `snapdata.xml` file to reattach and resynchronize all the volumes in the snapshot set. This xml file is deleted after the reattach operation has completed successfully. The snapshot volumes remain synchronized with the original volumes until the `vxsnap create` command is issued.

For SharePoint operations

```
vxsnap -x <Filename>[-f] [-b] reattach [writer=<WriterName>]
```

This command reattaches and resynchronizes the snapshot volumes in the snapshot set to the original SharePoint component volumes.

The following attributes apply:

- x<Filename> The file created by the vxsnap create command. Each snapshot set must have a unique name for the metadata file.
- Note:** Note: This file is deleted after the reattach operation has completed successfully.
- f Forces the reattach. Make sure the volume is not in use by another application before using this command. Use this option with care.
- b Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete.
- writer=<WriterName> Unique ID of the VSS writer, for example,
> SharePointServerWriter or the GUID for the writer.

Note: Make sure that the snapshot volumes are not in use before using this command.

Example

```
vxsnap -x SnapshotSet.xml reattach writer="SharePoint Server"
```

This command uses the information in the SnapshotSet.xml file to reattach and resynchronize all the volumes in the snapshot set. This xml file is deleted after the reattach operation has completed successfully. The snapshot volumes remain synchronized with the original volumes until the vxsnap create command is issued.

Note: Note: Any text string that contains spaces must be enclosed in quotation marks.

For Enterprise Vault operations:

```
vxsnap -x <Filename> [-f] [-b] reattach [writer=<WriterName>  
[site=<SiteName>[/VSG=<VSGName>[VS=<VSName>]]]  
[[/]component=<ComponentName>
```

This command reattaches and resynchronizes the snapshot volumes in the snapshot set to the original Enterprise Vault component volumes.

The following attributes apply:

-x<Filename>	The file created by the vxsnap create command. Each snapshot set must have a unique name for the metadata file. Note: This file is deleted after the reattach operation has completed successfully.
-f	Forces the reattach. Make sure the volume is not in use by another application before using this command. Use this option with care.
-b	Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete.
writer=<WriterName> >	Unique ID of the VSS writer, for example, EnterpriseVault or the GUID for the writer.
site=<SiteName>	Name of the Enterprise Vault Site.
VSG=<VSGName>	Name of the Enterprise Vault Vault Store Group.
VS=<VSName>	Name of the Enterprise Vault Vault Store.
component=<ComponentName>	Name of the Enterprise vault component. For example, Vault Store database, Fingerprint database, or Volume component, such as index, partitions, etc.

Note: Note: Any text string that contains spaces must be enclosed in quotation marks.

Note: Upon completion of the operation, the status (success/failure) of the selected components is recorded in a log, %VMPATH%\logs\EVStatus.log. The log contains information about the success or failure of the operation for the components. In the event that the reattach of a volume for a component fails, the operation continues to reattach the remaining volumes of the component and any other requested components. The components that successfully complete the operation are removed from the snapshot set. If the operation succeeds for all the volumes of a component, then the status of the component is logged as a success. If the operation fails for any one of the volumes of the component, then the status of the component is logged as a failure along with the cause of failure.

Example

```
vxsnap -x snapdata.xml reattach writer=EnterpriseVault
site=site1/vsg1/vs=vs1 site=site2
component="Index Location (V:)"
component="Directory DB"
```

This example reattaches all the snapshot volumes for the vault store vs1 of site1/vsg1, "Index Location (V:)" of site2 and "Directory DB".

For SQL operations:

```
vxsnap -x <Filename> [-f] [-b] reattach
[writer=<WriterName>] [secHosts=<SecondaryHosts>]
```

This command reattaches and resynchronizes the snapshot volumes in the snapshot set to the original database volumes.

The following attributes apply:

-x <Filename>	The file created by the vxsnap create command. Each snapshot set must have a unique name for the metadata file. Note: This file is deleted after the reattach operation has completed successfully.
-f	Forces the reattach. Make sure the volume is not in use by another application before using this command. Use this option with care.
-b	Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete.
writer=<WriterName>	Unique ID of the VSS writer, for example, SQLServerWriter or the GUID for the writer.
sechosts=<SecondaryHosts>	Applies to Veritas Volume Replicator (VVR) environment only. Comma separated list of secondary hosts on which a synchronized snapshot is to be taken.

Note: Make sure that the snapshot volumes are not in use before using this command.

Example

```
vxsnap -x billing_DB.xml reattach  
writer=SQLServerWriter
```

This command uses the information in the `snapdata.xml` file to reattach and resynchronize all the volumes in the snapshot set. This xml file is deleted after the reattach operation has completed successfully. The snapshot volumes remain synchronized with the original volumes until the `vxsnap create` command is issued.

Note: Any text string that contains spaces must be enclosed in quotation marks.

For volume operations:

```
vxsnap -x <Filename> [-f] [-b] reattach
```

This command reattaches and resynchronizes the snapshot volumes in the snapshot set to the original database volumes.

The following attributes apply:

-x <Filename>	The file created by the <code>vxsnap create</code> command. Each snapshot set must have a unique name for the metadata file. Note: This file is deleted after the reattach operation has completed successfully.
-f	Forces the reattach. Make sure the volume is not in use by another application before using this command. Use this option with care.
-b	Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete.

Note: Make sure that the snapshot volumes are not in use before using this command.

Example

```
vxsnap -x snapdata.xml reattach
```

This command uses the information in the `snapdata.xml` file to reattach and resynchronize all the volumes in the snapshot set. This xml file is deleted after the reattach operation has completed successfully. The snapshot volumes remain synchronized with the original volumes until the `vxsnap create` command is issued.

```
vxsnap restore
```

For Exchange operations:

```
vxsnap -x <Filename> [-f] [-b] [-r] [-a] restore
restoreType=<PIT|POF> writer=WriterName
[subComponent=<subComponentName>] [RSG=<Yes|No>]
```

Uses the snapshot volumes in a snapshot set created by the `vxsnap create` command to restore data, for example, after an original volume has become corrupted. You can restore the data either to the point in time that the snapshot set was last refreshed or to the point of failure of the storage group or a single database.

(COW snapshots can be used with this command.)

Note: For Exchange 2007, if you have a recovery storage group (RSG) for a storage group, you have the option to restore snapshot volumes to the databases in the RSG.

(COW snapshots are not supported when restoring to a recovery storage group (RSG)).

Note: After completing a point of failure (POF) recovery of a single database, Symantec recommends using the `vxsnap reattach` command to reattach and resynchronize the other databases in the storage group and to use the `vxsnap create` command to create a new snapshot set.

Implementing the point of failure recovery requires that the `writer=WriterName` and the `component=<ComponentName>` parameters were specified when the snapshot set was created.

The following attributes apply:

- | | |
|---------------|--|
| -x <Filename> | The file created by the <code>vxsnap create</code> command. Each snapshot set must have a unique name for the metadata file. |
| -f | Forces the snapback. Make sure the volume is not in use by another application before using this command. Use this option with care. |
| -b | Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete. |

<code>-r</code>	<p>Recover one or more of the original volumes are missing. Example below shows additional required steps.</p> <p>This option cannot be specified to recover using a COW snapshot.</p>
<code>-a</code>	<p>Dismount the databases before the restore operation and then mount the database after the restore operation.</p>
<code>restoreType=<PIT POF></code>	<p>PIT specifies a restore to the point in time that the snapshot set was created or last refreshed.</p> <p>POF specifies a roll-forward recovery to the point of failure.</p>
<code>writer=<i>WriterName</i></code>	<p>The name for the Exchange Server VSS Writer; used to located the default directory to search for the XML metadata file.</p> <p>For Exchange 2007, for which there can be both an active writer and a replica writer, you must specify the active writer “Microsoft Exchange Writer” with the POF option.</p>
<code>subComponent= <<i>subComponentName</i>></code>	<p>Name of the subcomponent to be restored. In Exchange, a subcomponent is a mailbox store (database). Use this attribute only in a point of failure recovery.</p>

RSG=<Yes | No>

For Exchange 2007 only.

Specifying Yes restores a snapshot of the Storage Group Component to the Recovery Storage Group (RSG).

Before using this command, an RSG must already exist and databases have already been created in the RSG. The names of the databases in the RSG must match the names of the databases of the source Storage Group.

When performing a PIT recovery for an RSG, all subcomponents of the Storage Group are recovered.

When performing a POF recovery for an RSG, only a subcomponent of the Storage group is recovered. This subcomponent must be specified in the command.

Note: COW snapshots do not support restoring a Recovery Storage Group (RSG).

Note: Before using this command, make sure that the source volumes and the snapshot volumes are not in use. Use the [-a] attribute to dismount and mount the databases automatically or use the Exchange System Manager to dismount all the databases in the storage group and then mount them after the command is completed.

Examples

```
vxsnap -x snapdata.xml restore
```

This command uses the information in the snapdata.xml file to restore all the volumes in the snapshot set identified in that file to the point in time the snapshot set was created or last refreshed.

Point-in-Time Recovery

```
vxsnap -x snapdata.xml restore restoreType=PIT
```

This command uses the information in the snapdata.xml file to restore all the volumes in the snapshot set identified in that file to the point in time the snapshot set was created or last refreshed.

If you want to restore to an RSG (Exchange 2007 only), use the RSG=Yes option.

Roll-Forward Recovery to the Point of Failure

```
vxsnap -x snapdata.xml restore restoreType=POF
```

This command uses the information about the storage group specified in the `snapdata.xml` file to snapback the database volumes and then use current transaction logs to roll forward to the point of failure.

Roll-Forward Recovery to the Point of Failure of a Single Database

```
vxsnap -x snapdata.xml restore restoreType=POF  
subcomponent=DB1
```

This command restores the specified database (subcomponent) DB1 and then uses current transaction logs to roll forward only that database to the point of failure.

If you want to restore to an RSG (Exchange 2007 only), use the `RSG=Yes` option.

Recovery After Hardware Failure

You can use the `-r` switch to perform a VSS-integrated recovery after a hardware failure. The following recovery scenarios are possible if the complete snapshot set including the XML metadata file is available.

Note: For more information about the `-r` switch, see the Snapshot Solutions section in the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange*, which is included with the software.

Table 9-1 Available recovery type after missing production volume

Scenario	Database Volumes	Transaction Logs Volume	Recovery
Scenario I	One or more volumes are missing.	Missing	point in time
Scenario II	All volumes are missing.	Available	point in time or point of failure
Scenario III	One or more volumes are missing. At least one volume is available.	Available	point of failure

Complete the following tasks to perform a VSS-integrated recovery:

- Identify the snapshot volume associated with each missing production volume. Note the drive letter or mount point of each volume.
- Use Exchange System Manager to dismount all remaining databases in the storage group.
- Delete the missing volumes from Storage Foundation for Windows.
- Replace the failed hardware and add the new disks to the dynamic disk group.
- Reassign the drive letters or mount points of the snapshot volumes so that they are the same as the missing production volumes.
- Perform a VSS-integrated recovery by including the `-r` switch in the `vxsnap restore` command. For example, type:

```
vxsnap -x snapdata.xml -r restore restoreType=PIT
```

This command uses the information the `snapdata.xml` file to restore all the volumes in the snapshot set identified in that file to the point in time the snapshot set was created or last refreshed.

Caution: Before using the `vxsnap restore` command, verify that you have correctly assigned the drive or mount point to each volume and that you have accounted for all the volumes in the storage group (component).

For SharePoint operations:

```
vxsnap -x <Filename> [-f] [-b] [-r] [-a]
```

```
restore[restoreType=[RECOVERY|NO_RECOVERY]]
```

writer=WriterName [component=<ComponentName>]

Uses the snapshot volumes in a snapshot set created by the vxsnap create command to recover a corrupted or missing SharePoint component. Exclusive access to the SharePoint component is required for this operation.

Before using this command verify that the source volumes and the snapshot volumes are not in use.

The following attributes apply:

- x <Filename> The file created by the vxsnap create command. Each snapshot set must have a unique name for the metadata file.
- f Forces the snapback. Make sure the volume is not in use by another application before using this command. Use this option with care.
- b Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete.
- r Recover even if original volume is not present. If this option is selected and the original volume is not present, the snapshot volume of the missing volume is changed from a read-only volume to a read-write volume.

After using this option you must explicitly assign the original drive letter/mount path of the missing volume to the snapshot volume in the VEA and then bring the database online.
- a Dismount the databases before the restore operation and then mount the database after the restore operation.

<p>restoreType= [RECOVERY NO_REC OVERY]</p>	<p>Specifies the type of database recovery, either recovery or no recovery:</p> <p>With RECOVERY database and transaction log files are restored from the snapshot set. No transaction backup logs are applied. The database is left in an operational state.</p> <p>To back up logs so that you can restore the database using log replay, at least one Full backup must have been created earlier.</p> <p>NO_RECOVERY restores from the specified snapshot set to the time of the snapshot. No logs are applied and the database is left in a loading state so that you can manually replay backup logs to a specific point in time.</p>
<p>writer=<WriterName ></p>	<p>The name for the Share Point Services Writer; used to located the default directory to search for the XML metadata file. Specify "Sharepoint Services Writer"..</p>
<p>component=<Compo nentName></p>	<p>Name of the SharePoint component to recover. If not specified , then all the components in the snapsot set are restored.</p>

The following are examples of the command:

- Recovering all components

```
vxsnap -x 1.xml -a restore RestoreType=RECOVERY
Writer="Sharepoint Services Writer"
```

This command uses the information in the 1.xml file to restore all the volumes for all components and bring the components online. The components are restored to the time the snapshot was created.
- Recovering each component separately

```
vxsnap -x 1.xml -a restore RestoreType=RECOVERY
Writer="Sharepoint Services Writer" component=wss_component1
vxsnap -x 1.xml -a restore RestoreType=RECOVERY
Writer="Sharepoint Services Writer" component=wss_component2
```

This command uses the information in the 1.xml file to restore all the volumes for each component and bring each component online. The components are restored to the time the snapshot was created.

For Enterprise Vault operations

```
vxsnap -x <Filename> [-b] [-f] [-r] [-a] restore
writer=WriterName [site=<siteName>[/VSG=<VSGName>[/VS=<VSName>]]]
```

```
[[/]component=<ComponentName>]  
{RestoreType=[RECOVERY[NO_RECOVERY]]}
```

Uses the snapshot volumes in a snapshot set created by the vxsnap create command to recover a corrupted or missing Enterprise Vault component.

Exclusive access to the Enterprise Vault component is required for this operation.

Before using this command verify that the source volumes and the snapshot volumes are not in use.

The following attributes apply:

-x <Filename>	The file created by the vxsnap create command. Each snapshot set must have a unique name for the metadata file.
-b	Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete.
-f	Forces the snapback. Use this option with care.
-r	Recover even if original volume is not present. If this option is selected and the original volume is not present, the snapshot volume of the missing volume is changed from a read-only volume to a read-write volume.
-a	Dismount the databases before the restore operation and then mount the database after the restore operation.
writer=<WriterName> >	Unique ID of the VSS writer, for example, EnterpriseVault or the GUID for the writer.
site=<SiteName>	Name of the Enterprise Vault site.
VSG=<VSGName>	Name of the Enterprise Vault Store Group.
VS=<VSName>	Name of the Enterprise Vault Store.
component=<ComponentName>	Name of the Enterprise vault component. For example, Vault Store database, Fingerprint database, or Volume component, such as index, partitions, etc.

`restoreType=` Specifies the type of database recovery, either recovery or no recovery:

`[RECOVERY|NO_RECOVERY]` With RECOVERY database and transaction log files are restored from the snapshot set. No transaction backup logs are applied. The database is left in an operational state.

To back up logs so that you can restore the database using log replay, at least one Full backup must have been created earlier.

NO_RECOVERY restores from the specified snapshot set to the time of the snapshot. No logs are applied and the database is left in a loading state so that you can manually replay backup logs to a specific point in time.

Note: Upon completion of the operation, the status (success/failure) of the selected components is recorded in a log, %VMPATH%\logs\EVStatus.log. The log contains information about the success or failure of the operation for the components. In the event that the restore of a volume for a component fails, the operation continues to restore the remaining volumes of the component and any other requested components. The components that successfully complete the operation are removed from the snapshot set. If the operation succeeds for all the volumes of a component, then the status of the component is logged as a success. If the operation fails for any one of the volumes of the component, then the status of the component is logged as a failure along with the cause of failure.

The following is an example of the command.

```
vxsnap -x snapdata.xml -a restore RestoreType=RECOVERY
writer=EnterpriseVault
site=site1/vsg=vsg1/vs=vs1 component="Directory DB"
```

This command restores the vault store vs1 and component DirectoryDB using the metadata from snapdata.xml.

For SQL operations:

```
vxsnap -x <Filename> [-f] [-b] [-r] restore
[restoreType= [RECOVERY|NO_RECOVERY]]
[noLogs|logFiles=<tlog1,tlog2,...>] writer=WriterName
```

Uses the snapshot volumes in a snapshot set created by the `vxsnap create` command to recover a corrupted or missing SQL Server database. Exclusive access to the SQL Server database is required for this operation.

(COW snapshots can be used with this command.)

Before using this command verify that the source volumes and the snapshot volumes are not in use.

The following attributes apply:

- x *<Filename>* The file created by the vxsnap create command. Each snapshot set must have a unique name for the metadata file.
- f Forces the snapback. Make sure the volume is not in use by another application before using this command. Use this option with care.
- b Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete.
- r Recover even if original volume is not present. If this option is selected and the original volume is not present, the snapshot volume of the missing volume is changed from a read-only volume to a read-write volume.

Use this option only with Recovery noLogs. After using this option you must explicitly assign the original drive letter/mount path of the missing volume to the snapshot volume in the VEA and then bring the database online.

This option cannot be specified to recover using a COW snapshot.

<pre>restoreType=[RECOVER Y NO_RECOVERY]</pre>	<p>Specifies the type of database recovery, either recovery or no recovery:</p> <p>RECOVERY can be used with either the <i>noLogs</i> or <i>logFiles=tlog1,tlog2,...</i> attributes. RECOVERY leaves the database in an online state.</p> <p>To back up logs so that you can restore the database using log replay, at least one Full backup must have been created earlier.</p> <p>NO_RECOVERY restores from the specified snapshot set to the time of the snapshot. No logs are applied and the database is left in an loading state so that you can manually replay backup logs to a specific point in time.</p>
<pre>noLogs</pre>	<p>Database and transaction log files are restored from the snapshot set. No transaction backup logs are applied. The database is left in an operational state.</p>
<pre>logFiles=tlog1,tlog2,..</pre>	<p>Transaction log backup files to be applied with the RECOVERY option to achieve a point of failure recovery and leave the database in an online state. Each transaction log must have a unique name and be created using the “overwrite existing media” option.</p>
<pre>writer=WriterName</pre>	<p>The name for the SQL Server VSS Writer; used to located the default directory to search for the XML metadata file. Specify SQLServerWriter.</p>

Examples

- Recovering using snapshots without log replay

```
vxsnap -x TestDB.xml restore RestoreType=RECOVERY
noLogs
```

This command uses the information in the TestDB.xml file to restore all the volumes in the snapshot set and brings the database online. The database is restored to the time the snapshot set was created or last refreshed.

You can use the **-r** option with the **RECOVERY noLogs** restore type if a production volume is missing due to hardware failure:

```
vxsnap -x TestDB.xml -r restore RestoreType=RECOVERY
noLogs
```

- sRecovering using snapshots and log replay

```
vxsnap -x TestDB.xml restore RestoreType=RECOVERY
logFiles=c:\backup\tLog1.bak, c:\tLog2.bak
```

This command uses the information in the TestDB.xml file to restore all the volumes in the snapshot set and then applies the specified transaction log backups (c:\backup\tLog1.bak and c:\tLog2.bak) and brings the database online.

- Restoring snapshots and manually applying logs

```
vxsnap -x TestDB.xml restore RestoreType=NO_RECOVERY
```

This command uses the information in the TestDB.xml file to restore all the volumes in the snapshot set and leaves the database in a loading state so that backup logs can be manually restored to a specific point in time.

Note: For more information about the `-r` switch, see the *Veritas Storage Foundation and High Availability Solutions Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft SQL*.

For volume operations:

```
vxsnap -x <Filename> [-f] [-b] [-r] restore
<restoreType=PIT>
```

Uses the snapshot volumes in a snapshot set created by the `vxsnap create` command to restore data, for example, after an original volume has become corrupted.

(COW snapshots can be used with this command.)

The following attributes apply:

- | | |
|---------------|--|
| -x <Filename> | The file created by the <code>vxsnap create</code> command. Each snapshot set must have a unique name for the metadata file. |
| -f | Forces the snapback. Make sure the volume is not in use by another application before using this command. Use this option with care. |
| -b | Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete. |

- r Recover one or more of the original volumes are missing.
This option cannot be specified to recover using a COW snapshot.
- restoreType=<PIT> PIT specifies a restore to the point in time that the snapshot set was created or last refreshed.

Examples

```
vxsnap -x snapdata.xml restore
```

This command uses the information in the snapdata.xml file to restore all the volumes in the snapshot set identified in that file to the point in time the snapshot set was created or last refreshed.

```
vxsnap refresh
```

For Exchange, SharePoint, Enterprise Vault, COW, and SQL operations:

```
vxsnap refresh
```

This command refreshes all VSS Writers and their component objects. (Exchange, SQL, Enterprise Vault, Sharepoint, and COW operations)

vxsnap diffarea

For COW snapshot operations:

```
Vxsnap diffarea <-a|-r|-c> source=<driveletter>  
/target=<driveletter>[/size=<size>]...
```

Manages creation, deletion, and modification of shadow storage area settings for COW snapshots.

The following attributes apply:

- a Create shadow storage area for volume specified in source. Shadow storage area resides on volume specified in target with specified size. The shadow storage area must reside in the same dynamic disk group as the source. It can reside on the same volume as the source volume.
- r Remove association of shadow storage area specified in target and volume specified in source.

-c	Change the shadow storage area settings for an existing shadow storage area specified in the target and the volume specified in source.
source	Source volume for COW snapshot. Note: A basic volume cannot be used as the source volume. Note: Source volume must be an NTFS volume.
target	Volume for storing blocks of source volume before write operation. Note: Note: A basic volume cannot be used as the target volume. Note: Note: Target volume must be an NTFS volume.
size	Size of volume that is shadow storage area. If size is set to -1 or if size is not specified, then the size of the shadow storage area is unlimited.

Note: Use the VEA GUI to view the settings for shadow storage areas.

Examples

```
vxsnap diffarea -a source=E:/target=F:/size=500  
source=G:/target=H:/size=300
```

This command creates two shadow storage areas. One is a 500MB shadow storage area on volume F that stores COW snapshots of volume E. The second is a 300MB shadow storage area on volume H that stores COW snapshots of volume G.

```
vxsnap diffarea -r source=E:/target=F:
```

This command removes the association between volume E and the shadow storage area on volume F.

vxsnap delete

For COW snapshot operations:

```
vxsnap -x <Filename> [-f] delete  
[writer=WriterName]
```

Deletes the COW snapshots corresponding to the information in the specified XML file. The XML file is deleted after all the snapshots have been successfully deleted.

The following attributes apply:

- x <Filename>** Name of the file that stores the metadata for COW snapshots. The file is created by the vxsnap create command.
- f** Forces the delete. Use this option with care.
Use the -f option when one or more snapshots in the snapshot set do not exist. For example, use the -f option when one or more snapshots in the snapshot set no longer exist because Windows has deleted older snapshots to make room for newer snapshots.
- writer=WriterName** The name for the VSS Writer associated with the snapshots to be deleted.

Examples

`vxsnap -x snapdata.xml delete writer="Microsoft Exchange Writer"`
Deletes the Exchange COW snapshots corresponding to information in snapdata.xml.

`vxsnap -x snapdata.xml delete writer=sqlserverwriter`
Deletes the SQL COW snapshots corresponding to information in snapdata.xml.

`vxsnap -x snapdata.xml delete`
Deletes the COW snapshots corresponding to information in snapdata.xml.

`vxsnap -x cow1.xml -f delete`
Forces the deletion of the COW snapshots corresponding to information in cow1.xml.

vxsnapsql

The `vxsnapsql` utility is designed to simultaneously snapshot all the volumes associated with an SQL Server 2000 or SQL Server 2005 database.

Note: The `vxsnapsql` command does not support SQL Server 2008. The `vxsnap` command can be used instead. See “[vxsnap](#)” on page 407.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxsnapsql` command.

`vxsnapsql` has the following keywords:

<code>prepare</code>	Creates mirrors for snapshots on the specified disks. Note: Either the <code>prepare</code> or <code>start</code> keyword may be used in the CLI, however <code>prepare</code> is recommended.
<code>create</code>	Creates a simultaneous snapshot of all the volumes in the specified component.
<code>restore</code>	Restores a corrupted database using the snapshot set. Restore can specify a recovery of the database with or without logs.
<code>reattach</code>	Reattaches and resynchronizes an existing snapshot set to the original database volumes.

Note: The `vxsnapsql create` command does not use the VSS snapshot method and does not create read only snapshots.

Typing the following sequence brings up a description of the command syntax:

```
vxsnapsql <Keyword> -?
```

Keywords or operands

```
vxsnapsql prepare
```

```
vxsnapsql [-b] prepare [server=<ServerName>]  
[instance=<InstanceName>] component=<DBname>  
[<Diskname>] . . .
```

This command creates mirrors of the volumes in the database (component) in preparation for creating a snapshot set using the `vxsnapsql create` command.

Note: Either the `prepare` or `start` keyword may be used in the CLI, however `prepare` is recommended.

The following attributes apply:

<code>-b</code>	Runs the command in the background.
<code>server=</code> <code><ServerName></code>	Name of the local system (localhost) or of the SQL virtual server created in a clustered environment. The default, localhost, need not be specified.
<code>instance=</code> <code><InstanceName></code>	SQL Server instance name. This parameter is not required for a default instance.
<code>component=</code> <code><DBname></code>	SQL Server database name as it appears in the SQL Enterprise Manager. Mirrors in preparation for snapshots are created for all the data and log volumes associated with the specified SQL Server database.
<code><Diskname></code>	Name of the disk or disks where the mirrors in preparation for snapshots are created, for example, <code>harddisk2</code> .

Example

```
vxsnapsql -b prepare instance=Accounting
component=TestDB harddisk3
```

This command creates a mirror in preparation for a snapshot (snapplex) on `harddisk3` for each data or log volume associated with the SQL Server database `TestDB` in the `Accounting` instance. The mirrors remain synchronized with the original volumes until the `vxsnapsql create` command is issued.

```
vxsnapsql create
vxsnapsql -x <Filename> [-o] create
[server=<serverName>] [instance=<InstanceName>]
component=<DBname> [<snapshot_tuple>...]
```

A `snapshot_tuple` consists of a number of attribute=value fields. Within each tuple, the source and snapshot volume attributes are paired by forward slashes (/). Although the entire `snapshot_tuple` is optional, if you choose to define the tuple for one volume, or you must define it for all volumes in the component. The tuple will be of the following form:

```
source=volume [/Newvol=SnapVol] [/plex=SnapPlexName]
[/DriveLetter={A|B|...|Z}] [/Label=<VolLabel>]
[/DrivePath=<DrivePath>]
```

This command creates split-mirror snapshots of the volumes in the specified database (component) and a metadata file containing information about the database and snapshot volumes. Together the snapshots and metadata file form the snapshot set.

The following attributes apply:

<code>-x <Filename></code>	Indicates the name assigned to the XML metadata file that is created to store the snapshot information. The metadata file is used for restore operations. Symantec recommends that the file name include the ".xml" extension. The default path to the file is \Documents and Settings\All Users\Application Data\VERITAS\SQLBACKUP. If you wish to place the file in another directory, specify a full path before the file name, for example J:\XML\Image1.xml. In a clustered environment, store the metadata file on shared storage.
<code>-o</code>	Overwrites an existing XML metadata file of the same name.
<code>server=<ServerName></code>	Name of the local system (localhost) or of the SQL virtual server created in a clustered environment. The default, local host, need not be specified.
<code>instance=<InstanceName></code>	SQL Server instance name. This parameter is not required for a default instance.
<code>component=<DBname></code>	SQL Server database name as it appears in the SQL Enterprise Manager. Snapshots are created for all the data and log volumes associated with the specified SQL Server database.

<code><snapshot_tuple></code>	Consists of a number of attribute=value fields. The source and snapshot volume attributes are paired by forward slashes (/). Although the entire snapshot_tuple is optional, if you choose to define the tuple for one volume, or you must define it for both the database and log volumes.
<code>source=<Volume></code>	Indicates the source volume for the split-mirror snapshot specified by a drive letter, drive path (mount point), or volume name of the form "\\?\Volume{GUID}\". Repeat this parameter for each volume associated with the specified SQL Server database.
<code>[/Newvol=<SnapVol>]</code>	Specifies the name of the new snapshot volume that is created. If the name is not specified with this option, the form "SnapVolume01" is created. The full device path will be: \Device\HarddiskDmVolumes\ <DiskGroupName>\<SnapVolName>
<code>[/plex=<SnapPlexName>]</code>	Specifies the name of the snapshot mirror (plex) to be detached. Use this parameter if there are multiple snap plexes available for the snapshot.
<code>[/DriveLetter={A B ... Z}]</code>	Specifies the drive letter assigned to the new snapshot volume.
<code>[/Label=<volLabel>]</code>	Specifies the volume label assigned to the new snapshot volume.
<code>[/DrivePath=<DrivePath>]</code>	Specifies the drive path assigned to the new snapshot volume. The drive path must reference an existing empty local NTFS folder. The path must include the drive letter and folder to be mounted, for example, C:\DB1VOL.

Examples

```
vxsnapsql -x TestDB.xml create component=TestDB  
source=M:/driveletter=R source=N:/driveletter=S
```

This command creates split-mirror snapshots of the data and log volumes associated with the TestDB database, in this example volumes M and N. TestDB is in a default instance running on the local host. The snapshots are assigned drive letters R and S respectively. Additionally, a metadata file, TestDB.xml, is created and stored in the default directory \Documents and Settings\All Users\Application Data\VERITAS\SQLBACKUP.

```
vxsnapsql -x TestDB.xml create server=SQLVS  
instance=acctpay  
component=TestDB  
source=E:\DB1\Data/DrivePath=F:\DB1Snapshot\Data  
source=E:\DB1\TLog/DrivePath=F:\DB1Snapshot\TLog
```

This command creates snapshots of the volumes associated with the TestDB database in the acctpay instance on the SQL virtual server SQLVS. The original volumes are mounted on E:\DB1\Data and E:\DB1\TLog. The resulting snapshot volumes are assigned mount points F:\DB1Snapshot\Data and F:\DB1Snapshot\TLog respectively. The metadata involved in this operation is stored in TestDB.xml in the default directory \Documents and Settings\All Users\Application Data\Veritas\SQLBACKUP.

```
vxsnapsql restore  
vxsnapsql -x <Filename> [-b] [-f] [-s] restore  
{RestoreType=[RECOVERY|NO_RECOVERY]} [noLogs]  
[logFiles=<tlog1,tlog2,...>]
```

This command restores the snapshot volumes in the snapshot set and is used to recover a corrupted or missing SQL Server database. After a restore with the recovery option, the database is left in an online state. After a restore with the no_recovery option, the database is left in a loading state. The following attributes apply:

- | | |
|---------------|--|
| -x <Filename> | The metadata file created by the vxsnapsql create command. Each snapshot backup set must have a unique name for the metadata file. |
| -b | Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete. |

- f Forces the operation. Make sure the volume is not in use before using this option.
- s Silent mode. Allows the restore operation to proceed without user interaction.
- RestoreType=
[RECOVERY|NO_RECOVER
Y] Specifies the type of database recovery, either recovery or no recovery. RECOVERY leaves the database in an online state. NO_RECOVERY leaves the database in a loading state.
- <noLogs> Database and transaction log files are restored from the snapshot backup set. No other logs are applied. The database is left in an online state.
- logFiles=<tlog1,tlog2,...> Transaction log backup files to be applied with the RECOVERY option to achieve a point of failure recovery and leave the database in an online state. Each transaction log must have a unique name and be created using the “overwrite existing media” option within SQL Server.

The options can be applied as follows:

Table 9-2 Recovery Options

Selected options	Database state after recovery	Description
RECOVERY, logFiles= <i>tlog1,tlog2,...</i>	online	Database and transaction log volumes are restored and the specified backup transaction logs are applied.
RECOVERY, noLogs	online	Database and transaction log volumes are restored and mounted. No additional transaction logs are applied.
NO_RECOVERY	loading	Database and transaction logs are restored. The database is left in a loading state so that backup logs can be replayed to a specified point in time.

Exclusive access to the SQL Server database is required for this operation. Before using this command verify that the source volumes and the snapshot volumes are not in use. In the SQL Enterprise Manager, close the tree view to the server level.

Examples

Point in Time Restore

```
vxsnapsql -x TestDB.xml restore  
RestoreType=NO_RECOVERY
```

This command uses the information in the TestDB.xml file to restore all the volumes in the snapshot set and leaves the database in a loading state so that backup logs can be manually restored to a specific point in time.

Point of Failure Restore

```
vxsnapsql -x TestDB.xml restore RestoreType=RECOVERY  
logFiles=c:\backup\tLog1.bak, c:\tLog2.bak
```

This command uses the information in the TestDB.xml file to restore all the volumes in the snapshot set and then applies the specified transaction log backups (c:\backup\tLog1.bak and c:\tLog2.bak) and brings the database online.

Time of Snapshot Restore

```
vxsnapsql -x TestDB.xml restore RestoreType=RECOVERY  
noLogs
```

This command uses the information in the TestDB.xml file to restore all the volumes in the snapshot set and brings the database online. The database is restored to the time the snapshot set was created or last refreshed.

```
vxsnapsql reattach
```

```
vxsnapsql -x <Filename> [-b] [-f] reattach
```

This command reattaches and resynchronizes the snapshot volumes in the snapshot set to the original database volumes. (This command is similar to a snapback operation.)

The following attributes apply:

- | | |
|---------------|---|
| -x <Filename> | The file created by the vxsnapsql create command. Each snapshot set must have a unique name for the metadata file.
Note: This file is deleted after the reattach operation has completed successfully |
| -b | Resynchronizes the volume in the background. A new snapshot cannot be made until the resynchronization is complete. |
| -f | Forces the operation. Make sure the volume is not in use before using this option. |

Example

```
vxsnapsql -x TestDB.xml reattach
```

This command uses the information in the TestDB.xml file to reattach and resynchronize all the volumes in the snapshot set. This xml file is deleted after the reattach operation has completed successfully. The snapshot volumes remain synchronized with the original volumes until the vxsnapsql create command is issued.

vxfsync

```
vxfsync -g <DynamicDiskGroupName> -m <Mastervolume> -s  
<Snapvolume> -f <filename>
```

The **vxfsync** utility uses Fast File Resync to resynchronize a single file in a snapshotted volume to the original volume. It is designed to restore a good copy of one corrupt file in a database application that has volumes with multiple database files.

See “[Fast file resync](#)” on page 614.

Note: The `vxfsync` command is only available from the Storage Foundation folder found at the following path,
%ProgramFiles%\Common Files\Veritas Shared\Storage Foundation.

The following attributes apply:

<code>-g <DynamicDiskGroupName></code>	The name of the disk group containing the original and snapshotted volumes.
<code>-m <Mastervolume></code>	The original volume.
<code>-s <Snapvolume></code>	The name of the split-mirror snapshot volume.
<code>-f <filename></code>	The file name of the file to be resynchronized to the original volume.

Example

```
vxfsync -g test -m vol1 -s vol1_snap01 -f test.dat
```

This command will use the snapshot volume (the replica), `vol1_snap01`, to resynchronize or restore the file **test.dat** on the master or original volume, **vol1**.

vxscrub

`vxscrub` is a command for removing unneeded entries in the registry that are a result of adding and deleting volumes. The command is designed to shrink the size of the registry by purging the system hive. Shrinking the size of the registry after adding and deleting volumes avoids problems during system reboot. Rebooting the system after running `vxscrub` is mandatory.

Caution: The `vxscrub` utility should be used only under the direction of Support. Use of this utility without supervision may cause performance problems when importing disk groups.

These are the operands for `vxscrub`:

- `[-a|-b|-l|-v]` Uninstalls all unused volumes, disks, or mounted devices only. Does not purge the system hive.
- `-p` Uninstalls all unused volumes, disks, and mounted devices, then purges the system hive.
- `-forcepurge` Purges the system hive only. Does not uninstall unused volumes, disks, or mounted devices.

Typing the following brings up a description of its syntax:

```
vxscrub
```

Keywords or operands

```
vxscrub [-a|-b|-l|-v]
```

```
vxscrub [-a|-b|-l|-v] [-d] [-m] [-q] [-c]
```

Uninstalls all unused volumes, disks, or mounted devices only. Does not purge the system hive.

Note: The system hive of the registry does not physically shrink using this command mode. Use the other command modes to physically shrink the system hive of the registry.

The following attributes apply:

-a	Uninstalls all unused volumes.
-b	Uninstalls all unused BASIC volumes.
-l	Uninstalls all unused LDM volumes.
-v	Uninstalls all unused SFW volumes.
-d	Uninstalls all unused disk instances.
-m	Cleans up the database of mounted devices.
-q	Does not display any output.
-c	Tests the uninstall and clean up operation. The uninstall and clean up operation is not performed.

Example

```
vxscrub -a -d -m
```

This command uninstalls all unused volumes, disks, and mounted devices.

```
vxscrub -p  
vxscrub -p [-q]
```

Uninstalls all unused volumes, disks, and mounted devices, then the system hive is purged.

Note: You must reboot the system after running this command.

The following attributes apply:

-p	Uninstalls all unused volumes, disks, and mounted devices, then the system hive is purged.
-q	Does not display any output.

Example

```
vxscrub -p
```

This command uninstalls all unused volumes, disks, and mounted devices; purges the system hive; and shrinks the size of the registry.

```
vxscrub -forcepurge
```

```
vxscrub -forcepurge [-c]
```

Purges the system hive only. Does not uninstall unused volumes, disks, or mounted devices.

Note: You must reboot the system after running this command.

The following attributes apply:

-forcepurge

Purges the system hive.

-c

Tests the purge operation and reports the new size of the registry. The purge operation is not performed.

Example

```
vxscrub -forcepurge
```

This command purges the system hive and shrinks the size of the registry.

vxverify

`vxverify` is a command that determines if there are any differences between plexes of mirrored volumes. This command compares the volumes on a block by block basis. Blocks that do not match are reported in the output.

Note: For RAID-5 volumes, `vxverify` also checks the integrity of the parity of the volumes.

Typing the following sequence brings up a description of its syntax:

```
vxverify -?
```

Keywords or operands

```
vxverify [-v] [-p] [-d <n|all>] <DynamicDiskGroupName>  
<Volume Name> [[offset] length]
```

The following attributes apply:

<code>-v</code>	Enables verbose output. This specifies that in addition to any blocks that do not match, the output includes the mirror volume name, block number, and number of blocks being compared.
<code>-p</code>	Enables the utility to process a partial plex for debugging purposes.
<code>-d</code>	Enables the utility to dump mismatched blocks.
<code>n all</code>	Specifies the number of mismatched blocks to dump. <ul style="list-style-type: none">■ <code>n</code> specifies the number of mismatched blocks.■ <code>all</code> specifies the dumping of all mismatched blocks.
<code><DynamicDiskGroupName></code>	Specifies the dynamic disk group of the volume. <p>Note: The name of the disk group is case sensitive.</p>
<code><Volume Name></code>	Specifies the volume to process.

offset	Specifies the offset for comparison. Offset is specified as a number of blocks.
length	Specifies the length for comparison. Length is specified as a number of blocks. Note: If no length is specified, then the entire volume is compared.

Example

```
vxverify -g Accounting test
```

This command performs a comparison of the volume test of the disk group Accounting and its mirrors.

vxcache

vxcache is a command that sets up a designated cache memory pool to improve performance for specific dynamic volumes.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the vxcache command.

vxcache has the following keywords:

cacheinfo	Displays the cache settings for the server or for a volume.
set	Enables or disables the cache and sets the size of the cache.

Keywords or operands

```
vxcache [-g <DynamicDiskGroupName>] cacheinfo [<VolumeName |  
DriveLetter |VmName|DrivePath>]
```

The following attributes apply:

-g	Specifies the dynamic disk group of the volume.
<DynamicDiskGroupName>	Note: The name of the disk group is case sensitive.
<VolumeName>	The path name of the volume, such as \Device\HarddiskDmVolumes\DG1\Volume1.
<DriveLetter>	The drive letter of the volume.
<VmName>	Internal name of the volume; requires the use of the -g option, such as -gDG1Volume1.
<DrivePath>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Example

```
vxcache cacheinfo -g Accounting test
```

This command displays the current vxcache settings for the volume test of the disk group Accounting.

```
vxcache [-g <DynamicDiskGroupName>] set [cache=on|off]  
[memorysize=<n>] [<VolumeName|DriveLetter|VmName|DrivePath>]
```

The following attributes apply:

<code>-g</code> <DynamicDiskGroupName>	Specifies the dynamic disk group of the volume. Note: The name of the disk group is case sensitive.
<code>cache=on off</code>	Turns vxcache on and off.
<code>memorysize=<n></code>	Sets the size of the cache to n MB.
<VolumeName>	The path name of the volume, such as \Device\HarddiskDmVolumes\DG1\Volume1.
<DriveLetter>	The drive letter of the volume.
<VmName>	Internal name of the volume; requires the use of the <code>-g</code> option, such as <code>-gDG1Volume1</code> .
<DrivePath>	A volume that is mounted on an NTFS folder; it is indicated by a path to that folder.

Example

```
vxcache -g Accounting set cache=on test
```

This command enables the cache for the volume test of the disk group Accounting.

```
vxcache set cache=on memorysize=20
```

This command enables the cache at the server level and sets the size of the cache to 20MB.

```
vxcache set memorysize=50
```

This command sets the size of the cache to 50MB at the server level.

vxprint

`vxprint` is a command that displays information about SFW and VVR objects. Specifying the name of an object results in a display of information for the object. Hierarchies within record associations are displayed in an orderly fashion so that the structure of records is clear. Dashes (-) are displayed in the output wherever there is no available output value. If no option is specified in the command, the command defaults to the -h option.

The typical output format consists of single line records, each of which include information such as record type, name, object association, object state, length, and other fields. A header line is also written before the record information.

When no disk group is specified with the command, objects in all the disk group are displayed.

Typing the following sequence brings up a description of its syntax:

```
vxprint -?
```

Keywords or operands

```
vxprint [-h] [-n] [-q] [-l] [-P] [-V] [-v] [-p] [-d] [-s] [-A] [-Q] [-G] [-E]
[-g <DynamicDiskGroupName> ] [Name]
```

The following attributes apply:

-h	List record hierarchies.
-n	List record names.
-q	Suppress field header in output display.
-l	List record information in verbose format.
-P	List VVR RLINK records.
-V	List VVR RVG records.
-v	List volume records.
-p	List plex records.
-d	List disk records.
-s	List subdisk records.
-A	Display all disk groups.
-Q	Suppress diskgroup header.
-G	List disk groups.

-E List enclosures.

Specifies dynamic disk group.
<-gDynamicDiskGroupName
>

<Name> Specifies an object to process.

Example

```
vxprint -gAccounting test
```

This command displays information for the volume test in the disk group Accounting.

```
vxprint -v
```

This command displays information of all the volumes on the system.

```
vxprint -p
```

This command displays information of all the plexes on the system.

Troubleshooting and recovery

- [Using disk and volume status information](#)
- [SFW error symbols](#)
- [Resolving common problem situations](#)
- [Commands or procedures used in troubleshooting and recovery](#)
- [Additional troubleshooting issues](#)
- [Automated System Recovery \(ASR\)](#)

Using disk and volume status information

If a disk or volume fails, it is important to repair the disk or volume as quickly as possible to avoid data loss. Because time is critical, Veritas Storage Foundation for Windows makes it easy for you to locate problems quickly. In the Status column of the **Disks** tab view or **Volumes** tab view, you can view the status of a disk or volume. You can also see indications of abnormal status in the tree view or the **Disk View** tab. If the status is not Healthy for volumes, Imported for dynamic disks, or Online for basic disks, use this section to determine the problem and then fix it.

The topics are the following:

- [Disk status descriptions](#)
- [Volume status descriptions](#)

Note: When there is a problem with a disk or volume, you can also look at the **Events** tab view for messages about problems that may have occurred.

Disk status descriptions

One of the following disk status descriptions will always appear in the Status column of the disk in the right pane of the console window. If there is a problem with a disk, you can use this troubleshooting chart to diagnose and correct the problem.

Caution: The suggested actions may bring the disks to an Imported status, but they do not guarantee data integrity.

Figure 10-1 Disk Status Descriptions

Status	Meaning	Action Required
Imported	The disk is accessible and has no known problems. This is the normal disk status for dynamic disks.	No user action is required.
Online	The disk is accessible and has no known problems. This is the normal disk status for basic disks.	No user action is required.
No Media	No media has been inserted into the CD-ROM or removable drive. Only CD-ROM or other removable disk types display the No Media status.	Insert the appropriate media into the CD-ROM or other removable drive, and the disk status will become Online. If you do not see the disk status change immediately, use the Refresh command to refresh the GUI.
Foreign	Only dynamic disks display this status. There are three situations where a disk may be marked as Foreign:	See “Bring a foreign disk back to an online state” on page 479.

Figure 10-1 Disk Status Descriptions

Status	Meaning	Action Required
	<p><i>Situation 1</i></p> <p>The disk was created as a dynamic disk on another computer and has been moved to your computer and has not been set up for use.</p>	<p><i>Situation 1</i></p> <p>Use Import Dynamic Disk Group to make the disk group available for use.</p> <p>In the Import Dynamic Disk Group dialog box, be sure to click the checkbox to clear the host ID of the other system.</p>
	<p><i>Situation 2</i></p> <p>The disk contains a secondary disk group (that is, a disk group other than disk group containing the computer's boot or system disk) and you have a dual-boot system. When you switch between operating systems, the disk with a secondary disk group is marked as Foreign and does not auto-import.</p>	<p><i>Situation 2</i></p> <p>Use Import Dynamic Disk Group to make the secondary disk group available for use. The primary disk group will import automatically when you switch between operating systems.</p> <p>In the Import Dynamic Disk Group dialog box, be sure to click the checkbox to clear the host ID of the other system.</p>
	<p><i>Situation 3</i></p> <p>The disk was originally created on this computer. It was moved or deleted. Now you want to bring it back to this computer as a member of the disk group in which it was originally created.</p>	<p><i>Situation 3</i></p> <p>Use the Merge Foreign Disk command to restore the disk as a member of its former disk group.</p>

Figure 10-1 Disk Status Descriptions

Status	Meaning	Action Required
No Disk Signature	Displays for new disks. The disk cannot be used because it has no signature.	Right-click on the disk and select Write Signature from the menu. The disk type will change to Basic Disk and the disk can be accessed or upgraded.
Offline	Only dynamic disks display this status. There are two situations where a disk may show a status of Offline:	
	<i>Situation 1</i>	<i>Situation 1</i>
	The disk was part of the system's disk configuration but currently cannot be found.	Make sure the disk is connected to the computer. Then use Rescan to bring the disk online. See " Bring an offline dynamic disk back to an imported state " on page 477.
	<i>Situation 2</i>	<i>Situation 2</i>
The disk is not accessible. The disk may be corrupted or intermittently unavailable. An error icon appears on the offline disk. If the disk status is Offline and the disk's name changes to Missing Disk (#), the disk was recently available on the system but can no longer be located or identified.	Make sure the disk is connected to the computer. Then use Rescan to bring the disk online. See " Bring an offline dynamic disk back to an imported state " on page 477.	
Disconnected	Displays for a dynamic disk when the system can no longer find the disk. The name of the disk becomes "Missing Disk."	Reconnect the disk.

Figure 10-1 Disk Status Descriptions

Status	Meaning	Action Required
Import Failed	The import of the dynamic disk group containing the disk failed. All disks in a dynamic disk group that failed to import will show this status.	Examine your configuration to determine what the problem might be.
Failing	Failing is a secondary message shown in parentheses after a disk status. This status indicates that I/O errors have been detected on a region of the disk. All the volumes on the disk will display Failed, Degraded, or Failing status, and you may not be able to create new volumes on the disk. Only dynamic disks display this status.	Right-click on the failing disk and select Reactivate Disk to bring the disk to Online status and all its volumes to Healthy status.

Volume status descriptions

One of the following volume status descriptions will always appear in the graphical view of the volume and in the Status column of the volume in list view. If there is a problem with a volume, you can use this troubleshooting chart to diagnose and correct the problem.

Caution: The suggested actions may bring the volumes to a Healthy status, but they do not guarantee data integrity.

Table 10-1 Volume Status Descriptions

Status	Meaning	Action Required
Healthy	The volume is accessible and has no known problems. This is the normal volume status. Both dynamic volumes and basic volumes display the Healthy status.	No user action is required.
Resynching	The volume's mirrors are being resynchronized so that both mirrors contain identical data. Both dynamic and basic mirrored volumes display the Resynching status. When resynchronization is complete, the mirrored volume's status returns to Healthy. Resynchronization may take some time, depending on the size of the mirrored volume.	No user action is required. Although you can safely access a mirrored volume while resynchronization is in progress, you should avoid making configuration changes (such as breaking a mirror) during resynchronization.
Regenerating	Data and parity are being regenerated for a RAID-5 volume. Both dynamic and basic RAID-5 volumes display the Regenerating status. When regeneration is complete, the RAID-5 volume's status returns to Healthy.	No user action is required. You can safely access a RAID-5 volume while data and parity regeneration is in progress.

Table 10-1 Volume Status Descriptions

Status	Meaning	Action Required
Degraded	The Degraded status applies only to mirrored or RAID-5 volumes on basic or dynamic disks. There are three situations where Degraded status can occur:	Take the following actions to resolve these situations:
	<p><i>Situation 1</i></p> <p>The data on the volume may no longer be fault tolerant because one of the underlying disks is not online. A RAID-5 volume loses redundancy if one disk is offline or failed. A mirrored volume can lose redundancy if one of the disks containing one of its subdisks fails.</p>	<p><i>Situation 1</i></p> <p>You can continue to access the volume using the remaining online disks, but you should repair the volume as soon as possible.</p> <p>It is important to repair the volume because if another disk that contains the volume fails, you will lose the volume and its data.</p> <p>See “Bring a dynamic volume back to a healthy state” on page 481</p> <p>See “Bring a basic volume back to a healthy state” on page 481.</p>
	<p><i>Situation 2</i></p> <p>A Degraded status will also display if a disk involving a RAID-5 or mirrored volume was physically moved.</p>	<p><i>Situation 2</i></p> <p>To correct the problem, you must move all the disks that contain the volume to the new location or return the moved disk or disks to the original location.</p>

Table 10-1 Volume Status Descriptions

Status	Meaning	Action Required
	<p><i>Situation 3</i></p> <p>The data on the volume is no longer fault tolerant, and I/O errors have been detected on the underlying disk. If an I/O error is detected on any part of a disk, all volumes on the disk display the (At Risk) status. Only dynamic mirrored or RAID-5 volumes display the Degraded (At Risk) status.</p>	<p><i>Situation 3</i></p> <p>To return the underlying disk to the Online status, reactivate the disk (using the Reactivate Disk command). Once the disk is returned to the Online status, the volume status should change to Degraded.</p> <p>Take further action as necessary to bring the volume back to a healthy state.</p> <p>See “Bring a dynamic volume back to a healthy state” on page 481</p>
<p>Failed</p>	<p>A failed volume will be started automatically. An error icon appears on the failed volume. Both dynamic and basic volumes display the Failed status. There are two situations where Failed status can occur:</p>	<p>Take the following actions to resolve these situations:</p>
	<p><i>Situation 1</i></p> <p>A volume that spans two or more disks has one or more disks fail. A striped volume, simple volume, spanned volume, or extended partition will fail with one disk failure. A RAID-5 volume will fail with two disk failures. A mirrored or mirrored-striped volume will fail when the disks containing all the mirrors in the volume fail.</p>	<p><i>Situation 1</i></p> <p>Replace or repair the failed or malfunctioning disk or disks.</p>

Table 10-1 Volume Status Descriptions

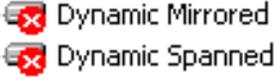
Status	Meaning	Action Required
	<p><i>Situation 2</i></p> <p>A disk or disks involving a volume that spans multiple disks is moved to another computer.</p>	<p><i>Situation 2</i></p> <p>Move all the disks that contain subdisks of the volume, or return the moved disk or disks to the original location.</p>
Formatting	The volume is being formatted using the specifications you chose for formatting.	No user action is required.
Stopped	The volume is in a dynamic disk group that is not imported.	Import the dynamic disk group containing the volume.
Missing	The volume status will be Missing if any of the subdisks of the volume are on disks that show an Offline status.	Reactivate the offline disks and Rescan . If the volume status changes to Stopped or Failed, reactivate the volume.
Failing	Failing is a secondary message shown in parentheses after a volume status. Failing means Veritas Storage Foundation for Windows encountered some I/O errors on at least one disk that contains subdisks of the volume; however, these errors did not compromise the data on the specific volume. Failing sends the message that the disk integrity is deteriorating. When the volume status is Degraded (At Risk), the underlying disk's status is usually Online (Failing).	Determine which disk is failing, and take corrective action. See " Disk status descriptions " on page 468.

SFW error symbols

When a problem occurs in a computer's storage subsystem, Veritas Storage Foundation for Windows will alert the user with error messages and error symbols placed on top of the disk or volume icons to show the source of the problem.

The table below lists these error symbols, explains their meaning, and gives examples of their usage.

Table 10-2 Veritas Storage Foundation for Windows Error Symbols

Symbol	Meaning	Example
	Warning. The yellow caution symbol indicates there is a potential problem but the system can still function normally.	Capacity warning, Degraded warning.
	Informational. The blue information symbol indicates the object is not accessible. This state is often caused by a user operation. No degradation or loss of data; the system can still function normally.	Server started, Device arrival, Write disk signature.
	Failure. The X symbol on a red circle indicates that a serious storage failure has occurred. Users need to look at the source of the problem and fix it as soon as possible. Any attempt to access the object will result in an error.	Failed volume, Missing disk.

Resolving common problem situations

This section provides information on how to resolve the most common problem situations that users encounter when managing their storage with Veritas Storage Foundation for Windows.

This section covers the following topics:

- [Bring an offline dynamic disk back to an imported state](#)
- [Bring a basic disk back to an online state](#)
- [Remove a disk from the computer](#)
- [Bring a foreign disk back to an online state](#)
- [Bring a basic volume back to a healthy state](#)
- [Bring a dynamic volume back to a healthy state](#)
- [Repair a volume with degraded data after moving disks between computers](#)
- [Deal with a provider error on startup](#)

Bring an offline dynamic disk back to an imported state

An Offline dynamic disk may be corrupted or intermittently unavailable.

To bring an offline dynamic disk back to an imported state

- 1 Repair any disk or controller problems, and make sure that the disk is turned on, plugged in, and attached to the computer.
- 2 Use the **Rescan** command to rescan all the devices on the SCSI bus to bring the disk back online.
 Select **Rescan** from the **Actions** menu, or right-click the StorageAgent node in the tree view to get a context menu and select **Rescan** from that menu. If you have a lot of devices on the computer's SCSI bus, the rescan of the bus may take some time.
 See "[Rescan command](#)" on page 485.
 If one of the disks has failed and you have a mirrored or RAID-5 volume, the repair involves recreating part of the volume in a different location.
 See the following topics for more information:
 "[Repair volume command for dynamic RAID-5 volumes](#)" on page 493
 "[Repair volume command for dynamic mirrored volumes](#)" on page 493
- 3 If the disk does not come back after doing a rescan, select the disk and use the **Reactivate Disk** command to manually bring the disk back online.

Right-click the disk's label in the tree view or the Disk View tab view to bring up the disk's context menu and select the **Reactivate Disk** command from the menu.

See "[Reactivate disk command](#)" on page 491.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Disk** command.

If reactivating the disk does not change its status, something must be wrong with the disk or its connections.

- 4 If a disk comes back online after reactivating, check to see whether its volumes are healthy. If not, try the **Reactivate Volume** command on its volumes.

See "[Reactivate volume command](#)" on page 492.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Volume** command.

- 5 Run **Chkdsk.exe** to make sure that the underlying data on the disk is not corrupted.

To run **Chkdsk**, open a command prompt window and enter the following command:

chkdsk x: /f

where *x* is the drive letter of the volume you want to check. The **/f** option tells **Chkdsk** to fix any errors it finds. If the **/f** option is omitted, **Chkdsk** will operate in a read-only mode.

Although **Chkdsk** will clean up the file system structure, there may still be invalid data on the disk if users were working when a problem occurred on the disk. It is highly recommended that you run utilities to check the integrity of the data. If the data is corrupted, you will need to replace it from backup storage.

Bring a basic disk back to an online state

If a basic disk is corrupted or unavailable, it will not show in the GUI.

To bring a basic disk back to an online state

- 1 Repair any disk or controller problems, and make sure that the disk is turned on, plugged in, and attached to the computer.
- 2 Use the **Rescan** command to rescan all the devices on the SCSI bus to bring the disk back online.

Select **Rescan** from the **Actions** menu, or right-click the StorageAgent node in the tree view to get a context menu and select **Rescan** from that menu. If you have a lot of devices on the computer's SCSI bus, the rescan of the bus may take some time.

See "[Rescan command](#)" on page 485.

- 3 If a disk comes back online after rescanning, check to see whether its volumes are healthy.

If they are not, you need to bring the volumes back to a healthy state.

See "[Bring a basic volume back to a healthy state](#)" on page 481.

- 4 Run **Chkdsk.exe** to make sure that the underlying data on the disk is not corrupted.

Even if the disk and volumes come back online, it is important to check whether the underlying data is intact.

To run **Chkdsk**, open a command prompt window and enter the following command:

chkdsk x: /f

where *x* is the drive letter of the volume you want to check. The **/f** option tells **Chkdsk** to fix any errors it finds. If the **/f** option is omitted, **Chkdsk** will operate in a read-only mode.

If the data is corrupted, you will need to replace it with data from backup storage.

Remove a disk from the computer

As part of troubleshooting you may need to remove a basic or dynamic disk from the computer. This information is covered in the topics on disk tasks.

See "[Remove a disk from the computer](#)" on page 145.

Bring a foreign disk back to an online state

To bring a foreign disk back to an online state depends on the original context of the disk. The following describe the various contexts:

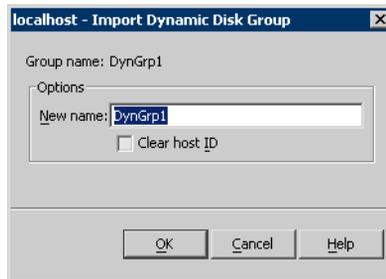
Note: Because a volume can span more than one disk (such as with a mirrored or RAID-5 volume), it is important that you first verify your disk configurations and then move all the disks that are part of the volume. If you do not move all the disks, the volume will have a Degraded or a Failed error condition.

- Use **Import Dynamic Disk Group** to bring a Foreign disk online if the disk was part of a dynamic disk group that was created on another computer and moved to the current computer.

Note: Microsoft Disk Management Disk Groups do not support the **Import Dynamic Disk Group** command.

To add a foreign disk that was created on another computer

- 1 Right-click on the disk and select **Import Dynamic Disk Group**.
A dialog box comes up that displays the name of the dynamic disk group.



- 2 Indicate the name for the dynamic disk group as follows:
 - If you want to leave the name as is, click **OK**.
 - If you want a new name for the dynamic disk group, type a new name for the group in the **New name** entry box and then click **OK**.
- 3 If you are importing a dynamic disk group from a different system, then click the checkbox to clear the host ID of the other system.
The disk group then imports. All existing volumes on the disk will be visible and accessible.
For more information on importing and deporting dynamic disk groups, see [“Importing and deporting dynamic disk groups”](#) on page 205.
 - Use **Import Dynamic Disk Group** if the Foreign disk has a secondary dynamic disk group (that is, a dynamic disk group other than the dynamic disk group containing the computer’s boot or system disk) and you have switched between operating systems on a dual-boot machine.
When you have one or more secondary dynamic disk groups on a disk in a dual-boot environment, the disk will be marked as Foreign when you switch between operating systems, because the secondary disk groups are not automatically imported. A shared primary dynamic disk group on a disk in that situation is automatically imported.
 - Use **Merge Foreign Disk** if the disk was originally created on the current computer but was removed and now you have reattached it to the current computer and want to restore it to its status as a member its original dynamic disk group.

See [“Merge foreign disk command”](#) on page 487.

Bring a basic volume back to a healthy state

To bring a basic volume back to a healthy state

- 1 Repair any disk or controller problems, and make sure that the disk is turned on, plugged in, and attached to the computer.
- 2 Use the **Rescan** command to rescan all the devices on the SCSI bus to bring the disk that the volume belongs to back online.
 Select **Rescan** from the **Actions** menu, or right-click the StorageAgent node in the tree view and select **Rescan** from the context menu. If you have a lot of devices on the computer’s SCSI bus, the rescan of the bus may take some time.
 See [“Rescan command”](#) on page 485.

Bring a dynamic volume back to a healthy state

To bring a dynamic volume back to a healthy state

- 1 First you need to attempt to bring the disk or disks to which the volume belongs to Online status by doing a **Rescan** and, if necessary, a **Reactivate Disk**.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Disk** command.

See [“Rescan command”](#) on page 485.

See [“Reactivate disk command”](#) on page 491.

If one of the disks has failed and you have a mirrored or RAID-5 volume, the repair involves recreating part of the volume in a different location.

See [“Repair volume command for dynamic RAID-5 volumes”](#) on page 493.

See [“Repair volume command for dynamic mirrored volumes”](#) on page 493.

- 2 If a disk comes back online after reactivating, check to see whether its volumes are healthy. If not, try the **Reactivate Volume** command on its volumes.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Volume** command.

See [“Reactivate volume command”](#) on page 492.

- 3 Run **Chkdsk.exe** to make sure that the underlying file system structure is intact.

To run **Chkdsk**, open a command prompt window and enter the following command:

chkdsk x: /f

where *x* is the drive letter of the volume you want to check. The **/f** option tells **Chkdsk** to fix any errors it finds. If the **/f** option is omitted, **Chkdsk** will operate in a read-only mode.

Although **Chkdsk** will clean up the file system structure, there may still be invalid data on the disk if users were working when a problem occurred on the disk. It is highly recommended that you run utilities to check the integrity of the data. If the data is corrupted, you will need to replace it from backup storage.

Repair a volume with degraded data after moving disks between computers

This section gives steps you can take if you used the **Deport Dynamic Disk Group** and **Import Dynamic Disk Group** commands to move disks between computers and the disks contain mirrored or RAID-5 dynamic volumes with degraded data.

To resolve the problem:

- 1 Deport the disks on the computer they were moved to and then physically move the disks back to the computer where they originated.
- 2 Use **Rescan** to make sure all the disks are installed correctly.
If the volume showed Degraded status before the disks were moved, the volume will still show Degraded status when the disks are moved back.
- 3 Make sure the status of the disk that contained the degraded mirror or parity information is not Offline.
If the status is Offline, check for any hardware problems, and reconnect the disk, if necessary.
- 4 Use the **Reactivate Disk** command to bring the disk back online.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Disk** command.

If the hardware problem is corrected, the disk will show Healthy status, and any mirrored volumes on the disk will be resynchronized and any RAID-5 volumes will regenerate parity.

- 5 If any volume still shows Degraded status, use the **Reactivate Volume** command on that volume.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Volume** command.

Veritas Storage Foundation for Windows will attempt to bring the volume back online. You may see a warning message indicating that Veritas Storage Foundation for Windows may not be able to bring back all of the data on the volume.

If Veritas Storage Foundation for Windows successfully brings the volume back online, the status of the volume becomes Healthy.

- 6 Now you can deport the dynamic disk group and move all the dynamic disk group's disks to the second computer.

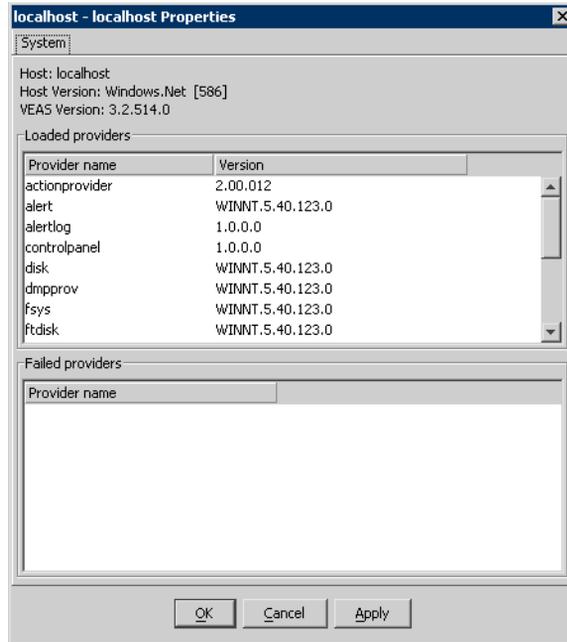
Be sure to move all the disks involved in the disk group at the same time to ensure that your volumes will have the Healthy status on the second computer.

Deal with a provider error on startup

In Veritas Storage Foundation for Windows, providers are similar to drivers. Each provider manages a specific hardware or software storage component. For example, there is a disk provider that manages all disks that the Windows operating system sees as disks. The providers discover the existing physical and logical entities and store that information in the Veritas Storage Foundation for Windows distributed database.

If you receive an error at Veritas Storage Foundation for Windows startup that a provider failed to load, you can check the provider status by right-clicking the managed server node in the Veritas Enterprise Administrator tree view and selecting **Properties** from the context menu that appears. An example of the Properties window is shown in the screen below.

Figure 10-2 Computer node properties window



The top section of the window displays the loaded providers. The bottom section of the window displays any providers that failed to load. Normally, the bottom section is blank.

If a certain provider failed to load at SFW startup, the features that the provider supplies will not work in SFW. It is necessary to determine why the provider did not load and start the application again. For assistance, contact Symantec Technical Support at the following web site:

<http://www.symantec.com/business/support/index.jsp>

Commands or procedures used in troubleshooting and recovery

The section covers the following topics:

- [Refresh command](#)
- [Rescan command](#)
- [Replace disk command](#)
- [Merge foreign disk command](#)
- [Reactivate disk command](#)
- [Reactivate volume command](#)
- [Repair volume command for dynamic RAID-5 volumes](#)
- [Repair volume command for dynamic mirrored volumes](#)
- [Starting and stopping the Veritas Storage Foundation for Windows Service](#)
- [Accessing the CLI history](#)

Refresh command

If you do not believe that anything is wrong with the disks or volumes but the GUI has not updated a recent change, try the **Refresh** command. **Refresh** refreshes drive letter, file system, volume, and removable-media information on the current computer. It also checks to see whether previously unreadable volumes are now readable. It may not pick up disk changes that occurred since the last reboot or rescan if there was no I/O occurring on the changed disk.

Select **Refresh** from the **Actions** or **View** menu, or right-click the StorageAgent node in the tree view to get a context menu and select **Refresh** from that menu.

Note: The **Refresh** command is only effective on the StorageAgent node and any of its sub-nodes.

Rescan command

The **Rescan** command rescans the SCSI bus for disk changes. It also does the equivalent of the **Refresh** command, updating information on drive letter, file system, volume, and removable media.

It is recommended that you use **Rescan** every time you make disk changes, such as removing or adding a disk. Rescanning can take several minutes, depending on the number of devices on the SCSI bus.

From the toolbar, select **Actions**, then **Rescan**.

A progress bar showing the percentage of completion for the rescan process is available by clicking on the **Tasks** tab located in the lower pane. When **Rescan** is finished, you should see accurate information about your system.

If error flags remain, you may need to reactivate the disks or volumes.

Note: The **Rescan** command is only effective on the StorageAgent node and any of its sub-nodes.

Additional important information about the rescan command

This section gives additional information on how a rescan affects redundant and nonredundant volumes.

Redundant volumes (Mirrored and RAID-5)

If a RAID-5 or a mirrored volume is in a Degraded state, doing a rescan also will automatically trigger an attempt to reactivate the disks and resynchronize the volume on the disks. This is done in the background and is the reason why it is not always necessary to invoke the **Reactivate Disk** and **Reactivate Volume** commands.

Nonredundant volumes (Simple, spanned, and striped)

If you have a simple, spanned, or striped volume that has failed, a rescan will NOT automatically attempt to reactivate the disk and the volumes. The data on these failed volumes may already be corrupted.

For a failed simple, spanned, or striped volume, you must manually reactivate the disk(s) and the volume. The error messages you receive may give you a hint of the reason for the problem. After manually reactivating the disk(s) and volume, the disks may come back as Online and the volume as Healthy, but you cannot assume that the underlying data has not been affected.

In this situation, you should also run **Chkdsk**. Although **Chkdsk** will clean up the file system structure, there may still be invalid data on the disk if users were working when a problem occurred on the disk. It is highly recommended that you run utilities to check the integrity of the data. If the data is corrupted, you will need to replace it from backup storage.

Note: If you have mirrored or RAID-5 volumes with a Failed state, a rescan will not automatically reactivate the disks and resynchronize the volumes on the disks. Once a redundant volume has failed, it is subject to the same conditions as a failed nonredundant volume.

Replace disk command

This command allows you to replace a failed disk with an empty basic disk. The volume configuration will be recreated on the new disk. The contents of the nonredundant volumes are not guaranteed. Redundant volumes will be automatically resynchronized. This command can be performed only for a disk that is designated as “Missing.”

See “[Replace disk](#)” on page 148.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Replace Disk** command.

Merge foreign disk command

If you remove a disk from the server and also remove it in Veritas Storage Foundation for Windows and then decide to reattach it to the server as a member of the same dynamic disk group, you will need to use the **Merge Foreign Disk** command. This command will reinstate the disk to its old status as a member of its former dynamic disk group on that server.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Merge Foreign Disk** command.

You will also need to use this command if you remove a disk without taking its disk group offline, move the disk to another server, and then attempt to reinstall it in the original server. The command is necessary in this case because the disk has the other server’s disk group ID.

In Veritas Storage Foundation for Windows, this command will probably not need to be used very often, because if a disk is removed from a computer that has subdisks from a redundant volume (such as a RAID-5 volume or a mirrored volume), the **Hot Relocation** command will automatically rebuild the missing subdisk on the volume. However, if the hot relocation feature is turned off, you may need this command.

See “[Hot relocation](#)” on page 268.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support hot relocation.

To use the merge foreign disk command

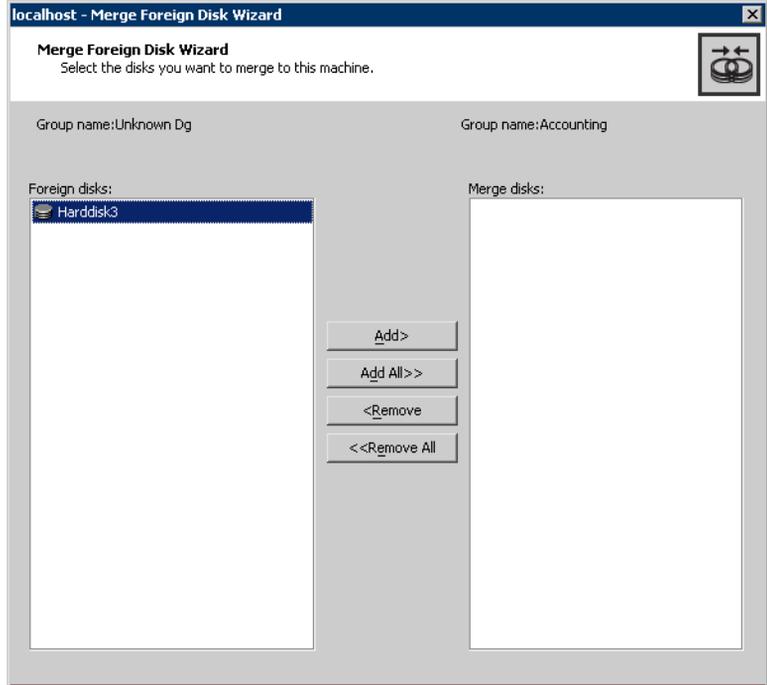
- 1 Reattach the disk to the original server.

- 2 In the VEA console, do a rescan (select **Rescan** from the **Actions** menu). The disk will show up in the tree with a red X. Its dynamic disk group will display as “Unknown Group.”
- 3 Right-click the disk label in the tree view to bring up the disk context menu.

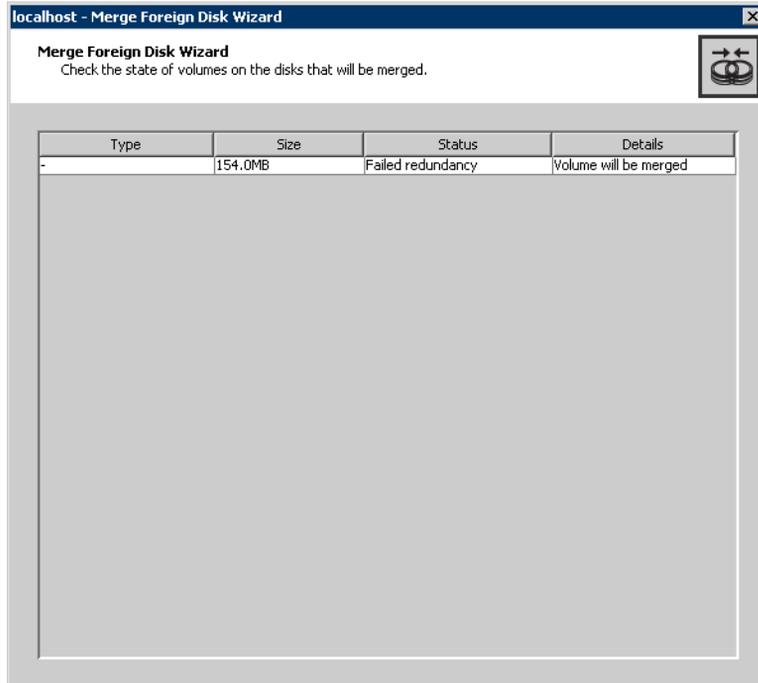


- 4 Select **Merge Foreign Disk** from the disk context menu.
- 5 After reading the first screen of the Merge Foreign Disk wizard, click **Next** to continue.
- 6 In the Merge Foreign Disk wizard screen that appears next, make sure that the disk that you want to merge is shown in the pane on the right side of the

screen (using the **Add** button to move it from the left pane of the screen to the right pane), and then click **Next** to continue.



- 7 In the next screen, click **Next** to continue if the data condition on the disk is Healthy.



The final screen of the Merge Foreign Disk wizard appears. The volume condition types are shown below:

Volume Condition	Details
Failed	Volume is not functional. Volume will be merged, may be unusable.
Failed Redundancy	Volume contents will not be current. Volume will be merged.
Missing	Volume does not have a subdisk on merged disks.

If the volume condition type is Failed, there is no guarantee that the data will be intact (though it may be).

See "[Bring a dynamic volume back to a healthy state](#)" on page 481.

If the disk is Missing, make sure that it is properly connected.

- 8 Click **Finish** to complete the process of merging the Foreign disk into the server.

The merged disk should now appear as it was before it was removed from the server. It should now be shown as being in its former dynamic disk group.

- 9 If the disk still has an error symbol, right-click the disk and click **Reactivate Disk** from the context menu that appears.
 The disk now should appear as normal.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Disk** command.

If you have a dynamic disk group with one disk marked as Missing and you revert the remaining disks in the group to basic, the dynamic disk group will no longer exist, and the disk marked as Missing will also disappear from the Veritas Storage Foundation for Windows GUI. This happens because the information about a dynamic disk group is stored in a database on each of the disks that reside in the group. The dynamic disk group information is no longer available from the disks that were reverted to basic, and the Missing disk is not connected. If you reconnect the Missing disk and rescan, it will show up as Foreign. Now its database is available, but the remaining disks in the group are gone.

For more information on removing a dynamic disk from the computer, see [“Remove a disk from the computer”](#) on page 145.

Reactivate disk command

Occasionally, **Rescan** will not clear error flags on a dynamic disk. When this happens, you can use **Reactivate Disk** to clear these flags. This command does a manual restart on a disk. Dynamic disks that are marked as Missing or Offline can be reactivated. After reactivating, disks should be marked as Online if they are attached and are not in a Failed condition.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Disk** command.

To clear error flags using the reactivate disk command

- 1 Right-click the disk with the error flags and select **Reactivate Disk** from the context menu that appears.

A dialog box appears with a confirmation message.



- 2 Click **Yes** to reactivate the disk.
The disk should be marked Online after it is reactivated unless there is a mechanical or other serious problem with the disk.
See also “[Additional important information about the rescan command](#)” on page 486.

Reactivate volume command

If you have errors on a dynamic volume, you must try to bring any disks on which it resides back online by first using **Rescan** and then, if that does not work, **Reactivate Disk**.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Disk** command.

Once the disk or disks come back online, if the volume does not return to a Healthy state, use the **Reactivate Volume** command.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Reactivate Volume** command.

Right-click on the volume to bring up the context menu, and then click **Reactivate Volume**.

This can be necessary if any of the mirrors or plexes of a mirrored volume are still not healthy. The same situation applies to a RAID-5 volume; you may need to use **Reactivate Volume** to allow the volume to regenerate.

If the underlying disks for a volume are sound, the volume most likely will come back to a Healthy state, but the data on it may be corrupted or stale. It is recommended that you run **Chkdsk.exe** before using the volume. If Chkdsk fails or finds an excessive number of errors, you may need to reformat the volume and restore its contents from backup.

The difference between the **Reactivate Volume** and **Repair Volume** commands is that **Reactivate Volume** resynchronizes the volume to bring it to a Healthy state

in its existing location, while **Repair Volume** removes the damaged section of the volume and recreates it in another location on a healthy dynamic disk.

See also “[Additional important information about the rescan command](#)” on page 486.

Repair volume command for dynamic RAID-5 volumes

You can repair a RAID-5 volume if its status is Degraded and if there is enough unallocated space available on other dynamic disks to recreate the degraded subdisks of the volume. To avoid data loss, you should attempt to repair the volume as soon as possible.

Note: After a disk fails, you may need to rescan before this menu option is available.

The difference between the **Reactivate Volume** and **Repair Volume** commands is that **Reactivate Volume** resynchronizes the volume to bring it to a Healthy state in its existing location, while **Repair Volume** removes the damaged section of the volume and recreates it in another location on a healthy dynamic disk.

To repair a dynamic RAID-5 volume using the repair volume command

- 1 Right-click the degraded volume. Select **Repair Volume** from the context menu that appears.
 The Repair Volume dialog box appears.
- 2 The default setting is for Veritas Storage Foundation for Windows to automatically assign the destination disks. To manually select the disks, click the **Manually assign destination disks** radio button and then select the disks you want assigned as destination disks. You may also check **Disable Track Alignment** to disable track alignment for the recreated volume.
- 3 When you are satisfied with your selection, click **OK**.

Repair volume command for dynamic mirrored volumes

When a disk on which a mirrored volume resides fails, the volume displays a Degraded status. The disk’s name is changed to Missing Disk, and an icon (X) appears on the Missing Disk icon. The status of the disk will be Offline.

The difference between the **Reactivate Volume** and **Repair Volume** commands is that **Reactivate Volume** resynchronizes the volume to bring it to a Healthy state in its existing location, while **Repair Volume** removes the damaged section of the volume and recreates it in another location on a healthy dynamic disk.

To repair a mirrored volume using the repair volume command

- 1 Right-click the degraded volume. Select **Repair Volume** from the context menu that appears.
The Repair Volume dialog box appears.
- 2 Select the mirror or mirrors to repair by clicking in the corresponding checkboxes. You may also check **Disable Track Alignment** to disable track alignment for the recreated mirrors.
- 3 Click **OK**.
New mirrors will be created on available disk space on other dynamic disks.

To repair a volume and manually select the target disks for the new mirrors

- 1 Right-click the degraded volume. Select **Mirror** from the context menu, then **Remove** from the submenu.
The **Remove Mirror** dialog box appears.
- 2 Remove the degraded mirror.
See “[Remove mirror](#)” on page 261.
Note that the mirrors on preserved disks (in the right pane) will not be removed.
- 3 Right-click the volume again. Select **Mirror** from the context menu, then **Add** from the submenu.
- 4 Manually select the target disk to add the mirror to and then click **OK**.
See “[Add a mirror to a volume](#)” on page 258.

Starting and stopping the Veritas Storage Foundation for Windows Service

It is useful to know how to start and stop the Veritas Storage Foundation for Windows service when you are troubleshooting. For example, if Veritas Storage Foundation for Windows stops running on the server, you can try restarting the service instead of rebooting. Sometimes stopping the service and restarting it again can resolve temporary problems. The Veritas Storage Foundation for Windows service is also referred to as the Veritas Object Bus or vxvm.

Note: For the current release, to start or stop the Veritas Storage Foundation for Windows service you start or stop the vxvm service (or the Veritas StorageAgent in the Windows Services GUI). This is different from earlier releases where you would start or stop the vxob service.

To start the Veritas Storage foundation for Windows service

Bring up the command window and enter the following command:

```
net start vxvm
```

Note: If you reboot, the service is automatically restarted.

To stop the Veritas Storage foundation for Windows service

Bring up the command window and enter the following command:

```
net stop vxvm
```

Accessing the CLI history

The history of CLI commands issued on a system and the system responses is contained in the command line log, vxcli.log. It is typically located at **C:\Program Files\Veritas\Veritas Volume Manager 5.1\logs**. This history is useful when trying to understand the problems that may arise from running or creating CLI scripts.

Each entry in the log is prefixed with the date and time of the command or system response, followed by the process identification and thread identification. Each CLI command is a separate entry in the log and each is identified by " ----- Command : ". Each system response is also a separate entry in the log and follows the CLI command.

Note: Help messages are not recorded in the command line log.

Additional troubleshooting issues

This section contains additional troubleshooting issues.

The topics are organized in the following areas:

- [Disk issues](#)
- [Volume issues](#)
- [Disk group issues](#)
- [Connection issues](#)
- [Issues related to boot or reboot](#)
- [Cluster issues](#)
- [Dynamic multi-pathing issues](#)
- [vxsnap issues](#)
- [vxsnapsql issues](#)
- [Other issues](#)

Disk issues

This section has the following issues:

- [Disk type shows no signature](#)
- [A disk is marked as foreign](#)
- [Error when upgrading a basic disk to dynamic](#)

Disk type shows no signature

If the type of disk shows No Signature, you need to write a signature to the disk. When installing a new disk, the software must write a signature to the disk that prepares it for use. This signature is not written automatically, in case that disk has been imported from another operating system and the configuration information needs to be kept intact.

Check the following:

- To write the configuration data to the disk, right-click on the disk under the **Disks** node and choose **Write Signature**.

A disk is marked as foreign

Information about foreign disks is covered in the following topics:

- [Bring a foreign disk back to an online state](#)

- [Disk status descriptions](#)

Error when upgrading a basic disk to dynamic

This topic describes known problems when upgrading a basic disk to dynamic.

Basic disk has more than 32 logical drives

If you attempt to upgrade a basic disk that has more than 32 logical drives in its extended partition, it will not upgrade to a dynamic disk. You will get the error message “Disk cannot be partitioned after it has been upgraded.” There is a limit of 16 logical drives for a basic disk to be upgraded to a dynamic disk.

Basic disk has an “Active” volume with no system files

If you mark a basic mirrored volume active that does not contain the current system files, the computer will not be able to reboot. A basic disk that contains an unbootable active volume cannot be upgraded to dynamic.

You receive an error about disk geometry

If you receive an error about disk geometry when you are trying to upgrade a basic disk to a dynamic disk and the disk does not upgrade, the geometry on the disk is inconsistent with the disk geometry used on the current Windows operating system. If the disk is not upgraded, Veritas Storage Foundation for Windows maintains the disk with its current partition structure; but if the partition structure is changed in any way, the disk partitions and their data become inaccessible.

The fix for the situation, which is described in the error message, is:

- Back up all your data from the affected disk.
- Delete all partitions on the disk.
- Upgrade the disk to dynamic.
- Create volumes on the disk.
- Restore your data to the disk.

It is very likely that you have a disk that was created under NT 4.0 with partitions on it and this disk has a different geometry because it was attached to a secondary host bus adapter with the BIOS turned off and mapping features turned off.

Once you have done the above steps, the disk will have the proper geometry and can still be connected to the secondary host adapter with the BIOS and mapping features turned off. The geometry problem was the result of the change from NT 4.0 to Windows 2000. It is a known problem and is discussed in more detail on the Microsoft web site.

Volume issues

This section has the following issues:

- [Cannot create a RAID-5 volume](#)
- [Cannot create a mirror](#)
- [Cannot extend a volume](#)
- [Cannot extend a dynamic boot or system volume](#)
- [When creating a spanned volume over multiple disks within a disk group, you are unable to customize the size of subdisks on each disk](#)
- [An attempt to mirror a boot or system volume fails or has an error message](#)

Cannot create a RAID-5 volume

Check the following:

- Adequate unallocated space on three or more disks? You must have at least three disks to create a RAID-5 volume or four disks to create a RAID-5 volume with a log.

Cannot create a mirror

Check the following:

- Adequate unallocated space on two or more dynamic disks? You must have two or more disks to create a mirrored volume.

See also “[An attempt to mirror a boot or system volume fails or has an error message](#)” on page 499.

Cannot extend a volume

One possible reason for not being able to extend a volume is that the RAID-5 or DRL log that was associated with the volume cannot be found, possibly because a disk has failed or is offline. The workaround is to delete the log from the failed disk or bring the missing disk back online, and then you should be able to extend the volume. If your volume has a boot or system disk, see the next section.

Cannot extend a dynamic boot or system volume

- A boot or system volume cannot be extended unless there is enough contiguous space after the volume for the desired extension. If you have another volume on the disk, you cannot use space before that volume and after that volume for the extension.

- If the extension of a dynamic boot or system volume requires adjustment of an extended partition boundary, then the extension will not be allowed. The error message “Requested operation not supported” will be returned.
- A boot or system disk volume that was originally created on a logical drive and later upgraded to a Veritas Storage Foundation for Windows dynamic volume cannot be extended in Veritas Storage Foundation for Windows.

When creating a spanned volume over multiple disks within a disk group, you are unable to customize the size of subdisks on each disk

When you create a spanned volume over multiple disks, Veritas Storage Foundation for Windows does not allow you to use the Custom mode to create subdisks of a specified size on the disks in the volume. Veritas Storage Foundation for Windows automatically uses all the available disk space in the first disk before moving to the second disk, and likewise does the same with the second disk before moving to the third, and so on.

To work around this problem, create a simple volume on the first disk with a specified size (the size will be a fraction of the total size needed). Once this is created, use the Expand Volume command with the Custom mode to specify additional space on another disk. Repeat for the total number of disks being used.

This technique will allow you to create a spanned volume with specific subdisk sizes on each disk in the group.

An attempt to mirror a boot or system volume fails or has an error message

There are several causes for this problem.

- **The Only Available Dynamic Disk Large Enough for the Mirror Has More than Two Retained Partitions**
 If you try to add a mirror to a system or boot disk but the only dynamic disks that have enough space contain more than two retained partitions, the Add Mirror operation will fail. The error message will say “insufficient disk space,” even though there is plenty of space on the disk.
- **No Available Dynamic Disk Has the Same Offset as the Original Boot or System Disk**
 In order to boot from a mirrored system volume, its offset from the beginning of the disk must be in the same location as that of the original system volume’s offset. If you try to add a mirror to a system volume where there are no dynamic disks that can have the offset in the same location, you will receive a message to that effect and be asked whether you wish to

continue. You can choose to continue, so that a mirror at a different offset will be created. The mirror will correctly mirror the data, but you cannot boot from the mirror.

Disk group issues

This section has the following issues:

- [Unknown group appears after upgrading a basic disk to dynamic and immediately deporting its dynamic disk group](#)
- [Cannot use SFW disk groups in disk management after uninstalling Veritas Storage foundation for Windows](#)
- [After uninstalling and reinstalling Veritas Storage foundation for windows, the private dynamic disk group protection is removed](#)
- [Cannot import a cluster dynamic disk group or a secondary disk group with private dynamic disk group protection when SCSI reservations have not been released](#)

If you are having a problem with the dynamic disk group split and join commands, see the following topic:

- [DGSJ troubleshooting tips](#)

Unknown group appears after upgrading a basic disk to dynamic and immediately deporting its dynamic disk group

Upgrading a basic disk and immediately deporting its dynamic disk group will occasionally result in the appearance of a dynamic disk group named “Unknown.” Refreshing the display or trying to import the deported dynamic disk group will remove the original group from the display and, in the case of import, generate an error that the disk could not be found.

Do NOT attempt any other operations on these disks from within Veritas Storage Foundation for Windows. Doing so can result in a loss of data. To recover the dynamic disk group and its contents requires a reboot of the computer. After rebooting, the dynamic disk group will display correctly as a deported group as “Offline, Foreign.” Then you can import it without any problems.

Cannot use SFW disk groups in disk management after uninstalling Veritas Storage foundation for Windows

After uninstalling Veritas Storage Foundation for Windows, the existing disk group may not be able to be imported and used in Disk Management.

When you uninstall Veritas Storage Foundation for Windows, Disk Management will automatically import only primary disk groups.

If, in Veritas Storage Foundation for Windows, you do not have a primary disk group because your system or boot disk is not encapsulated, and then you uninstall Veritas Storage Foundation for Windows, Disk Management will be unable to import the disk group or groups, because it cannot import a secondary disk group as a primary disk group. Without a primary disk group, you cannot merge the foreign disk group.

The workaround is to create a new dynamic disk group in Disk Management and then the Foreign disk group(s) can be merged into the dynamic disk group.

After uninstalling and reinstalling Veritas Storage foundation for windows, the private dynamic disk group protection is removed

If you uninstall Veritas Storage Foundation for Windows and then reinstall it again (either through an upgrade or for other purposes), the private dynamic disk group protection is removed during the uninstall process. If you then reinstall Veritas Storage Foundation for Windows and want to continue the private dynamic disk group protection for the disk groups that had it previously, add the feature back to the disk groups through the **Add Dynamic Disk Group Protection** command. Private dynamic disk group information is stored in the registry; and, by necessity, the registry entries are removed during an uninstall.

Cannot import a cluster dynamic disk group or a secondary disk group with private dynamic disk group protection when SCSI reservations have not been released

Importing a cluster dynamic disk group or a secondary disk group with private dynamic disk group protection may not be possible when a Storage Foundation server on a shared bus had failed to release SCSI reservations when the cluster dynamic disk group or secondary disk group was deported. Performing the clear SCSI reservation operation releases these reservations and allows importing the cluster dynamic disk group or secondary disk group.

To clear SCSI reservation

- 1 Select the StorageAgent node in the VEA tree view and click **Actions>Clear SCSI reservation**.
 Alternatively, you may right-click the Storage Agent node and select **Clear SCSI reservation** on the context menu.
- 2 Review the information message in the window that appears and click **Yes** to complete the operation.

Connection issues

This section describes computer connection issues.

When attempting to connect to a remote computer, you are denied access or get an error message

This topic describes situations where you are unable to connect to a remote computer.

Most common situation

If, from within Veritas Storage Foundation for Windows, you attempt to connect to a remote computer but are denied access, your situation probably falls under one of the two following conditions:

- You are logged on to a local server that is not in any domain.
- You are logged on to a domain, but that domain does not contain the remote server. Also your domain does not have a trust relationship with the domain that the remote server is in.

The workaround in this situation is to create an account on the local machine that has the name and password that are the same as the administrator name and password of the remote computer and then use that account to log on to the local machine.

Client-only installation

Another situation where you may get an error message is when you have just done a client-only installation of SFW and you bring up the SFW client and attempt to connect to a remote server that has Disk Management.

Veritas Storage Foundation for Windows assumes that its client will connect first to a remote server running SFW or Volume Manager for Windows before connecting to a system running Disk Management.

Once you connect to a server with SFW or Volume Manager for Windows, you will then be able to connect successfully to a remote system running Disk Management.

Note: Windows Disk Management is the disk and volume management program that comes with the Windows operating system. Veritas Storage Foundation for Windows can connect to a remote server with Disk Management because the Disk Management software was jointly developed by Veritas and Microsoft.

Error message: “The connection to *RemoteComputer* has terminated. *RemoteComputer* will be removed from view.”

The remote computer that you were connected to has been disconnected from your console. Most often there is a problem with the network connection and the transmissions timed out. This can also occur if the remote machine was restarted or the Veritas Storage Foundation for Windows service on the remote machine was stopped. You can also get the message “Connection Failed” instead.

Check:

- Make sure that the remote machine is turned on and available to the network and that the service is started.
- Reconnect to the remote computer.

Issues related to boot or reboot

This section has the following issues:

- [During reboot, a message may appear about a “Corrupt drive” and suggest that you run autocheck](#)
- [Error that the boot device is inaccessible, bugcheck 7B](#)
- [Error message “vxboot- failed to auto-import disk group repltest_dg. all volumes of the disk group are not available.”](#)

See also the issue [“Cannot extend a dynamic boot or system volume”](#) on page 498.

During reboot, a message may appear about a “Corrupt drive” and suggest that you run autocheck

Let autocheck run, but do not worry about the message. Autocheck will finish and the reboot will be complete. Depending on the size of the system, this may take quite a while.

Error that the boot device is inaccessible, bugcheck 7B

There are two known situations that can result in this message:

After a Dynamic Disk Group with a Boot Device Has Been Renamed

A dynamic disk group that contains a boot volume should not be renamed when the dynamic disk group is imported. Normally, SFW does not allow you to deport a dynamic disk group that contains the current boot volume. However, if you move a disk to another system or boot from another boot volume in a different dynamic disk group on the same system, you will then be able to deport the dynamic disk group that contains the boot volume.

Booting from a boot volume contained in a renamed dynamic disk group can, under certain circumstances, cause the error message “Bugcheck 7B, Inaccessible Boot Device.”

When Attempting to Boot from a Stale or Damaged Boot Plex

If you get the error message “Bugcheck 7B, Inaccessible Boot Device” and the boot volume is mirrored, try booting off one of the other mirrors. You are not allowed to boot from a stale mirror. A stale mirror is one that was detached because it was missing at some point or because it had errors.

Error message “vxboot- failed to auto-import disk group repltest_dg. all volumes of the disk group are not available.”

The situation that causes the error message is that disks from a dynamic disk group in SFW have been removed without being deported, deleted, or converted

to basic disks. The next time the computer is rebooted, SFW expects to find these disks so that the disk group can be autoimported and when the disks are not there, the error message is generated.

Even when you have uninstalled SFW and reinstalled it again, information about the disk group is retained in the registry because it is needed in upgrading from one version of the program to the next.

If you are not planning to use the disk group again, you need to remove the record of that disk group from the registry; otherwise, you will continue to get this message on reboot. Here are the steps to do so:

- 1 Run the command **Regedit** to bring up the Registry Editor window.
- 2 Locate the reference to the disk group in the registry. It is under the following key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vxio\Boot Info\Disk Group 1, Disk Group 2, ...`
- 3 The disk groups are not listed by the actual name, only by a general name of Disk Group 1, Disk Group 2, and so on. To determine which disk group to delete, click the general name to see a further listing that includes the actual name of the disk group.
- 4 Once you have determined which disk group to delete, highlight its general name (such as Disk Group 2) and hit the **Delete** key.

Cluster issues

This section has the following issues:

- [Unable to bring a cluster disk group online when a minority of the disks in the disk group are available](#)
- [Problem on a SQL server system with Microsoft Clustering when migrating to a dynamic mirrored quorum volume on a volume Manager disk group resource](#)

Unable to bring a cluster disk group online when a minority of the disks in the disk group are available

Safeguards are put into effect so that normally you cannot bring a cluster disk group online on a node when a minority of disks in the disk group are available. However, in certain situations, you may want to force the import of the disk group or find some other way to bring the disk group online. One example is a campus cluster situation with a two-node cluster, where each node of the cluster is located in a separate physical location and each node has an even number of disks, with the disks evenly distributed between the two sites. In such a

situation, if one site goes down, the remaining site will not be able to access the cluster data because it cannot reserve a majority of the disks in the disk groups. With both Microsoft Clustering and other cluster types, there are methods to allow a site with a minority of the disks to bring disk groups online, if necessary, until the site with failed equipment can be repaired. The following section describes these methods.

To bring a cluster online that has a minority of the disks in the cluster

Caution: When bringing a cluster disk group online with a minority of cluster disks, make sure that a majority of the disk group disks are NOT online on any other cluster node before (and after) onlining the disk group. If a majority of disk group disks are online on another node, data corruption can occur.

- If you have a cluster, use the following `vxclus` command for each disk group on your cluster node:

```
vxclus enable -g<DynamicDiskGroupName>
```

You will be asked to confirm the use of this command.
If necessary, start the cluster service (`clusvc`) if the cluster service has stopped because of a dynamic quorum resource failure.
Then, using the Windows Server 2003 Cluster Administrator or Windows Server 2008 Failover Cluster Management, bring the cluster disk groups online.
For more on the `vxclus` utility, see “[vxclus](#)” on page 325.
- If you have any other cluster type, enter the following command at the command line to receive further information on how to force an import of a cluster disk group when the cluster disk group does not have a majority of disks available.

```
vxdg -g<DynamicDiskGroupName> -s import
```

A message comes up describing the command for forcing the import and giving cautions about the use of the command.
Enter the command to force the import as follows:

```
vxdg -g<DynamicDiskGroupName> -s -f import
```

You will be asked to confirm the use of this command.

For more information about campus clusters, see the white paper “Campus Clustering: Using Veritas Volume Manager for Windows with Microsoft Cluster Server (MSCS)” at:

<http://prod.veritas.com/Products/vnet?c=collateral&refId=31>

Problem on a SQL server system with Microsoft Clustering when migrating to a dynamic mirrored quorum volume on a volume Manager disk group resource

If you have a system running SQL Server with Microsoft Clustering (MSCS on Windows Server 2003; or Failover Cluster feature of Windows Server 2008) and decide to migrate the quorum volume from a non-fault-tolerant physical disk resource to a dynamic mirrored volume on a Volume Manager Disk Group resource, you should be aware that the cluster may have a Microsoft Distributed Transaction Coordinator (MSDTC) resource that has a dependency on the physical disk resource. If this is the case, you may need to take special steps to move the MSDTC resource to the new mirrored quorum volume.

MSDTC is a component used by SQL Server to manage distributed transactions and some replication functions. To determine whether MSDTC has a dependency on the physical disk resource, use the Windows Server 2003 Cluster Administrator or Windows Server 2008 Failover Cluster Management to view the resources in Cluster Group. If there is a resource named MSDTC, right-click on it and select Properties. Select the Dependencies tab. If the MSDTC resource has a dependency on the physical disk quorum volume, you can create the dynamic mirrored quorum, but you cannot remove the physical disk resource that contained the old quorum volume from Cluster Group until you have reassigned the MSDTC resource to a fault-tolerant volume.

You can leave the MSDTC resource on the physical disk resource that formerly held the quorum volume. However, since the log file contains critical transaction data, Microsoft recommends that it be located on a mirrored volume for maximum reliability. For more information about MSDTC, refer to Microsoft's SQL Server and COM+ (Component Services) documentation.

If you decide to move the MSDTC resource to the new quorum volume, it must be done with care to avoid the loss of any information related to unresolved transactions. Instructions on how to move the MSDTC resource can be found on the Microsoft Support web site in the article "HOWTO: Rebuild or Move MSDTC Used With a SQL Fail-Over Cluster" (Q294209) at:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q294209>

This link was accurate when this manual was written, but the link may change in the future.

Dynamic multi-pathing issues

This section has the following issues:

- [When a dynamic multi-pathing license is no longer valid](#)
- [When an unknown disk group appears in a dynamic multi-pathing environment](#)

Note: Look in the SFW Release Notes for documentation of additional issues relating to Dynamic Multi-pathing. Also, refer to the Hardware Compatibility List on the technical support web site for the list of equipment that has been tested to work with Dynamic Multi-pathing.

When a dynamic multi-pathing license is no longer valid

If you have a demo license and have DMP DSMs installed on an array and your demo license expires or you replace the demo license key with a permanent license key that does not include Dynamic Multi-pathing, the program will not allow you to make changes to your settings. However, all of your current settings will remain in effect. You need to purchase a license that enables Dynamic Multi-pathing to make any additional changes to your settings.

When an unknown disk group appears in a dynamic multi-pathing environment

When an unknown disk group appears in a Dynamic Multi-pathing environment, it is likely that there is a problem with a path to a storage array or that a storage array was not placed under the control of Dynamic Multi-pathing. Make sure that all paths are healthy and perform a rescan of all the disks and recheck the status of the disk groups.

vxsnap issues

This section contains a general issue with `vxsnap` and a listing of `vxsnap` error codes with suggested actions to take for each error code.

For a description of the `vxsnap` CLI command, see “[vxsnap](#)” on page 407.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxsnap` command.

General issue

When performing a roll-forward recovery to the point of failure with at least 1,008 log files, you may encounter an Exchange initialization error. If you encounter this issue, rename the checkpoint file back to the original name and remount the database stores using Exchange System Manager.

The Microsoft Knowledge Base Article #812962 (<http://support.microsoft.com/default.aspx?scid=kb;en-us;812962>) describes this situation in an Exchange 2000 environment.

Note: The above URL is accurate as of this writing but may be subject to change in the future.

vxsnap command error codes

Occasionally, you may encounter a `vxsnap` error code. For example, the following command can result in the error code 8004230e, if there are conditions that cause the `vxsnap` operation to fail.

C:\Documents and Settings\Administrator>vxsnap create source=A:

Failed to complete the operation...

8004230e:

Error code 8004230e is probably the most common `vxsnap` error code and can occur for several different reasons. In the list below, error code 8004230e and other codes are given, along with suggested actions to take to overcome the error condition.

ERROR CODE: 8004230e

VSS snapshot is not supported for the volume(s).

- 1 Possible Reason: Basic partition on a basic disk was used.
 Suggested Action: Create a new dynamic disk group or add the disk to an existing dynamic disk group of SFW.

- 2 Possible Reason: Dynamic disk group version is an earlier version than 4.0 version, when vxsnap was introduced.
Suggested Action: Upgrade the dynamic disk group to the 5.1 version.
- 3 Possible Reason: Snapshot operation is not supported.
Suggested Action: Purchase FlashSnap license and install the FlashSnap option.

ERROR CODE: 80042316

VSS snapshot already in progress.

- 1 Possible Reason: Another VSS job is running.
Suggested Action: VSS supports only one job at a time. Wait for the other job to finish and then retry the command.
- 2 Possible Reason: A VSS job was abruptly terminated, leaving the VSS Service in an intermediate state.
Suggested Action: Wait for at least 3 minutes for VSS to reset the state, or, if you are sure there is not another job running, restart the Volume Shadow Copy Service. The Services console is located at **Start>All Programs>Administrative Tools>Services**.

ERROR CODE: 80042301

The VSS service timed out.

Suggested Action: Wait for at least 3 minutes, then retry.

Suggested Action: When using the `vxsnap` command to snapshot multiple volumes under stress conditions, close the VEA GUI and retry the `vxsnap` command.

ERROR CODE: e5090008

The path cannot be used for creating a drive path.

Suggested Action: Make sure that the folder used for the drive path is an empty NTFS folder on the local computer.

vxsnapsql issues

This section has the following issues:

- [When moving a snapshot set](#)
- [When changing the drive letter of a volume containing datafiles or log files](#)
- [When consolidating database files and log files to the same disk group](#)

For a description of the `vxsnapsql` CLI command, see “[vxsnapsql](#)” on page 447.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxsnapsql` command.

When moving a snapshot set

If a disk group contains the SQL database files and another disk group contains the SQL database log files, and a disk group join operation is used to consolidate these database and log files into one disk group, the MSSQLServer service must be stopped and restarted after the disk group join operation completes. The `vxsnapsql create` and the `vxsnapsql restore` commands fail with a device not found error, if the MSSQLServer service is not stopped and restarted.

When changing the drive letter of a volume containing datafiles or log files

If you change the drive letter of a volume that contains datafiles or log files, the MSSQLServer service must be stopped and restarted to update this change with the SQL Server. A device not ready error occurs if the service is not stopped and restarted.

When consolidating database files and log files to the same disk group

The `vxsnapsql` utility requires that a SQL user-defined database volume and its associated log volume be located in the same disk group. If SQL user-defined database files and log files are initially configured on volumes in different disk groups and the disk groups are later consolidated using the disk group join operation, the MSSQLServer service must be stopped and restarted before issuing a `vxsnapsql create` or `vxsnapsql restore` command.

Other issues

This section has the following issues:

- [An option is grayed out](#)
- [Disk view on a mirrored volume does not display the DCO volume](#)

An option is grayed out

When an option is grayed out in a menu, the task cannot be performed on the object at this time. Certain operations are valid only for certain types of objects. If there is a task currently running on that object, wait until it has finished and try again. Otherwise, the operation may not be appropriate at this time.

Disk view on a mirrored volume does not display the DCO volume

The Disk View for a selected mirrored volume will not show the DCO volume if that DCO volume was moved to a disk that does not contain any of the other plexes of the mirrored volume. A DCO volume can be moved manually by the user through a subdisk move or it can be moved automatically with the hot relocation function when the subdisk has an I/O error.

If you select the Disk View for all disks (by selecting the Disks folder and clicking the **Disk View** tab in the right pane or by selecting **Disk View** from the Disks folder context menu), you can see the DCO volume. However, finding the DCO volume on all disks may not be practical if you have a large number of disks.

Automated System Recovery (ASR)

This section describes the Automated System Recovery (ASR) feature available in Microsoft Windows Server 2003 as it is supported by Veritas Storage Foundation for Windows.

Note: SFW does not support the Automated System Recovery (ASR) feature in Microsoft Windows Server 2008. For information about SFW and the backup and restore of disk groups and layouts of volumes, see the command, “[vxcbr](#)” on page 404.

This section covers the following topics:

- [Automated system recovery \(ASR\) overview](#)
- [SFW’s support for ASR](#)
- [ASR recovery process](#)
- [Cluster recovery](#)

Automated system recovery (ASR) overview

Automated System Recovery (ASR) is a disaster recovery feature that is part of the Microsoft Windows Server 2003 operating system. ASR extends the functionality of a traditional backup and restore application by providing an external mechanism to save information about the system state and configuration, including Veritas Storage Foundation for Windows information. ASR captures and stores the information to a floppy disk and tape or other backup media. Information saved includes the system registry, critical Windows files, and volume configuration information, including the number and type of partitions as well as file system and drive letter information. If a disaster or other event causes a computer to be unbootable, ASR can be used to restore the system to a bootable state and prepare it for data recovery. The actual data recovery needs to be done through backup software.

Veritas Storage Foundation for Windows supports ASR on systems running Microsoft Windows Server 2003 and any backup and restore application specifically designed to support ASR, such as Veritas Backup Exec or NTBackup, the backup utility packaged with Microsoft Windows Server 2003.

An ASR backup should be performed after the system is initially configured and repeated whenever there is a change in the system configuration. Examples of such changes include the creation of a new dynamic volume or installation of a patch or service pack.

Caution: As part of the ASR backup process, Veritas Storage Foundation for Windows saves the configuration information only of those dynamic disk groups that are currently imported on the system running the ASR backup. For example, in a cluster setup, configuration information about cluster dynamic disk groups currently imported on the node that is being backed up will be saved, but information about cluster dynamic disk groups currently owned by other nodes will not be saved.

Caution: The ASR backup operation fails when the SFW configuration contains a disk group that contains a missing dynamic disk. Before using ASR, you need to delete all missing dynamic disks from the SFW configuration or deport any dynamic disk groups with missing disks.

Note: ASR attempts to make the target system bootable and recovers the original disk and volume configuration where possible. Sometimes it may not be possible to recover all of the disk and volume configuration. In this case, ASR will attempt to create a bootable system and allow the administrator to manually reconstruct the disk and volume configuration.

SFW's support for ASR

During an ASR backup, several files are created, including **asr.sif**, **asrnpn.sif**, and **setup.log**. This section describes these files and the type of Veritas Storage Foundation for Windows information that is stored in each.

The **asr.sif** (ASR State Information File) stores the system name, host ID, and other system state information and contains a number of subsections that store specific types of information.

SFW uses the following subsections to save dynamic disk group and volume configuration information:

- **InstallFiles** – lists the set of files that are needed to perform the recovery of the dynamic disk groups and volumes. It also contains information about the original installation media where these files are located. ASR uses this section during the text-only mode of recovery to prompt the user to insert the correct media and to copy the listed files to the requested location.
- **Commands** – contains two command entries: one is for installing the necessary SFW program components that will be used for recovery, and the other is the file that runs the recovery process.

- **VXVMASR.VOLUMECONFIG** – contains the configuration information for all the SFW volumes on the system.

Caution: Manual edits to the **asr.sif** file may result in an invalid ASR backup and cause a recovery operation to fail.

The **asrnpn.sif** and **setup.log** files are used to store the PNP state and the system configuration information, respectively. Together with the **asr.sif** file, they create a complete picture of the layout and configuration of your system.

ASR recovery process

This section presents the high-level steps for the ASR recovery process. For a detailed description of the ASR recovery process, see the documentation that accompanies your backup and recovery application.

To begin the recovery process, boot the repaired or replacement system from the operating system CD (or other optical disc media), and then press F2 to begin the text-only mode of the ASR recovery process. This will be followed by a prompt to insert the floppy disk created during the ASR backup process.

During the text-only mode, you will be prompted to insert the Veritas Storage Foundation for Windows DVD, as well as the CDs from your backup and recovery application and any other third-party applications that participate in the ASR recovery process. Make sure that the Veritas Storage Foundation for Windows DVD is inserted into a bootable drive.

At the end of the text-only mode of recovery, the system will perform an automatic reboot. You may have to remove any floppy disks or CDs in order for the system to continue to the GUI mode of setup by booting through the hard disk.

The system will reboot into GUI mode, and the ASR recovery process will continue automatically. In the event of a failure, on-screen directions will guide you.

Caution: If there is a failure related to Veritas Storage Foundation for Windows during this phase, it is highly recommended that you retrieve and save all the error and trace logs when you are provided the opportunity to do so. You may not have access to these diagnostic files later because the system may not be bootable if the error encountered is critical in nature.

After the successful completion of the GUI mode, the system will perform an automatic reboot. Any RAID or mirrored volumes will resynchronize and regenerate during this reboot.

Following this final reboot, your system should be recovered and you will be ready to begin the process of data recovery.

Cluster recovery

This section describes the general process for ASR recoveries with Microsoft Clustering. Please refer to your backup and recovery application documentation and related Microsoft articles for further information.

There are two types of recoveries that may occur within a Microsoft Clustering setup: node restore and cluster restore.

A **node restore**, the most common scenario, will be necessary when a single node of a cluster has failed. In this case, the shared disks will fail over to another node, but the local node needs to be recovered using the ASR backup. The backup-and-restore application should recognize that the local node is part of the cluster and restore the cluster database on that node. The recovery process will be similar to the general process previously described; the system configuration is recreated except that the disks that failed over to another node will be inaccessible to the local node during the ASR recovery.

The shared disks, although recognized by the ASR backup and properly logged to the **asr.sif** file, are not available to ASR at the restore time. As long as they are noncritical disks (which they should be), they will not be accessed. When the ASR recovery is complete, the node should reboot and automatically join the cluster.

A **cluster restore** will be necessary when a cluster with a single node running fails. In this case, since there is no node available for failover, the disk containing the quorum information will need to be restored. The quorum information is saved during the ASR backup process but is not automatically copied to the quorum disk during the ASR recovery process. Instead, the quorum information must be manually restored using the resource kit utility **clustrest.exe**. Following this, a reboot should be forced. The single-node cluster will boot and should begin operating properly.

Optimizing

- [Chapter 11, “Performance tuning”](#) on page 519
- [Chapter 12, “FlashSnap”](#) on page 563
- [Chapter 13, “Dynamic multi-pathing software”](#) on page 717
- [Chapter 14, “Microsoft Clustering support”](#) on page 753
- [Chapter 15, “VCS support in SFW HA”](#) on page 783
- [Chapter 16, “Implementing disaster recovery with VVR”](#) on page 797

Performance tuning

- [Statistics overview](#)
- [Real-time statistics collection and display](#)
- [Historical statistics collection and graphing](#)
- [Subdisk move, split, and join](#)
- [Command line commands for statistics](#)
- [VxCache](#)
- [SmartMove](#)

About performance tuning

Veritas Storage Foundation for Windows provides performance tuning for storage objects on dynamic disks.

The key ways you do performance tuning are using statistics and using the subdisk move, split, and join functionality.

Statistics overview

The statistics feature of Veritas Storage Foundation for Windows provides I/O statistics to allow you to do performance tuning to improve overall disk and system performance.

Veritas Storage Foundation for Windows provides the following statistics parameters:

- **Read Requests/Second**
The number of read requests per second for selected storage objects.
- **Write Requests/Second**
The number of write requests per second for selected storage objects.

- **Read Blocks/Second**
The amount of read request data (in blocks per second) that is processed for selected storage objects. It is the throughput on the read requests made.
- **Write Blocks/Second**
The amount of write request data (in blocks per second) that is processed for selected storage objects. It is the throughput on the write requests made.
- **Average Time/Read Block**
The average time in microseconds that it takes to process a read block from the time a request is made until the data is returned.
- **Average Time/Write Block**
The average time in microseconds that it takes to process a write block from the time a request is made until the data is returned.
- **Read and Write Requests/Second**
The number of read and write requests per second for selected storage objects.
- **Read and Write Blocks/Second**
The number of read and write blocks per second for selected storage objects.
- **Queue Depth**
The current number of read and write requests in the queue for selected disks. It does not apply to volumes and subdisks.

With these statistical tools, you will be able to improve disk and system performance by the following actions:

- Identifying high I/O areas, known as “hot spots.”
- Moving data among physical drives to evenly balance the I/O load among the disk drives. This is known as “load balancing.”

Bottlenecks occur when a program or device uses too much disk I/O, creating a hot spot and degrading performance. By monitoring a system’s I/O, you can find the problem areas and prevent bottlenecks, thus ensuring smooth operation. SFW’s performance monitoring utility allows you to continuously monitor and tune system performance. You can make adjustments by moving subdisks from an area of high I/O usage to another disk that has lower usage. You also have the feature of splitting subdisks and joining them back together again. This gives you added flexibility of breaking subdisks down to smaller parts and then moving them.

You can view the statistics in a real-time format in the Online Monitoring window. You can also set up the statistics collection so that you can do an

analysis of the statistics over time with the historical statistics collection and graphing functions.

The table below summarizes the similarities and differences between the two types of statistics.

Table 11-1 Comparison of real-time and historical statistics

	Real-time	Historical
Displays in	The Online Monitoring window that shows real-time statistical values in a tabular format for selected storage objects.	A graph that represents historical statistics for one storage object. You can select multiple storage objects to track, but each object is graphed individually.
Statistical Parameters	You can select one or more of nine statistical parameters to display in the Online Data Display Options window.	All nine statistical parameters are included in the data collection, but you select one parameter at a time for graphing from the graphing window.
Storage Objects	When you select Online Monitoring, the Select Objects for Online Monitoring window comes up first to allow you to select the storage objects to monitor.	You select storage objects to monitor in the Start Historical Data Collection window.
Time Frame	Current values since last refresh. Data is not saved. Online monitoring data is available only when the Online Monitoring window is open.	Data is accumulated over time and saved in a file. You indicate the file size. You can start and stop data collection. You view the data only through a graph.

For details on these two types of statistics formats, see the following topics:

- [Real-time statistics collection and display](#)
- [Historical statistics collection and graphing](#)

Real-time statistics collection and display

This section describes real-time statistics collection and its display, which is done in the Online Monitoring window.

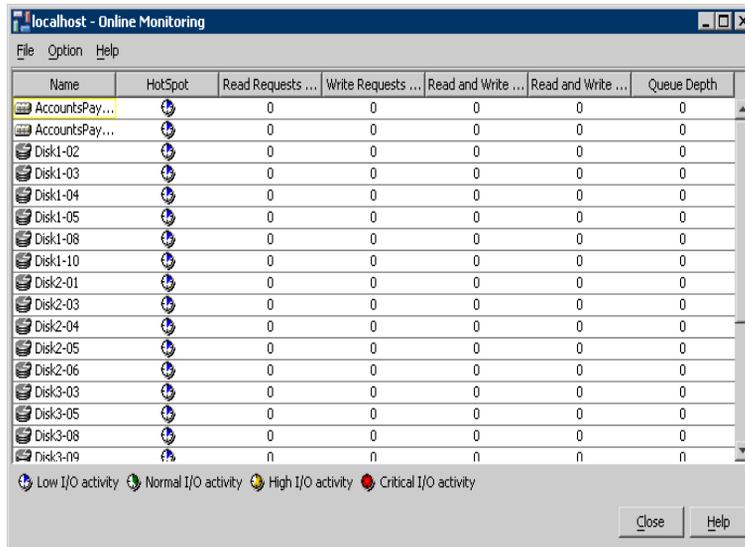
The section has the following topics:

- [Online monitoring window features](#)
- [Setup steps for real-time statistics](#)

Online monitoring window features

The Online Monitoring window displays real-time statistics for storage objects you select. It can include disks, subdisks, and volumes. To access the Online Monitoring window, select **Statistics>Online Monitoring** from the **Tools** menu, then select the storage objects to monitor in a preliminary window that comes up, and click **OK**.

Figure 11-1 Online monitoring window



The Online Monitoring window collects statistics as long as you have it open. The window can operate in the background. You can do other commands while the window is open. When you set up the real-time statistics, you can change the refresh rate, the time interval of the refresh of the screen display. The default is 5 seconds. The statistics are being computed continuously in the background.

The Online Monitoring window is organized as follows:

■ **Name**

The first column contains the names of the storage objects that have been selected for monitoring. Thus, each row contains the statistical data on a selected storage object.

■ **Hot Spot**

The second column has a pie symbol that is designed to be used as an indicator for hot spot detection. A hot spot is an area of high I/O activity that may cause bottlenecks in I/O throughput. The color and shading of each pie symbol indicate the current state of I/O activity for the associated storage object. The pie symbol for the highest amount of I/O activity, Critical activity, is red and fully shaded, making it easy to notice on the screen. You can select the statistical parameters you want to use for hot spot detection.

■ **Statistical Parameters**

The remaining columns represent the different statistical parameters available in the program. By default, Read Requests per Second, Write Requests per Second, Read and Write Requests per Second, Read and Write Blocks per Second, and Queue Depth are selected, but you can select any of the nine statistical parameters.

See “[Statistics overview](#)” on page 519.

■ **Legend for the Hot Spot Indicator**

The legend at the bottom of the window describes the four pie symbol categories for the hot spot indicator. The table below gives more detail on these categories. If the pie symbol indicator displays the High or Critical category, it signals the fact that you have a hot spot—that is, an area of high I/O activity.

Table 11-2 Explanation of the pie symbol categories for hot spot indicator

I/O Activity	Pie Symbol	Subdisk I/O	Dynamic Disk I/O
Low	Blue Small section in pie	Does not apply	More than 30% below average if it is not below minimum I/O threshold
Normal	Green Section less than half of pie	80% or less of parent disk I/O	30% below average up to 30% above average
High	Yellow Section more than half of pie	81% to 90% of parent disk I/O	31% to 50% above average

Table 11-2 Explanation of the pie symbol categories for hot spot indicator

I/O Activity	Pie Symbol	Subdisk I/O	Dynamic Disk I/O
Critical	Red Color in all of pie	More than 90% of parent disk I/O	More than 50% above average

■ **Context Menu**

If you right-click any row in the Online Monitoring window, a context menu appears with the following two menu choices relating to the storage object being monitored:

- Graph Historical Statistics Information
- Remove Object from Online Monitoring

The first menu choice is grayed out unless you have previously selected that storage object for historical statistics monitoring.

Setup steps for real-time statistics

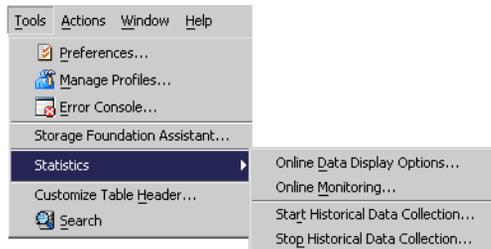
This section describes what is involved in setting up the real-time statistics, so that you can view them in the Online Monitoring window.

The topics are the following:

- [Getting acquainted with the statistics submenu](#)
- [Selecting online display options](#)
- [Selecting storage objects to monitor](#)

Getting acquainted with the statistics submenu

The commands for setting up the real-time statistics are located on the **Statistics** submenu on the **Tools** menu.



The table that follows summarizes the available commands:

Table 11-3 Table of statistics commands

Command	Description
Online Data Display Options	Sets display options for real-time statistics.
Online Monitoring	Brings up the Select Objects to Monitor window to allow you to select objects to monitor for a real-time statistics session. Once you have selected objects to monitor, the Online Monitoring window appears.
Start Historical Data Collection	Starts the data collection for historical statistics.
Stop Historical Data Collection	Stops the data collection for historical statistics.

Historical statistics are displayed as graphs of individual storage objects that you select.

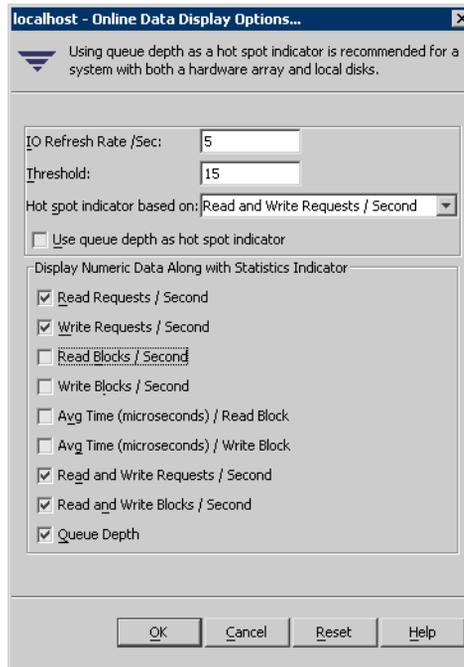
See “[Historical statistics collection and graphing](#)” on page 531.

Selecting online display options

The first task in the setup process is to set the display options. This task is not absolutely necessary. If you do not use this window, the default settings, which are shown in this window the first time you bring it up, will apply. The default settings are shown in the sample screen below.

To select the online data display options

- 1 Choose **Statistics>Online Data Display Options** from the **Tools** menu to bring up the Online Data Display Options window.



- 2 If desired, change the **I/O Refresh Rate/Sec** setting.
This is the time interval of the refresh of the screen display. The program continuously runs the actual statistics in the background but changes the display of them in the Online Monitoring window according to the refresh rate you set. The default and minimum I/O refresh rate is 5 seconds.
- 3 If desired, change the **Threshold** setting.
The threshold is the minimum amount of I/O per second that a disk or subdisk has to have to display a color other than blue. Blue is the lowest state, low I/O activity. The default threshold is 15.
- 4 Determine which statistical parameter or parameters to use for the **hot spot indicator**.
See “[Hot Spot](#)” on page 810.
The window provides the following two places to enter a hot spot indicator:
 - The drop-down list that is labeled “Hot spot indicator based on.”
 - The checkbox labeled “Use queue depth as hot spot indicator.”

Queue depth applies only to disks. The other eight statistical parameters that are in the “Hot spot indicator based on” drop-down list apply to disks, volumes, and subdisks.

If you select the checkbox to use queue depth as a hot spot indicator, queue depth will be used to calculate the hot spot statistic for disks only. The indicator that is used to calculate the hot spot statistic for volumes and subdisks will be the statistical parameter shown in the “Hot spot indicator based on” drop-down list.

If you don't select queue depth as a hot spot indicator, then the indicator that is used to calculate the hot spot statistic for volumes, subdisks, and disks will be the statistical parameter shown in the “Hot spot indicator based on” drop-down list.

Why Use Queue Depth?

It is recommended that you select queue depth when you have both disks that are directly connected to your computer and disks that are in a hardware disk array. Because a disk in a disk array can have a much higher level of reads or writes and still function well, reads or writes per second are not really a good way to compare directly connected disks and array disks. Queue depth is the current number of read and write requests in the queue for selected disks. It is a better indicator of how well a disk in an array is working, and it also works for disks that are directly attached to the computer.

- 5 Select the statistics parameters you wish to monitor by clicking the checkbox in front of each parameter. The statistics parameters are described as follows:
 - **Read Requests/Second**
The number of read requests per second for selected storage objects.
 - **Write Requests/Second**
The number of write requests per second for selected storage objects.
 - **Read Blocks/Second**
The amount of read request data (in blocks per second) that is processed for selected storage objects. It is the throughput on the read requests made.
 - **Write Blocks/Second**
The amount of write request data (in blocks per second) that is processed for selected storage objects. It is the throughput on the write requests made.
 - **Average Time/Read Block**
The average time in microseconds that it takes to process a read block from the time a request is made until the data is returned.
 - **Average Time/Write Block**

The average time in microseconds that it takes to process a write block from the time a request is made until the data is returned.

- **Read and Write Requests/Second**

The number of read and write requests per second for selected storage objects.

- **Read and Write Blocks/Second**

The number of read and write blocks per second for selected storage objects.

- **Queue Depth**

The current number of read and write requests in the queue for selected disks. It does not apply to volumes and subdisks.

Note: By default, Read Requests per Second, Write Requests per Second, Read and Write Requests per Second, Read and Write Blocks per Second, and Queue Depth are selected parameters. The **Reset** button restores default settings.

- 6 When you are finished with your changes, click **OK**.

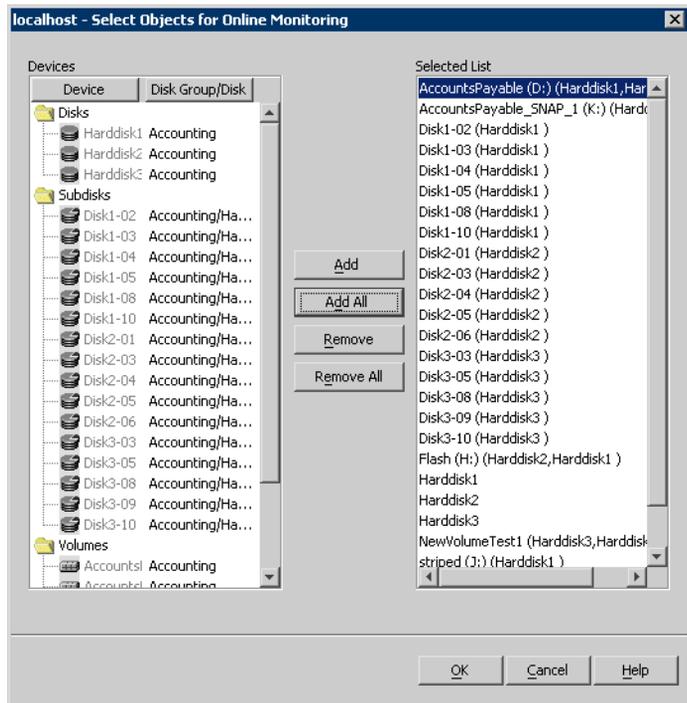
Selecting storage objects to monitor

When you select the **Online Monitoring** command, the Select Objects for Online Monitoring window appears to allow you to select the storage objects to monitor. The detailed steps are given in the procedure that follows.

To select objects for online monitoring

- 1 Choose **Statistics>Online Monitoring** from the **Tools** menu, or click the **Online Monitoring** button from the Storage Foundation Assistant.
The Select Objects for Online Monitoring window appears. You can select an entire disk group or its individual disks, subdisks, and volumes.

You may need to click on the plus symbol next to a disk group icon to display the disks, subdisks, and volumes.



- 2 Select the storage objects you want to display by using the following options:
 - **Add:** Adds one or more selected objects in the left pane of the window to the **Selected List** in the right pane of the window. If you select a dynamic disk group and click **Add**, all associated objects (disks, subdisks, and volumes) will be added to the **Selected List** in the right pane.
 - **Add All:** Adds all disks, subdisks, and volumes to the **Selected List** in the right pane.
 - **Remove:** Removes any objects that are selected from the **Selected List** in the right pane.
 - **Remove All:** Removes all available objects from the **Selected List** in the right pane.
- 3 Click **OK** to view the statistics in the Online Monitoring window. See “[Online monitoring window features](#)” on page 522.

Name	HotSpot	Read Requests ...	Write Requests ...	Read and Write ...	Read and Write ...	Queue Depth
AccountsPay...		0	0	0	0	0
AccountsPay...		0	0	0	0	0
Disk1-02		0	0	0	0	0
Disk1-03		0	0	0	0	0
Disk1-04		0	0	0	0	0
Disk1-05		0	0	0	0	0
Disk1-08		0	0	0	0	0
Disk1-10		0	0	0	0	0
Disk2-01		0	0	0	0	0
Disk2-03		0	0	0	0	0
Disk2-04		0	0	0	0	0
Disk2-05		0	0	0	0	0
Disk2-06		0	0	0	0	0
Disk3-03		0	0	0	0	0
Disk3-05		0	0	0	0	0
Disk3-08		0	0	0	0	0
Disk3-09		0	0	0	0	0

Low I/O activity Normal I/O activity High I/O activity Critical I/O activity

Close Help

Historical statistics collection and graphing

The historical statistics collection and graphing function allows you to monitor one or more storage objects (disks, subdisks, or volumes) over time and to create individual graphs for these storage objects. You invoke the graphing function by right-clicking a storage object and then selecting the command **Graph Historical Statistics Information** from the context menu that appears. However, the command will not be available on the context menu without certain setup steps having been done first.

This section first describes the graphing window and then details the setup functions that are necessary before you can do the graphing.

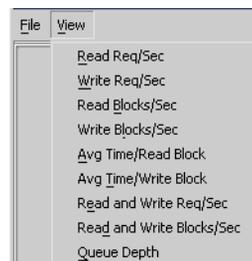
The topics are the following:

- [Features of the graphing window](#)
- [Setup steps for historical statistics](#)
- [Stopping historical data collection](#)

Features of the graphing window

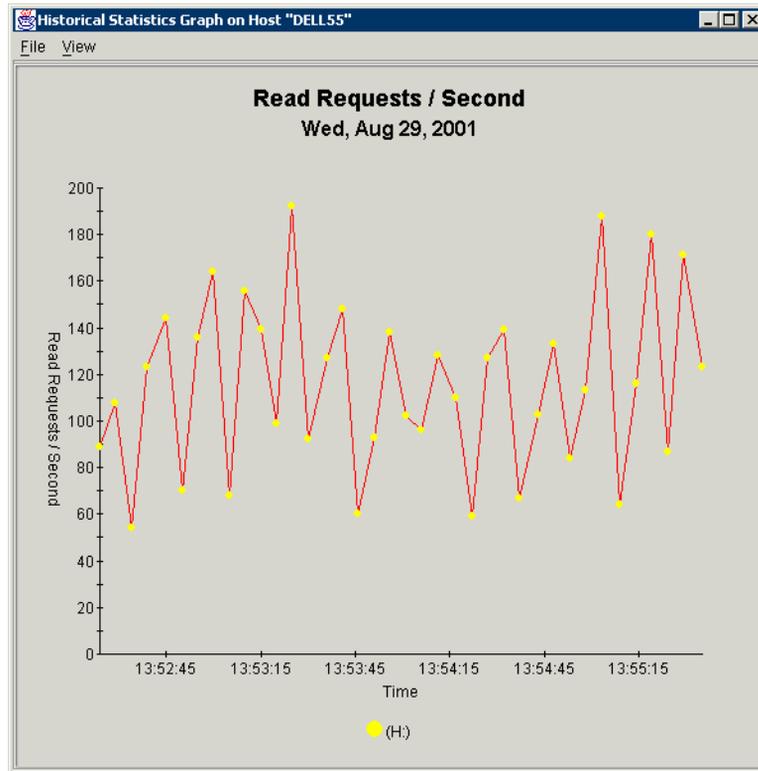
After you select the **Graph Historical Statistics Information** command from a storage object's context menu, a graphing window comes up, but it does not display a graph because no statistical parameter has been selected. To display the statistics, you select the **View** menu at the top left corner of the graph and click to choose one of the nine statistical parameters to graph.

Figure 11-2 View menu in graphing window



The graph then generates and displays, as shown in the sample graph that follows:

Figure 11-3 Historical statistics graph



The features of the graph include the following:

- The vertical axis displays a scale for the statistical parameter being graphed, and the name of the statistical parameter is also displayed vertically next to the axis.
- The horizontal axis shows time, which is determined by the data collection rate setting. The name of the storage object being graphed is displayed under the axis.
- The **View** menu, as mentioned previously, has the various statistical parameters, allowing you to change the graph to show a different parameter.
- The **File** menu has an **Exit** command, but you can also close the graph window by clicking the close box in the top right corner.

A graph can be saved and printed by copying it to the Clipboard with Alt+PrintScreen and then pasting it into a program, such as Microsoft Word.

Setup steps for historical statistics

This section describes how to configure and graph historical statistics.

The topics are the following:

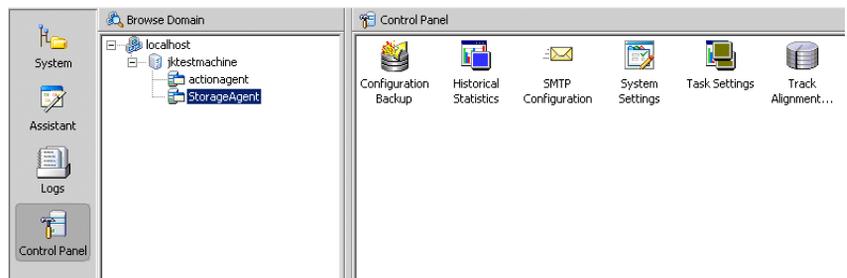
- [Configuring settings in the historical statistics settings window](#)
- [Selecting storage objects and starting the data collection for historical statistics](#)
- [Graphing steps](#)

Configuring settings in the historical statistics settings window

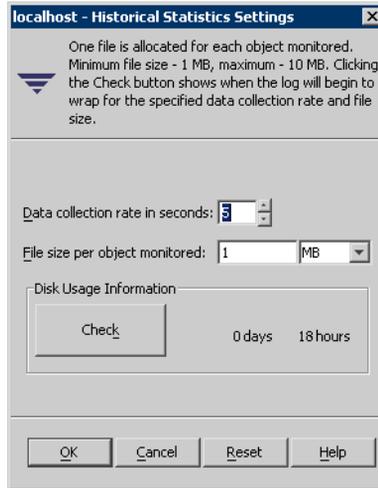
The first task in the setup process is to configure the settings in the Historical Statistics Settings window. This window is accessed by clicking **StorageAgent** in the tree view and then clicking Control Panel in the Perspective bar. If you accept the default settings, which are settings that are appropriate for most data collection purposes, then you do not need to use the following procedure.

To access the historical statistics settings window to view and adjust settings

- 1 In the VEA console tree view, click the **StorageAgent** node and then click **Control Panel** in the Perspective bar.
The Control Panel icons appear in the right pane of the window, including the **Historical Statistics** icon.



- 2 Double-click the **Historical Statistics** icon to bring up the Historical Statistics Settings window.



- 3 Check the settings in the Historical Statistics Settings window (as described below), and make changes if desired. Click **OK** to confirm the settings and close the window.

Note that the **Reset** button restores default settings.

Historical Statistics Window Settings

- **Data collection rate in seconds**

This is the rate at which the data is collected. It is the time interval between data samples. The default is every 5 seconds. You may prefer the data to be collected every hour (3,600 seconds). This setting establishes the point when the data is graphed. If you plan to run the statistics for several days, it is easier to read the graph with a longer data collection rate.

- **File size per object monitored**

Veritas Storage Foundation for Windows collects the data in a file. You set the desired size of the file. Once the file reaches the specified size, the older statistics information is deleted as new information is added. This feature allows you to continuously monitor the statistics without taking up increasing file space.

- **Disk Usage Information section**

The numbers at the bottom of this window are an estimate of how long (in days and hours) it would take to compile statistics per storage object monitored to fill up the file size indicated. If you change either the data

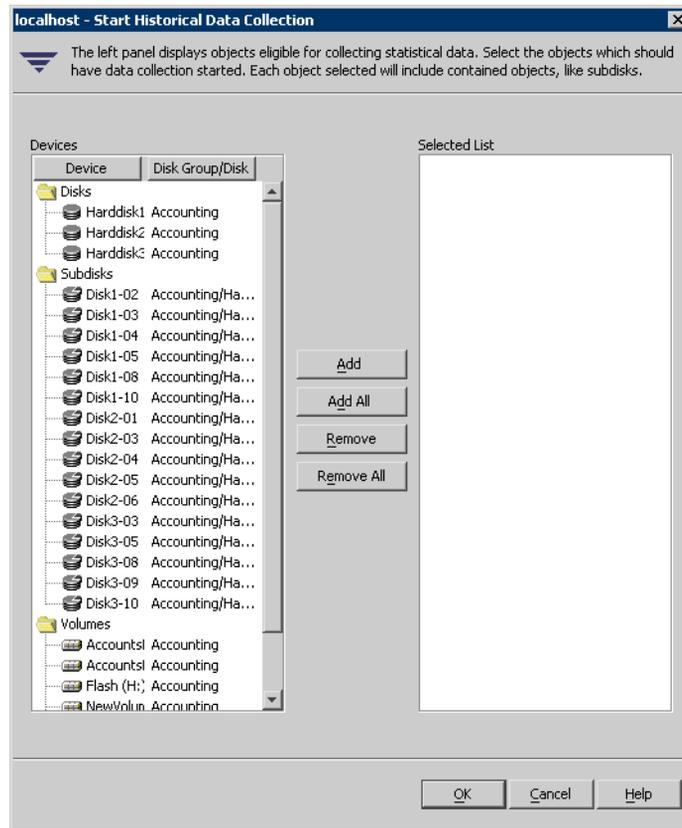
collection rate or the file size per object monitored, click the **Check** button to update the estimate.

Selecting storage objects and starting the data collection for historical statistics

The next task in the setup for the historical statistics is to select the storage objects you want to monitor and start the historical statistics data collection. These functions are available through the **Start Historical Statistics** command. This task is not optional.

To select storage objects and start the historical data collection

- 1 Select **Tools>Statistics>Start Historical Data Collection** to bring up the Start Historical Data Collection window, as shown in the sample screen.



This window allows you to select the storage objects for historical data collection. Once you have made your selection and clicked **OK**, the historical data collection begins. The data collection continues in the background until you stop it with the **Stop Historical Data Collection** command or until

Veritas Storage Foundation for Windows is stopped or the computer is rebooted.

- 2 Select the storage object or objects you want to monitor for historical statistics data collection by highlighting the object or objects and using the **Add** button to move the objects to the **Selected List**.
You can also move the objects to the right pane by double-clicking them or by dragging them to the right pane. Use the **Remove** or **Remove All** button to move items on the **Selected List** in the right pane back to the **Devices** list in the left pane.
- 3 Click **OK** when you have made your selection.
The data collection begins in the background. You now have the settings necessary for invoking the graphing function. If you select a storage object that was one of the selected objects or that is included under a selected object (for example, if you selected an entire disk group), the **Graph Historical Statistics Information** command will be available on that storage object's context menu.

Graphing steps

This section covers the specific steps for creating a graph.

You must have selected one or more storage objects and have started the historical data collection for the graph to be displayed.

See [“Selecting storage objects and starting the data collection for historical statistics”](#) on page 536.

When creating a graph, you select which statistical parameters to use.

See [“Statistics overview”](#) on page 519.

To create a graph

- 1 Right-click the storage object you want to graph, and select **Graph Historical Statistics Information** from the context menu that appears.
A graphing window appears, but no graph is generated until you select a statistical parameter.
- 2 Choose **View** from the menu bar at the top of the screen, and then click one of the statistical parameters from the **View** menu.
Once you click a parameter, the **View** menu closes and the graph is generated.
See [“Features of the graphing window”](#) on page 531.

Stopping historical data collection

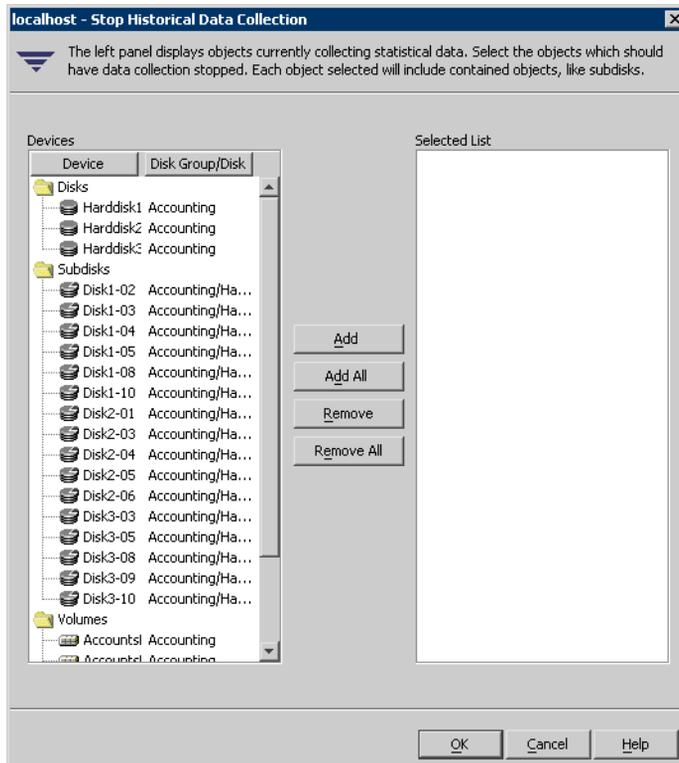
You can stop the collection of historical data by using the **Stop Historical Data Collection** command. The historical data collection is also stopped when Veritas Storage Foundation for Windows is stopped or when the computer is rebooted.

In those cases, you will need to restart the historical data collection.

See “[Selecting storage objects and starting the data collection for historical statistics](#)” on page 536.

To stop the historical data collection

- 1 Select **Tools>Statistics>Stop Historical Data Collection** to bring up the Stop Historical Data Collection window, as shown in the sample screen that follows.



- 2 In the left pane of the window, highlight the storage objects for which you no longer want to collect historical data, and use the **Add** or **Add All** button to move the objects to the right pane. You can also move the objects to the right pane by double-clicking them or by dragging them to the right pane.

- 3 Click **OK** when you are satisfied with your selections.

Subdisk move, split, and join

This section describes the Subdisk Move, Split, and Join commands.

Topics include the following:

- [Purpose of the subdisk commands](#)
- [Subdisk context menu](#)
- [Subdisk properties](#)
- [Moving subdisks](#)
- [Splitting subdisks](#)
- [Joining subdisks](#)

Purpose of the subdisk commands

With the commands **Move Subdisk**, **Split Subdisk**, and **Join Subdisk**, you can move subdisks to other locations within the dynamic disk group, split subdisks, and join them back together. The flexibility of moving subdisks, splitting them, and joining them lets you make best use of your disk space.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Move Subdisk**, **Split Subdisk**, and **Join Subdisk** commands.

These are the following main purposes for moving and splitting your subdisks:

- [Load balancing](#)
- [Disk failure or removal](#)
- [Disk phaseout](#)

Load balancing

If disk activities are heavily concentrated on one or a small number of disks in the storage subsystem, it may create bottlenecks. You can use the **Move Subdisk** and possibly the **Split Subdisk** command to spread out disk accesses more evenly across all the disks.

If a disk has High or Critical I/O activity (shown by a yellow or red pie symbol), you may consider moving one or more of its subdisks to another disk that shows below-average I/O activity (shown by a blue pie symbol). The idea is to move just enough activity to achieve balance. A careful study of the statistics for the disk

with Critical activity may identify the best subdisks to move. You should move subdisks only when a disk has High or Critical I/O activity over a prolonged time and performance is affected. Moving a subdisk to another disk has an effect on I/O as well, but it should be compensated for by the other disk's having much lower I/O activity. You would need to look at the statistics after the subdisk move to see whether the move was effective in balancing the load.

Disk failure or removal

The **Move Subdisk** command can also be used to move the part of a volume that is on a failed or missing disk to a healthy one. Moving a subdisk for redundant volumes (mirrored or RAID-5) will use the redundant data to recreate the subdisk on the healthy disk. However, for nonredundant volumes (concatenated or striped), the data cannot be recreated, and doing a subdisk move will therefore lose data, which could be recovered if the disk can be repaired. Thus, when you attempt to move a subdisk from a failed or missing disk that has nonredundant data, a dialog box appears that asks if you want to force the move. You may want to force the move if you don't need the data any more or you can no longer recover the data. By doing so, you will retain the volume structure, but there is no guarantee that the data will be recoverable.

Disk phaseout

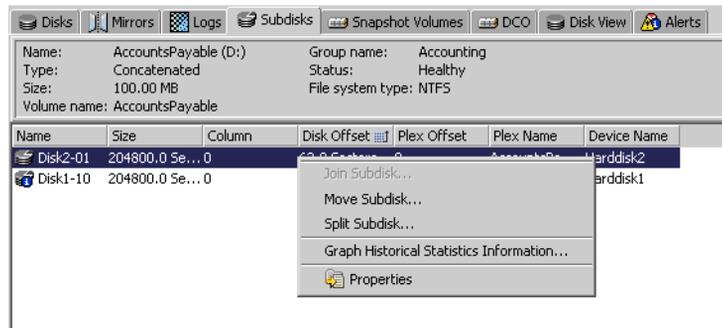
When a disk starts getting intermittent I/O errors and shows signs of hardware fatigue, you can use the **Move Subdisk** command to move all its subdisks to healthier disks. The benefit of moving subdisks instead of copying the volumes is that you need only enough space on the receiving disks for the subdisks on the one failed disk, not for entire volumes that may span multiple disks. Another advantage is that there is no interruption in I/O.

Moving subdisks provides you a flexible means of making adjustments in your storage system while it is up and running.

Subdisk context menu

The subdisk commands are available from the subdisk context menu, which is shown below:

Figure 11-4 Subdisk context menu

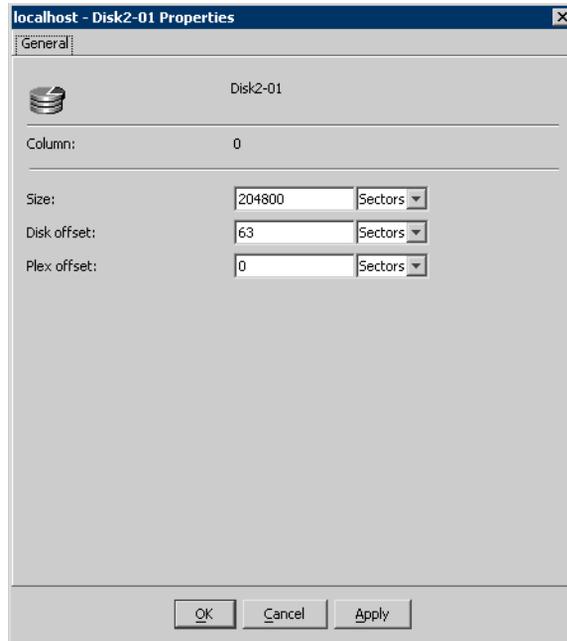


To access this menu, display the subdisk you want to work with by first clicking on its volume in the tree view and then clicking the **Subdisks** tab above the right pane. Once the subdisk is displayed, right-click the subdisk to bring up this menu.

Subdisk properties

When you select **Properties** from the subdisk context menu, the following screen displays the properties of the selected subdisk:

Figure 11-5 Subdisk properties screen



Note: The **Size**, **Disk offset**, and **Plex offset** fields have pull-down lists that allow you to select the units you want the number to be displayed in (Sectors, KB, MB, GB, or TB).

Name

In the screen captures showing subdisks in this chapter, you may have noticed that the subdisks on a disk are assigned numbers in a sequence, such as 1-01, 1-02, 1-03 or 12-01, 12-02, 12-03. The subdisk number is an internal number generated by the program. There is no particular significance to the one or two digits before the dash except that for any one disk, the first one or two numbers identifying its subdisks must be the same. The numbers after the dash represent a number for the subdisk within the disk. Thus, if the subdisk was the first one created for a particular disk, it would have a 01 after the dash, the second disk created would have a 02 after the dash, and so on.

Column

Column displays the column that the subdisk occupies in the volume. Striped and RAID-5 volumes have multiple columns.

Size

This field displays the size of the subdisk.

Disk offset

This is the offset where the subdisk starts on the disk. This is included in the Properties window because for a subdisk to be split, it must be contiguous to the subdisk next to it. By looking at the offsets, you can determine which subdisks are contiguous.

Plex offset

This is the offset of a subdisk within a plex. It shows the distance from the start of a plex to the start of a specific subdisk. The first subdisk within a plex will have an offset of 0. The second subdisk will be offset by the size of the first subdisk.

Moving subdisks

The purpose of moving a subdisk is discussed in “[Purpose of the subdisk commands](#)” on page 539.

Note: You are not allowed to move a subdisk that is part of a boot or system volume.

Veritas Storage Foundation for Windows automatically checks the state of the data before beginning the subdisk move. If the data is degraded, the subdisk can still be moved. After moving, you will need to reactivate the disk to clear the Degraded state.

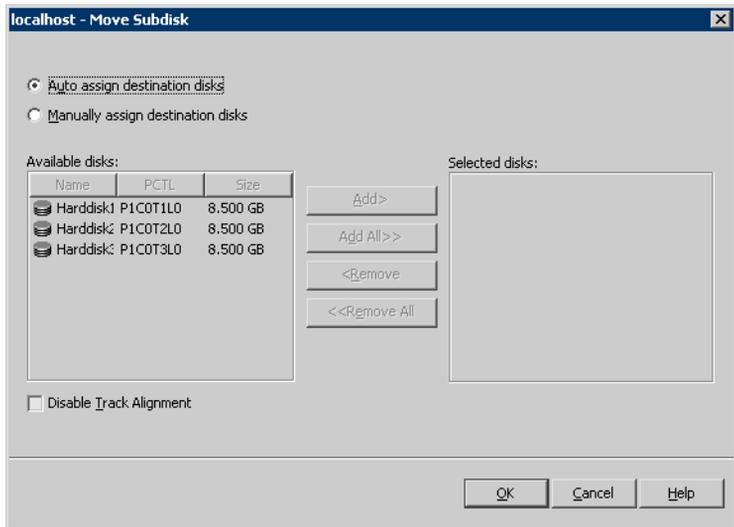
Note: Moving a subdisk from one disk to another involves a certain amount of time. The SmartMove feature can help reduce the time for this operation. See “[SmartMove](#)” on page 130.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Move Subdisk** command.

To move a subdisk

- 1 In the tree view, select the volume that contains the subdisk you want to move.
- 2 Identify the subdisk that you want to move, and display it in the right pane of the VEA console.
If you are concerned about load balancing, look for a disk with High or Critical I/O activity. It will have a yellow or red pie symbol in the cell to the right of its name in the Statistics tabular view. You may also be aware that a disk has had difficulties because of minor disk errors that have occurred. Such a disk may display an Online (Errors) state from time to time.
To display the subdisk in the right pane, click on its volume in the tree view, and then click on the **Subdisks** tab in the right pane. The subdisks for that volume will display. You can use the subdisks’ **Properties** command to further identify the characteristics of a volume’s subdisks.
- 3 Right-click the subdisk you want to move to bring up its context menu.
- 4 Select **Move Subdisk** from the context menu.

The Move Subdisk window appears.



Choose either automatic or manual selection of the destination disk or disks for the subdisk to be moved to.

If you want to select the destination disk(s), click **Manually assign destination disks**. In the left panel of the window, highlight the disk(s) you want to assign as the destination disk or disks and use the **Add** or **Add All** button to move the disk(s) to the right pane of the window.

You may also check **Disable Track Alignment** to disable track alignment on the destination disks.

- 5 Click **OK** when you are satisfied with the changes.

Splitting subdisks

The **Split Subdisk** command allows you to split a subdisk. After the subdisk is split, the resulting two subdisks will reside on the same sections of the same disk. You can then use the **Move Subdisk** command to move one or both subdisks to other disks. You may want to split and move a subdisk to make the best use of your disk space. A split subdisk can be joined back together with the **Join Subdisk** command.

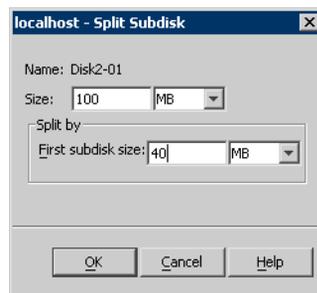
Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Split Subdisk** command.

To split a subdisk

- 1 In the tree view, select the volume that contains the subdisks you want to split.
- 2 In the right pane, click the **Subdisks** tab to display the volume's subdisks.
- 3 Right-click on the subdisk you want to split to bring up its context menu.
- 4 Select **Split Subdisk** from the context menu.
- 5 In the window that comes up, specify the subdisk size for the first of the two subdisks.

The remaining space will be assigned to the second subdisk. For example, if the original subdisk was 100 MB and you assigned 40 MB to the first subdisk, the other subdisk will be 60 MB.

The drop-down list to the right of the **Size** and **First subdisk size** text entry boxes allow you to select sectors, KB, MB, GB, or TB.



- 6 Click **OK** to complete the command.
After a few moments, two subdisks will appear in the right pane of the VEA console.

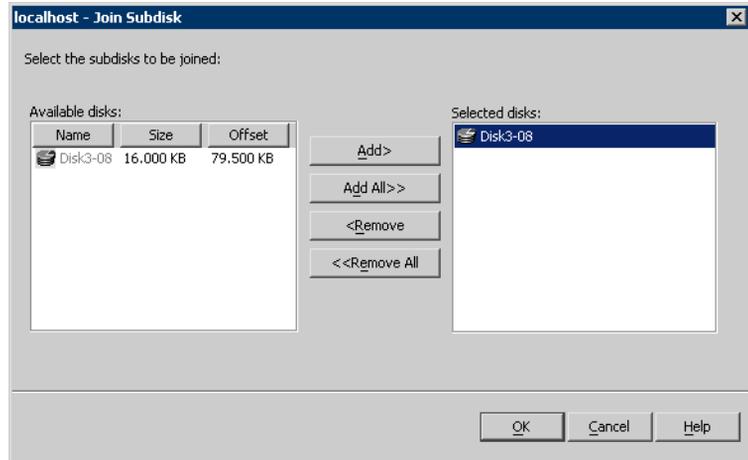
Joining subdisks

The **Join Subdisk** command allows you to join subdisks. You can join two subdisks that had been one subdisk but that were split by the **Split Subdisk** command. You cannot split a subdisk and join it back to another subdisk that it was not split from. There also has to be room on the disk for the two subdisks.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Join Subdisk** command.

To join subdisks

- 1 In the tree view, select the volume that contains the subdisks you want to join.
- 2 In the right pane, click the **Subdisks** tab to display the volume's subdisks.
- 3 Right-click on a subdisk you want to join to bring up its context menu.
- 4 Select **Join Subdisk** from the context menu.
- 5 In the window that appears, select the subdisks to be joined.



- 6 Click **OK** to complete the command.
Within a short time, the two subdisks in the right pane of the VEA GUI will be replaced with one subdisk.

Command line commands for statistics

Statistics commands can be done through the command line interface.

See “[vxstat](#)” on page 381.

VxCache

VxCache can improve the performance of specific dynamic volumes on 32-bit and 64-bit servers by assigning a designated cache memory pool of up to 4 GB for those volumes.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support vxcache.

The following topics are included in this section:

- [Overview](#)
- [Identifying the memory capabilities of your servers](#)
- [Determining the memory to assign to VxCache for a server](#)
- [Determining the volumes to include on the server](#)
- [Enabling VxCache](#)
- [VxCache volume monitoring](#)
- [More on the policy file](#)

Overview

Applications that manipulate large amounts of data achieve better performance by keeping data for I/O in memory rather than on disk. VxCache is designed to improve the performance of designated volumes by assigning up to 4 GB of cache that uses a portion of the system's memory for I/O operations on volumes.

Implementing VxCache requires the following two tasks:

- **Enabling VxCache at the Server Level**
Involves indicating the amount of physical memory available for VxCache on the server and enabling the feature by using the **VxCache Memory Configuration** command.
- **Enabling VxCache at the Volume Level**
Involves selecting the dynamic volumes that will use VxCache on the server and enabling the feature for each volume by using the **Enable VxCache I/O** command, which is available from the volume context menu.

These tasks do require preliminary analysis.

For more information to assist you in making those decisions, see the following topics:

- [“Determining the memory to assign to VxCache for a server”](#) on page 551

- [“Determining the volumes to include on the server”](#) on page 553

Optionally, if the server (32-bit only) supports the use of PAE memory, you can increase the amount of memory available by enabling PAE. You enable PAE on a server before enabling VxCache.

See [“About PAE”](#) on page 550.

After VxCache is set up, you can monitor the server’s performance through the VxCache Volume Monitoring window. A policy file is used to record settings for the volumes that use VxCache. This XML file is automatically set up when VxCache is enabled. The policy file will also record volume settings for Automatic Volume Growth, if that feature is enabled.

Identifying the memory capabilities of your servers

Identifying the memory capabilities of the servers on which you plan to use VxCache is the first step in implementing the feature. One question is whether or not you can use PAE. You also may need to look at each system’s installed memory to see whether more RAM should be installed.

Topics in this section include the following:

- [About PAE](#)
- [Microsoft Windows memory support](#)

About PAE

Physical Address Extension (PAE) is an addressing strategy that enables 32-bit systems to address more than 4 GB of physical memory. PAE must be supported by both the processor and the operating system.

On 32-bit versions of Windows, PAE is disabled by default. You must use the `/PAE` boot parameter to enable PAE.

For more information about PAE memory support, consult the Microsoft Windows Large (PAE) Memory Support Hardware Compatibility List (HCL).

For systems without the required PAE hardware support or systems running Microsoft Windows Server 2003 Standard Edition, you may dedicate a portion of the 4 GB memory range for use by VxCache.

Microsoft Windows memory support

You may wish to add memory to your system to maximize the performance benefits of VxCache. Although the maximum amount of memory that can be allocated to VxCache is 4 GB, you should also consider the memory requirements of other applications running on your system to determine the amount of memory to add.

The following table shows the maximum amount of memory supported by each version of the Microsoft Windows Sever 2003 and Windows Server 2008 operating systems.

Table 11-4 Maximum Amount of Operating System RAM Support

Operating System	Maximum Memory of 32-bit Windows	Maximum Memory of 64-bit Windows
Windows Server 2003 Web Edition	2 GB	n/a
Windows Server 2003 Standard Edition	4 GB	16 GB
Windows Server 2003 Standard Edition SP1	4 GB	32 GB
Windows Server 2003 Enterprise Edition	32 GB	64 GB
Windows Server 2003 Enterprise Edition SP1	64 GB	1 TB
Windows Server 2003 Datacenter Edition	64 GB	512 GB
Windows Server 2003 Datacenter Edition SP1	128 GB	1 TB
Windows Server 2008 Web Edition	4 GB	32 GB
Windows Server 2008 Standard Edition	4 GB	32 GB
Windows Server 2008 for Itanium-Based Systems	n/a	2 TB
Windows Server 2008 Enterprise Edition	64 GB	2 TB
Windows Server 2008 Datacenter Edition	64 GB	2 TB
Windows Server 2008 Datacenter Edition (Server Core)	64 GB	2 TB

Determining the memory to assign to VxCache for a server

This section has guidelines on how to determine the amount of physical memory to assign to VxCache for a server.

Note: VxCache requires a minimum of 512 MB physical memory. However, Symantec recommends an allocation of at least 1 GB for VxCache.

To determine the amount of memory for VxCache

- 1 Run your system under normal production conditions and allow enough system run time to establish a state of typical memory usage.
- 2 Use the information available under the Performance tab of the Windows Task Manager to determine the total physical memory and the amount of unused memory in your system.
- 3 The unused memory is the maximum available amount of memory that can be allocated to VxCache—subject to the 4 GB limit.
In consideration of system performance and peak demand situations, Symantec suggests the following in determining the amount of memory for VxCache:
 - Reserve 20% of the total physical memory and allow it to be available for potential system use.
 - Allocate 1 GB of memory to VxCache, if available, on servers that have 3 GB to 4 GB total physical memory.
 - Allocate 1 GB of memory to VxCache, if available, on 32-bit servers that have more than 4 GB of total physical memory on which PAE is not enabled.
 - On servers with more than 4 GB of physical memory, performance improves with larger allocations of memory to VxCache.

The following are other factors that affect the amount of memory allocated to VxCache:

- The amount of memory that can be allocated to VxCache is dependent on the amount of memory available in the nonpaged pool of the system. The amount of available memory in the nonpaged pool must be able to support the VxCache memory allocation as well as the needs of the operating system and other applications running on the system. After allocating memory and enabling VxCache, check the amount of memory from the nonpaged pool that is being used. If necessary, reduce the memory allocation of VxCache so that the amount of memory being used from the nonpaged pool is less than half of the 256 MB maximum allowed for that resource.
- The maximum amount of memory that can be allocated to VxCache is limited to approximately 4 GB even though the total system memory on the server and the memory usage of the applications may allow more.

The demand that VxCache places on the nonpaged pool of the system limits the VxCache size to 4 GB.

When the /3GB switch (available only on 32-bit systems) is included in the Boot.ini file, the size of the nonpaged pool decreases. In this case, the maximum amount of memory that can be allocated to VxCache is limited to approximately 2 GB because of the decreased nonpaged pool size.

Example: If the total physical memory of a system is 4 GB and 2.5 GB of the physical memory is available, then the amount of memory available to VxCache is 2.5 GB. In this case, 1 GB of memory can be allocated to VxCache. This allocation addresses the recommendations to reserve 20% of the total system memory for potential system use and the 1 GB VxCache size for system performance. After allocating the 1 GB of memory and enabling VxCache, checking the amount of memory being used in the nonpaged pool shows 58465K being used. This amount of memory used in the nonpaged pool meets the guideline and no further adjustment to the VxCache allocation is required.

Determining the volumes to include on the server

Once you have established the amount of memory available for VxCache, you need to identify the volumes on each server that will be set up to use the feature. You will want to establish how many volumes to use and which type of volumes would be best suited. For example, business-critical data volumes that are typically associated with a high level of read requests might have improved performance with VxCache enabled. Another example would be a Microsoft Exchange database store that is dedicated for executive or VIP use.

VxCache is most effective for read-intensive volumes because most read requests can be satisfied by retrieving data from the cache memory rather than reading it from disk, which is much slower. Write-intensive volumes, such as a log volume in a database, do not benefit as much from additional cache because they require more disk access.

Enabling VxCache

Enabling VxCache on a server involves the following tasks:

- Set up PAE on the server.
 - If PAE is available on your Windows 2003 server, add the /PAE boot parameter to the Boot.ini file.
See “[Adding the /PAE boot parameter to the Windows Server 2003 boot.ini file](#)” on page 554.
 - For servers with Windows 2008 and later, use the BCDEdit /set command in a command window and specify an appropriate PAE and nx parameter combination as recommended by Microsoft documentation.
For more information about BCDEdit, refer to the Microsoft technical support information at <http://www.microsoft.com>.
- Indicate the amount of memory available for VxCache on the server and enable the feature on the server.
See “[Enabling VxCache at the server level](#)” on page 555.
- Select the volumes that will use VxCache and enable the feature for each volume.
See “[Enabling and disabling VxCache at the volume level](#)” on page 556.

Additionally, there are some steps you need to take if you want to change the VxCache memory usage setting after it has been set initially.

See “[Changing the VxCache memory setting](#)” on page 556.

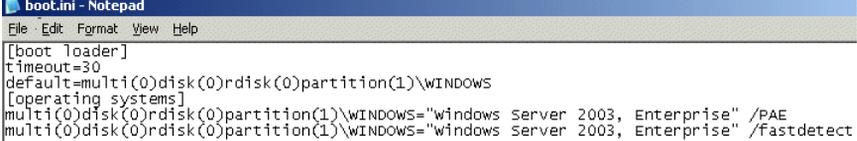
Adding the /PAE boot parameter to the Windows Server 2003 boot.ini file

If more than 4 GB of physical memory is available on your 32-bit system, modify the Boot.ini file to enable Physical Address Extension (PAE) prior to enabling VxCache. This will allow VxCache to access the increased memory.

To enable PAE

- 1 Locate the Boot.ini file of your server and make it accessible for editing by following these steps:
 - Open Windows Explorer.
 - On the **Tools** menu, click **Folder Options**.
 - On the **View** tab, clear the **Hide protected operating system files** checkbox, if necessary.
 - Click **OK**.

- In the root directory of the system's boot disk, right-click the Boot.ini file and select **Properties**.
 - Uncheck the Read-only attribute, if necessary, and click **OK**.
- 2 Open the Boot.ini file with a text editor. Add the /PAE boot parameter to the ARC path as shown in the example below:



```
boot.ini - Notepad
File Edit Format View Help
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="windows Server 2003, Enterprise" /PAE
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="windows Server 2003, Enterprise" /Fastdetect
```

- 3 Save the Boot.ini file.
- 4 Reboot the server for the change to take effect.
- 5 To verify the change, right-click on **My Computer**, then select **Properties**.
- 6 On the **General** tab, the full physical capacity of the RAM installed on the server and the Physical Address Extension label are displayed.
If desired, restore the Read-only attribute to the Boot.ini file.

Enabling VxCache at the server level

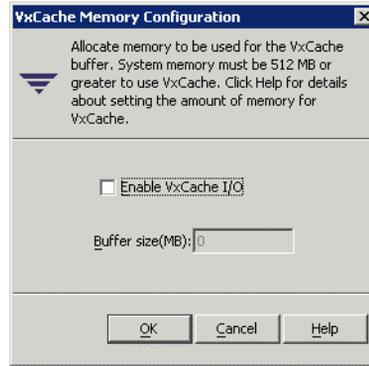
VxCache must be enabled at the server level before you can select the specific volumes whose performance you want to improve. This process creates a pool of cache memory that will be used by all the volumes that have VxCache enabled on that server.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support vxcache.

To initially enable VxCache at the server level

- 1 Using VEA, connect to the appropriate host or select the appropriate host in the tree view.
- 2 Select the StorageAgent node of the appropriate host and click **Actions>VxCache Memory Configuration**.
Alternatively, you may right-click the Storage Agent node and select **VxCache Memory Configuration** on the context menu.
- 3 Check the **Enable VxCache I/O** checkbox.

- 4 Enter a value in MB for the amount of memory to commit to VxCache and click **OK** to continue.



Enabling and disabling VxCache at the volume level

VxCache I/O must be enabled individually for the volumes you have determined will benefit from the improved performance VxCache offers.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support vxcache.

To enable VxCache I/O for a volume

- 1 Right-click on the desired volume, then select **Enable VxCache I/O** from the menu.
- 2 The Enable VxCache I/O window appears. Click **Yes** to continue.

To disable VxCache I/O for a volume

- 1 Right-click on the desired volume, then select **Disable VxCache I/O** from the menu.
- 2 The Disable VxCache I/O window appears. Click **Yes** to continue.

Changing the VxCache memory setting

To change the amount of memory for the VxCache buffer, you must first disable VxCache and then enable it again with the new amount.

To change an existing VxCache memory setting

- 1 Select the StorageAgent node of the appropriate host and click **Actions>VxCache Memory Configuration**.

- 2 Clear the **Enable VxCache I/O** checkbox and click **OK**.
- 3 Again, Select the StorageAgent node of the appropriate host and click **Actions>VxCache Memory Configuration**.
- 4 Check the **Enable VxCache I/O** checkbox and enter the new amount for VxCache.
- 5 Click **OK** to set the new amount.
- 6 You will need to enable VxCache again for any volumes that were set previously.
Right-click the desired volume and select **Enable VxCache I/O** from the menu to display the Enable VxCache I/O window. Click **Yes** to enable VxCache.

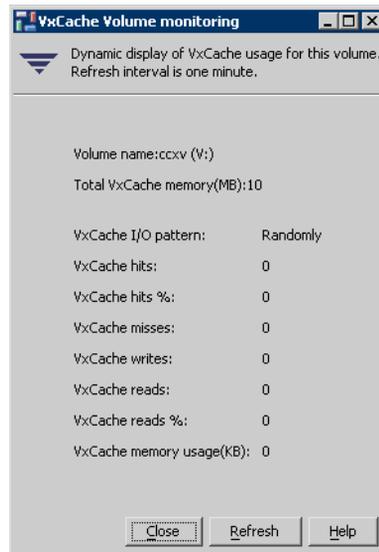
VxCache volume monitoring

You can monitor the use of the VxCache buffer with the VxCache Volume Monitoring window. The VxCache Volume Monitoring window displays real-time statistics about the use of VxCache for a selected volume.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support vxcache volume monitoring.

To enable VxCache volume monitoring

- 1 Right-click on the desired volume, then select **VxCache Volume Monitoring** from the menu.
- 2 The VxCache Volume Monitoring window appears.
The statistics are automatically refreshed every 60 seconds. Clicking **Refresh** will manually refresh the statistics.



The following table describes the information shown in the VxCache Volume Monitoring view:

Table 11-5 VxCache Volume Monitoring

Term	Description
Volume name	Name of the volume that has VxCache enabled
Total VxCache memory	Total amount of VxCache memory available
VxCache I/O pattern	I/O pattern that VxCache uses to improve performance
VxCache hits	Number of requests (reads and writes) satisfied by VxCache
VxCache hits %	Percentage of hits of the total number of requests (satisfied and not satisfied) made to VxCache
VxCache misses	Number of reads and writes not satisfied by VxCache
VxCache writes	Number of writes to VxCache
VxCache reads	Number of reads satisfied by VxCache
VxCache reads %	Percentage of reads of the total number of all requests (reads and writes) satisfied by VxCache
VxCache memory usage	Amount of VxCache memory used by this volume

Monitoring VxCache performance

The information presented in the VxCache Volume Monitoring window allows you to determine if VxCache is improving the I/O performance of the volume. We recommend that you monitor the read/write ratio over a period of time. If the number of VxCache reads is greater than the number of VxCache writes, then performance is improved by using VxCache. If, over time, there are consistently more writes than reads, VxCache may be degrading performance because each write is written to both the volume and the extended memory. In this case, you may wish to disable VxCache for that volume.

More on the policy file

As mentioned earlier, a policy file is used to record settings for the volumes that use VxCache. This XML file is automatically set up when VxCache is enabled. This policy file will also record volume settings for the Automatic Volume Growth feature, if that feature is enabled.

If you are using VxCache in a cluster and the second node is configured the same as the first and if the first node's policy settings for Automatic Volume Growth and VxCache are to be maintained on the second node, then you need to copy the VxVolPolicies.xml file of the first node to the second node. Copy the VxVolPolicies.xml file to the same path location on the second node as its location on the first node. The default path of the file is **Documents and Settings\All Users\Application Data\Veritas**.

SmartMove

The performance of mirror operations and subdisk moves can be enhanced with the SmartMove feature. SmartMove helps reduce the resynchronization time required by mirror operations and subdisk moves. The resynchronization time is reduced by using the NTFS file system metadata to resynchronize only selected regions. Operations that involve mirrors, like adding a mirror to a volume, off-host backup, and array migration, could have improved performance by using the SmartMove feature.

To enable SmartMove, see “[SmartMove](#)” on page 130.

Note: SmartMove does not support non-NTFS disks.

FlashSnap

- [FlashSnap overview](#)
- [FlashSnap components](#)
- [Summary of the FlashSnap procedure](#)
- [FastResync](#)
- [Snapshot commands](#)
- [Dynamic disk group split and join](#)
- [CLI FlashSnap commands](#)
- [Fast file resync](#)
- [Volume Shadow Copy Service \(VSS\)](#)
- [Using the VSS snapshot wizards with Microsoft Exchange](#)
- [Using the VSS snapshot wizards with Microsoft SharePoint](#)
- [Using the VSS snapshot wizards with Enterprise Vault](#)
- [Using the VSS snapshot wizards with Microsoft SQL](#)
- [Copy on Write \(COW\)](#)
- [Using the VSS COW snapshot wizards with Microsoft Exchange](#)
- [Using the VSS COW snapshot wizards with Microsoft SQL](#)

FlashSnap overview

Veritas FlashSnap is a multi-step process that allows you to create independently addressable snapshot volumes that are copies or mirrors of the volumes on your server. These snapshots can be used for backup, application testing, or reporting and analysis. One of the main advantages of using FlashSnap is that the snapshot volumes can be easily moved to another server.

Thus, backup or other processing can be performed on another server without affecting the performance of applications on the applications server.

With SFW, you also have the capability of creating simultaneous, multiple split-mirror snapshots. These snapshots can be done either through the GUI or through the `vxsnap` CLI command.

SFW supports both traditional full snapshots or Microsoft Copy on Write (COW) snapshots. The SFW GUI or the `vxsnap` CLI utility can be used to take COW snapshots. Microsoft COW snapshots are faster than full snapshots and take up less storage space because COW snapshots use a shadow copy that is differential. The initial state of the original volume can be reconstructed using the blocks in the differences area and unchanged blocks in the original volume.

SFW provides support for taking snapshots of Microsoft SQL databases.

FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with an SQL database without taking the database offline.

SFW provides support for taking snapshots of Microsoft Sharepoint databases. FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with a Sharepoint database without taking the database offline. The VSS Snapshot wizard and the `vxsnap` CLI command both use VSS and either can be used to take snapshots of Sharepoint components. The VSS process allows the Sharepoint components to be quiesced before the snapshot operation and reactivates them immediately after. The quiescing at the Sharepoint component level allows for Microsoft supported and guaranteed persistent snapshots of the data. Snapshots of the Sharepoint components can be reattached and resynchronized to match the current state of the storage group with the VSS Snapback wizard or the `vxsnap` reattach CLI command.

SFW provides recovery support for a select Sharepoint component. Using the VSS Restore wizard or the `vxsnap` restore CLI command, the snapshots taken with the VSS Snapshot wizard or the `vxsnap` CLI command can be used for a point-in-time recovery of the Sharepoint component.

SFW also provides support for taking snapshots of Microsoft Exchange 2003 and Exchange 2007 storage groups. FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with an Exchange storage group without taking the storage group's databases offline. The VSS Snapshot wizard and the `vxsnap` CLI command both use VSS and either can be used to take snapshots of storage groups. The VSS process allows the storage group's databases to be quiesced before the snapshot operation and reactivates them immediately after. The quiescing at the storage group level allows for Microsoft supported and guaranteed persistent snapshots of the data. Snapshots of the storage groups can be reattached and

resynchronized to match the current state of the storage group with the VSS Snapback wizard or the `vxsnap reattach` CLI command.

In addition, SFW provides recovery support for an Exchange storage group or a select database within a storage group. Using the VSS Restore wizard or the `vxsnap restore` CLI command, the snapshots taken with the VSS Snapshot wizard or the `vxsnap` CLI command can be used for a point-in-time recovery of the storage group or a roll-forward recovery to the point of failure of either the storage group or an individual database in the storage group.

For Exchange 2007 only, if you have set up a recovery storage group (RSG), you have the option to restore to the RSG rather than to the production volume, leaving the production volume intact. Follow the Microsoft instructions in creating the RSG. The database names in the recovery storage group must match those in the source storage group.

Refer to the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange* for detailed procedures on how to use the VSS Snapshot wizard or the `vxsnap` utility with Microsoft Exchange to perform and to implement recovery procedures. This guide is included in PDF format with the product.

Also see the following topics:

- [“vxsnap”](#) on page 407
- [“Using the VSS snapshot wizards with Microsoft Exchange”](#) on page 624

SFW also provides a VSS Snapshot Scheduler Wizard that enables you to set up a schedule for automating the snapback process.

At the time scheduled for the snapshot, the snapshot volumes are automatically reattached, resynchronized, and then snapshotted again. The schedule is maintained by a scheduler service, `VxSchedService.exe`, that runs in the background.

See [“Using the VSS Snapshot Scheduler wizard”](#) on page 627.

FlashSnap is a licensable option. For licensing details, see the licensing section of the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Fast File Resync is a feature that uses Veritas FastResync technology to resynchronize selected files in a snapshotted volume to the original volume. It is designed for database applications using volumes with multiple database files and can be used to restore one or more corrupt files.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support Flashsnap or SFW VSS related commands.

FlashSnap components

FlashSnap is a multi-step process that involves the following components:

- [FastResync](#)

FastResync (FR) supports resynchronizing of mirrors by copying only changes for the temporarily split mirror by using FR logging. This reduces the time it takes to rejoin a split mirror to the mirror set and also reduces the server CPU cycles needed to complete the resynchronization.

Note: The **Fast File Resync** command provides the capability to restore a single file from a snapshot back to the original volume.

See “[Fast file resync](#)” on page 614.

- [Snapshot commands](#)

The snapshot commands are used to create the mirrored volumes that are useful for backup or other resource-intensive processing purposes.

These features are necessary for the FlashSnap procedure, but they can also be used for other, more general purposes. The descriptions of these features in this section contain complete information about each feature, not just the part of the feature used in the FlashSnap procedure. However, to make use of these commands, you have to purchase the license that enables the FlashSnap option.

Note: Some snapshot commands, such as **Prepare**, may take a significant amount of time. These mirror-related operations can be tuned for better performance with the Configuration Task Performance Tuning settings.

See “[Configuration task performance tuning](#)” on page 134.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support snapshot commands.

- [Dynamic disk group split and join](#)

Dynamic Disk Group Split and Join (DGSJ) supports the ability to split a dynamic disk group into two disk groups so that the newly formed disk group can be moved to another server. This allows splitting a mirror for backup and having a separate server handle the backup. After the backup is completed, the split-off disk group is moved back to the original server and joined to its former disk group, and the mirror is reassociated with its mirror set and resynchronized. DGSJ also can be done on the same server for same-host backup or for reorganizing the disk groups on the server.

The disk group split and join commands are necessary for FlashSnap, but they can also be used for other, more general purposes.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support dynamic disk group split and join commands.

Summary of the FlashSnap procedure

You can use the FlashSnap procedure with two servers (using a remote server to do the processing of the backup or other resource-intensive activities), or you may prefer to have the processing done on the same server.

This section includes a summary for both situations. These steps can be implemented through the VEA GUI or through the command line.

Note: The same host procedure can be used for quick recovery snapshots to recover a data.

Off-host FlashSnap procedure (Two servers)

To use the off-host FlashSnap procedures with two servers

- 1 Use the **Prepare** command to attach a snapshot mirror to a volume on the working server.
This step of creating the snapshot mirror of the volume and resynchronizing it to the volume does take considerable time, but it has to be done only one time for the initial setup.
The **Prepare** command replaces the **Snap Start** command in the GUI. Both `prepare` and `start` keywords are available in the CLI, however `prepare` is the recommended keyword.
- 2 Use the **Snap Shot** command to automatically detach the snapshot mirror and create a new volume that is associated with the snapshot mirror.
This new volume can be used for backup or other purposes. The snapshot process typically takes less than 20 seconds.
- 3 Split the new volume from its dynamic disk group with the **Split Dynamic Disk Group** command, creating a new dynamic disk group on the server.
- 4 Deport the new dynamic disk group from the original server.
When using the command line, a separate `deport` command is not necessary. It is needed only for the GUI command.

If you do not have a SAN where you can access the deported dynamic disk group from the second server, move the split-off dynamic disk group by physically moving its disks and connecting them to the second server.

- 5 Rescan on the second server so that the computer recognizes the split-off dynamic disk group.
- 6 Import the dynamic disk group on the second server where the backup or other off-host processing occurs.
- 7 Perform the backup or other off-host processing activity, using the snapshot volume.
If you are backing up the server, Veritas NetBackup or Veritas Backup Exec is recommended for the backup software.
- 8 Deport the dynamic disk group from the second server.
If you do not have a SAN where you can access the deported dynamic disk group from the original server, physically move the split-off disk group's disks back to the original server.
- 9 Rescan on the original server, so that the server recognizes the split-off dynamic disk group.
You do not need to import the dynamic disk group back to the original server.
- 10 Use the **Join Dynamic Disk Group** command to join the split-off dynamic disk group back to its original dynamic disk group.
- 11 Join the mirrored volume back to its original volume, using the **Snap Back** command.
The mirrored volume is now resynched to the data source and is continually updated. Because FR is used in resynchronizing the mirrors, the time for the resynchronization is greatly reduced.
The next time the sequence of commands is run again, the snapshot mirror is ready for the snapshot step. The **Prepare** step, step 1, does not have to be done again.

Same-host FlashSnap procedure (One server)

Steps 1 and 2 are the same as in the two-server procedure: 1) using **Snap Prepare** to attach a snapshot mirror to the original volume, and 2) detaching the snapshot mirror and creating a new volume that is associated with it.

Because no remote host is involved, you do not need to use Disk Group Split and Join to do any deporting or importing of the disk group. The backup or other resource-intensive processing is done on the same server.

In both the off-host and same-host procedures, the final step is to join the mirrored volume back to its original volume, using the **Snap Back** command. In

this step, as already mentioned, the time for synchronizing the mirrors is greatly reduced.

FlashSnap on the same host can also be used for quick recovery snapshots to recover a data. Quick Recovery is the process of using on-host point-in-time copies of production data and a transaction log to recover a database that has been corrupted or that has missing data. If a database becomes corrupted, for example, you could reload the original data from the most current snapshot, and then use the transaction log to bring the database current to the point before the corruption.

For a general discussion of Quick Recovery, see the Quick Recovery section of the *Veritas Storage Foundation and High Availability Solutions Solutions Guide*.

If you are using Microsoft Exchange, refer to the Quick Recovery section of the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange*, which has detailed recovery procedures for an Exchange database.

FastResync

FastResync (FR) provides the following two enhancements to Veritas Storage Foundation for Windows.

- **Resynchronization**
Optimizes the resynchronization of a mirror that is detached from and then returned to a volume.
- **Reconnection**
Extends the snapshot model by providing the ability to refresh and reuse a snapshot, rather than discarding it.

FR increases the efficiency of the Veritas Storage Foundation for Windows snapshot mechanism and improves the performance of operations, such as backup and decision support (organized methods of collecting data that are designed to facilitate decision-making). Typically, these operations require that a volume is quiescent and that they are not impeded by updates to the volume by other activities in the system. FR reduces the amount of time that a volume must be out of service during such operations.

FR can be enabled or disabled by the user on a per-volume basis. When you enable FR for a volume, a DCO (Disk Change Object) volume is created to track the regions on a volume that are changed while a mirror is detached.

Note: Only a limited subset of operations is permitted on a DCO volume. You can perform a subdisk move, or add and remove a mirror.

FR is automatically enabled for a volume when the prepare the volume for snapshot operation is performed on the volume through the command line interface `vxassist prepare` command or through the VEA GUI **Prepare** command.

Note: The **Prepare** command replaces the **Snap Start** command in the GUI. Both `prepare` and `start` keywords are available in the CLI, however `prepare` is the recommended keyword.

FR limitations

FastResync cannot be used with software RAID-5 volumes.

Resynchronization

FR keeps track of data store updates missed by mirrors that are unavailable at the time that the updates are applied to a volume. When a mirror returns to service, FR resynchronizes the mirror with the volume by applying only the updates missed by that mirror while it was detached. This generally takes less time than the traditional method of copying the entire data store to the returning mirror.

If you want FR to resynchronize a mirror, FR must be enabled for the volume before the mirror is detached and continue to be enabled until after the mirror is reattached and resynchronized. However, if you are using any of the snapshot commands, FR is automatically turned on.

FR does not alter the traditional mirror failure and repair administrative model. The only visible effect is that typical mirror repair operations conclude more quickly.

Note: Although both FR and dirty region logging (DRL) keep track of regions on a volume where the mirrors are not synchronized, they perform different functions. FR keeps track of data store updates missed by a detached mirror, while DRL keeps track of whether a write to a mirrored volume has been completed on all mirrors. The write region on the volume is considered “dirty” because the mirrors are out of sync until the write to all mirrors is completed. DRL is used to resynchronize mirrors following a system crash. See [“Dirty region logging \(DRL\) and RAID-5 logging”](#) on page 274.

Reconnection

Reconnection extends the snapshot model by providing the ability to refresh and reuse a snapshot mirror, rather than discarding it. FR is automatically enabled when you take a snapshot of a volume. FR retains the association between the snapshot mirror and the volume when the snapshot mirror is detached from the volume.

See [“Resynchronization”](#) on page 571.

FR reattaches and resynchronizes the snapshot mirror with the volume when the **Snap Back** command is issued, either through the `vxassist` command line command or the GUI.

See [“`vxassist snapback`”](#) on page 368.

See [“Snapshot commands”](#) on page 577.

Enabling and disabling FR

FastResync can be enabled and disabled on a per-volume basis. For FR to be active when a mirror is reattached and resynchronized with its associated volume, FR must be enabled before the mirror is detached and remain enabled until the mirror has been reattached and resynchronized with the volume.

The procedure for enabling FR from the VEA GUI is described below.

You can also enable and disable FR from the command line.

See “[vxvol set fastresync=on|off](#)” on page 290.

Note: You cannot enable FR on RAID-5 volumes.

To enable FR for a volume

Note: If you are using snapshot commands, you do not need to use the following steps, because FR is automatically enabled for snapshot commands. These steps are needed only when you want to enable FR on a volume that is not used with any snapshot commands.

- 1 Right-click on the mirrored volume that you want to enable FR for.
The volume context menu is displayed.
- 2 Select **FastResync>Add**.
A dialog box is displayed, asking you to confirm adding FR for the volume.
- 3 Click **Yes**.
FR is now enabled for the volume.

To disable FR for a volume

- 1 Right-click on the mirrored volume that you want to disable FR for.
The volume context menu is displayed.
- 2 Select **FastResync>Remove**.
A dialog box is displayed asking you to confirm removal of FR.
- 3 Click **OK**.
FR is now disabled for the volume.

Disk change object (DCO) volume

The DCO volume is created when you enable FR or when a snapshot operation is started. The DCO volume keeps track of the changes made to a volume while a mirror is detached. The DCO volume is not visible in the tree view in the left

pane of the VEA console. It is visible in the Disk View (when Vol Details is not selected).

You can perform the following two optional operations on a DCO volume:

- Add or remove a mirror – you can add a mirror to the DCO volume and remove a mirror from it.
- Move a subdisk – you can move the DCO volume and the mirrored subdisk associated with it to another disk with the **Subdisk Move** command.

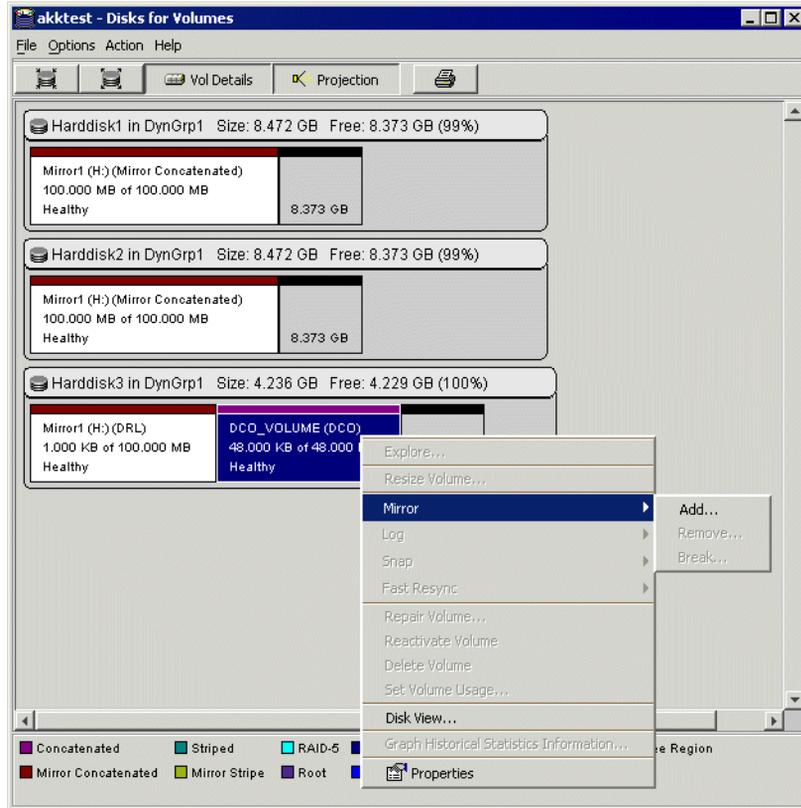
Add a mirror to a DCO volume

You might want to add a mirror to a DCO volume to have a backup copy of the DCO volume.

To add a mirror to a DCO volume

- 1 Under the Volumes folder, right-click the volume whose DCO volume you want to add a mirror to.
- 2 From the volume's context menu, select **Disk View** to get a separate Disk View window. You can also select the **Disk View** tab to have the Disk View display in the right pane.

- 3 Right-click the DCO volume to bring up a context menu, as shown in the sample screen.



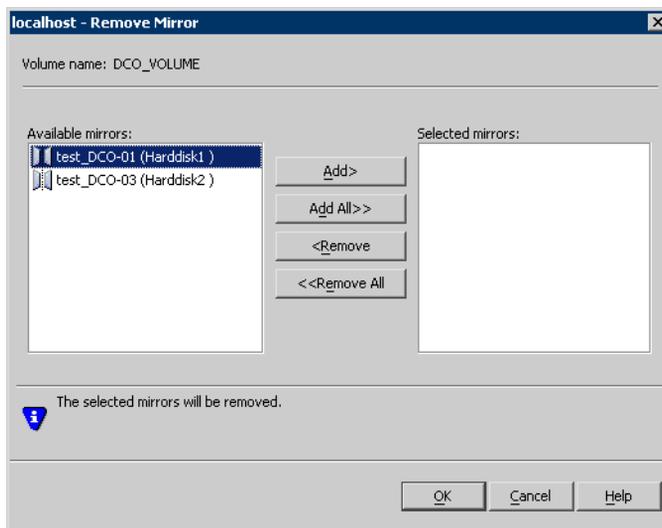
- 4 Select **Mirror>Add**.
The Add Mirror window is displayed.
- 5 If you want to add the mirror to a specific disk, click the radio button **Manually select disks**, select the desired disk, and then click the **Add** button to move the disk to the right pane. If you want the disk to be selected automatically, leave the default setting of **Auto assign destination disks** selected.
- 6 Click **OK** to add the mirror.
Note that any mirrors added to the DCO volume of a snapshot volume are deleted when you snap back the snapshot volume.
The process for adding a mirror to a volume that is not a DCO volume is different.

See “[Add a mirror to a volume](#)” on page 258.

Remove a mirror from a DCO volume

To remove a mirror from a DCO volume

- 1 Under the Volumes folder, select the volume whose DCO volume you want to remove a mirror from.
- 2 Select the **Disk View** tab in the right-hand pane, and right-click on the DCO volume.
A context menu is displayed.
- 3 Select **Mirror>Remove**.
A dialog box is displayed, asking you to select the mirror to remove.



- 4 Select the mirror and click the **Add** button to move it to the right pane.
- 5 Click **OK**.
The mirror is removed from the DCO volume.

Move the DCO volume subdisk

You might want to move a DCO volume and the mirrored subdisk associated with it to another disk if something happens to the original disk, or you may prefer to have this subdisk on another disk to split the disk group differently. The DCO volume and the mirrored subdisk associated with it have to be moved to a disk in the same disk group.

To move a DCO volume subdisk

- 1 Under the Volumes folder, select the volume whose DCO volume subdisk you want to move.
- 2 Right-click in the empty space on the **Disk View** tab in the right-hand pane. A context menu is displayed.
- 3 Select **Vol Details**.
The display changes. The **Disk View** tab now displays the subdisk names for the volumes.
- 4 Right-click on the subdisk containing the DCO volume. A context menu is displayed.
- 5 Select **Move Subdisk**.
The Subdisk Move window appears.
- 6 Click the radio button **Manually assign destination disks**.
- 7 Highlight the disk you want to move the mirrored volume subdisk with the DCO volume to, and click the **Add** button. The selected disk is moved to the right pane of the window.
- 8 Click **OK** to complete the command.
The mirrored volume subdisk with the DCO volume is moved to the other disk.
For more information about subdisk move, see “[Subdisk move, split, and join](#)” on page 539.

Snapshot commands

You can use the VEA console to take a snapshot of a volume.

The snapshot feature can also be accessed through the command line interface.

See “[CLI FlashSnap commands](#)” on page 613.

You can take a snapshot of mirrored or unmirrored volumes, but not of RAID-5 volumes.

The Snapshot feature enables quick and efficient online backup of volumes, with minimum disruption to the user. Snapshot automatically enables FastResync (FR) and creates a snapshot image of a volume, which can be detached from the volume. The detached snapshot image can be used for backup or other purposes, while the original volume remains in service.

The snapshot can then be quickly reattached and resynchronized with the volume through the FR reconnection capability.

See “[Reconnection](#)” on page 571.

The snapshot volume can also be permanently disconnected from the original volume.

You can attach more than one snapshot plex to a volume by issuing successive **Prepare** commands on the volume. This enables you to take multiple snapshots of a single volume.

Note: The **Prepare** command replaces the **Snap Start** command in the GUI.

You can attach a snapshot to either the original volume or the snapshot volume.

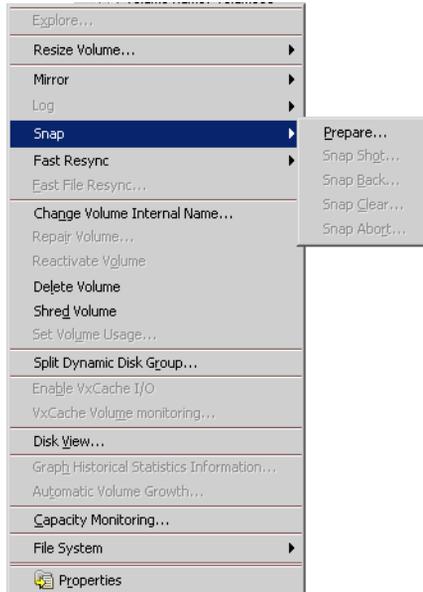
The following five snapshot commands are supported by the VEA console and are accessed through the volume context menu:

- [Prepare](#)
Creates the snapshot mirror and attaches it to the original volume.
- [Snap shot](#)
Detaches the snapshot mirror from the original volume and creates a snapshot volume that is associated with the snapshot mirror.
- [Snap back](#)
Reattaches the snapshot mirror to the original volume.
- [Snap clear](#)
Permanently removes the snapshot mirror from the original volume.
- [Snap abort](#)

Aborts the snapshot operation after a **Prepare** or **Snap Back** command is issued. **Snap Abort** permanently removes the snapshot mirror from the volume and releases its space.

The five snapshot commands are subcommands of the **Snap** command on the volume context menu.

Snap command submenu



Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support snapshot commands (**Prepare**, **Snap Shot**, **Snap Back**, **Snap Clear**, or **Snap Abort**).

Using the snapshot procedure

In summary, the snapshot procedure consists of the following steps:

- Attaching a snapshot mirror to a volume, using **Prepare**.
- Detaching the snapshot mirror and creating the snapshot volume that is associated with the snapshot mirror.
- Either reattaching the snapshot to the volume after you are done using it, or permanently disconnecting it from the volume. **Snap Back** reattaches the snapshot mirror; **Snap Clear** permanently disconnects the snapshot mirror

from the volume, removing the association between the snapshot volume and the original volume.

The **Prepare** procedure takes considerable time because it involves creating a mirror, but it has to be done only the first time you perform the snap commands sequence. After that, you use the commands **Snap Shot** to break off the mirror for backup (or other purposes) and then **Snap Back** to reattach the snapshot mirror to the original volume. Both of those are very quick procedures (typically less than a minute for each one).

Snap Abort aborts the snapshot operation after the **Prepare** or **Snap Back** command is issued.

Prepare

Prepare creates a snapshot mirror or plex, which is attached to and synchronized with a volume. Alternatively, if you are applying the command to a volume that already has one or more normal mirrors, you can designate an existing mirror to be used for the snapshot mirror. The advantage of selecting an existing mirror is that it saves time, since it is not necessary to resynchronize the mirror to the volume.

Note: The **Prepare** command replaces the **Snap Start** command in the GUI.

The mirror synchronization process can take a while, but it does not interfere with use of the volume. If the prepare the volume for snapshot process fails, the snapshot mirror is deleted if it was created from scratch, and its space is released. If you selected a normal mirror to be used for the snapshot mirror, that mirror reverts to its normal state if the prepare the volume for snapshot process fails.

When the prepare the volume for snapshot process is complete, the status of the snapshot mirror displays as Snap Ready on the **Mirrors** tab in the right pane of the GUI. The snapshot mirror can be associated with a snapshot volume by using the **Snap Shot** command. Once the snapshot mirror is created, it continues to be updated until it is detached.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Prepare** or **Snap Start** commands.

To create a snapshot mirror

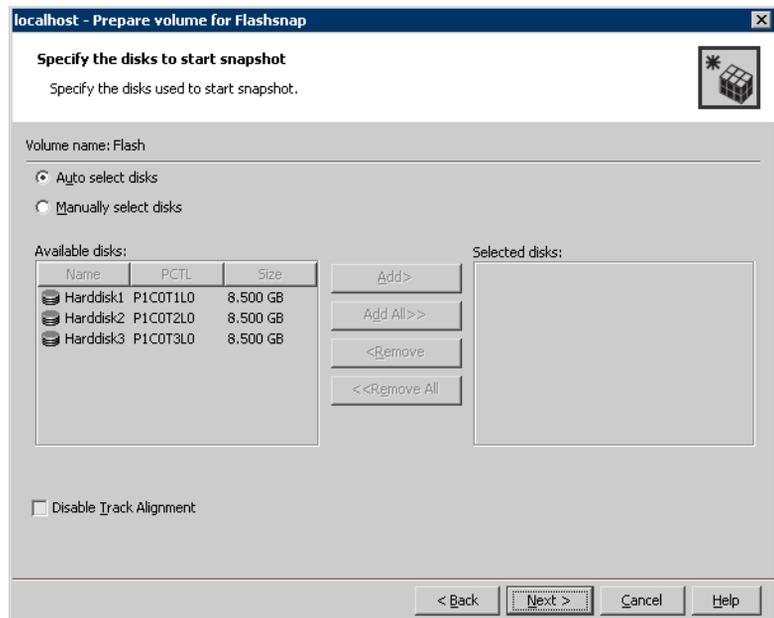
- 1 Right-click on the volume that you want to take a snapshot of. A context menu is displayed.
- 2 Select **Snap>Prepare**.
The Prepare volume for Flashsnap wizard welcome screen appears. Click **Next** to continue.
- 3 The next screen that appears depends on whether you already have a mirrored volume or not. If you already have a mirrored volume, the snapshot mirror continues to be updated until it is detached by using the **Snap Shot** command.
 - a **Mirrored volume:** If you have a mirrored volume, a screen appears to allow you to select an existing mirror to be used for the snapshot mirror.

- If you have a mirrored volume and there is also a disk available on your system to create an additional mirror, the screen allows you to choose either to use an existing mirror for the snapshot or to have a new mirror created.
- If you have a mirrored volume and there is no disk available for creating a new snapshot mirror, the screen allows you to select from existing mirrors in the volume.

If you select an existing mirror, click **Next** to continue to the summary screen and click **Finish** to complete the **Prepare** command.

If you do not select an existing mirror, click **Next** to continue and follow the instructions for an unmirrored volume.

- b** Unmirrored volume: If you have an unmirrored volume or you have not selected an existing mirror to use for the snapshot mirror, select the disk to be used for the snapshot mirror from the window for disk selection, as shown in the sample screen that follows.



The default setting is to have the program automatically select the disks where the mirror is created.

Alternatively, you can specify the disks that can be used to create the snapshot mirror by clicking the **Manually select disks** radio button. If

you select the manual setting, use the **Add** or **Add All** button to move the selected disks to the right pane of the window. The **Remove** and **Remove All** buttons allow you to move selected disks back to the left pane.

You may also check **Disable Track Alignment** to disable track alignment on the snapshot mirror volume.

Click **Next** to continue to specify attributes.

c Specify attributes

On this screen select one of the following volume layout types:

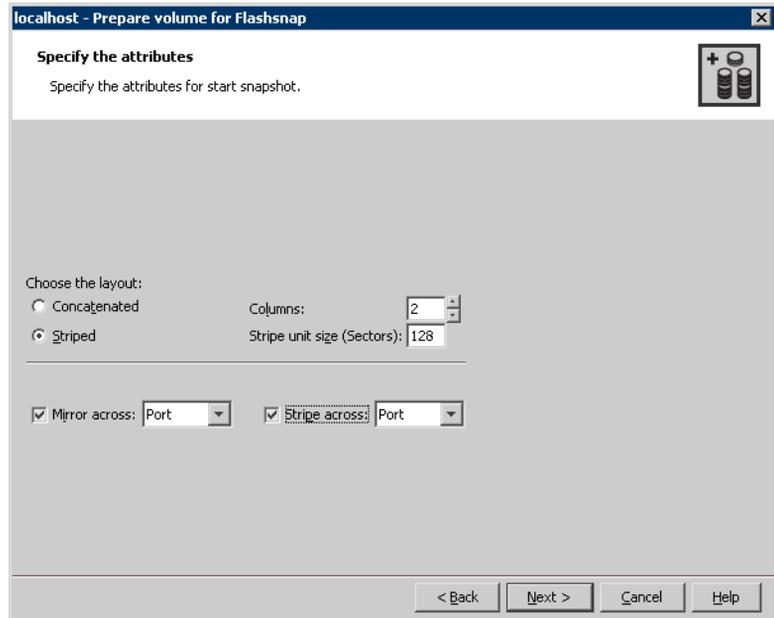
- Concatenated
- Striped

If you are creating a striped volumes the **Columns** and **Stripe unit size** boxes need to have entries. Defaults are provided.

For a concatenated or striped volume, you may also specify to mirror across disks by the following:

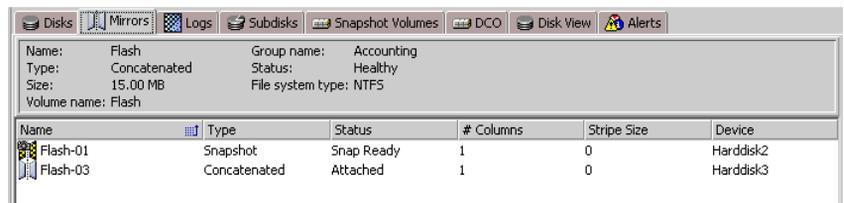
- Port
- Target
- Enclosure
- Channel

The operation to prepare a volume for a snapshot fails if the appropriate resources are not available to support the selected attributes to mirror across disks.



After the **Prepare** command completes, a new snapshot mirror is attached to the volume. See the sample screen below. In that screen, the volume Flash has a snapshot mirror attached to it.

The new mirror is added to the **Mirrors** tab for the volume. In the sample screen, the mirror is identified as a snapshot mirror and has the Snapshot icon. After the snapshot mirror is synchronized with the volume, its status becomes Snap Ready.



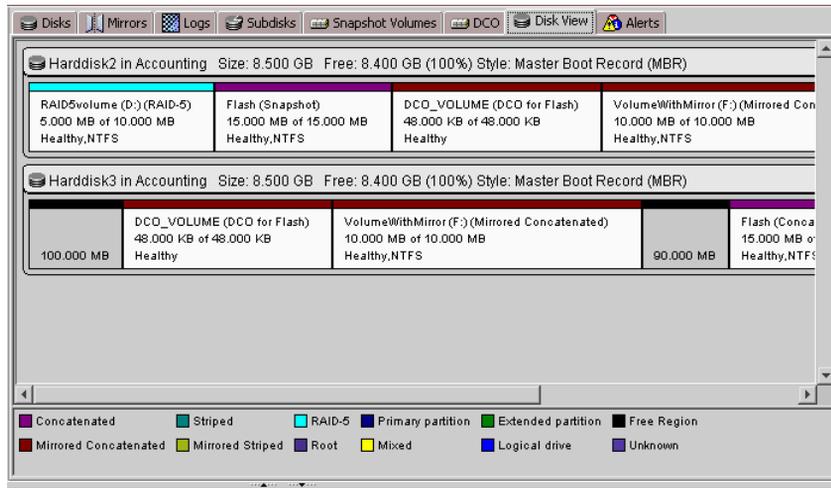
Note: It is important to make sure that the snapshot mirror (or snap plex) has completed its resynchronization and displays the status of Snap Ready before continuing with the **Snap Shot** command or doing any other operations on the snapshot mirror. Also, if you shut down the server or deport the disk group containing the volume being prepared for a snapshot before resynchronization completes, the snapshot mirror is deleted when the disk group with the original volume comes online again.

The DCO (Disk Change Object) volume is created to track the regions on a volume that are changed while a mirror is detached.

See “[Disk change object \(DCO\) volume](#)” on page 572.

The DCO volume is not included in the tree view of the VEA GUI. To view the DCO volume, you must use the Disk View. To access the Disk View, click the **Disk View** tab in the right pane or select Disk View from a disk’s or volume’s context menu.

The sample Disk View screen that follows shows the DCO log that is created by the **Prepare** command.



Note: The **Break Mirror** and **Remove Mirror** commands do not work with the snapshot mirror.

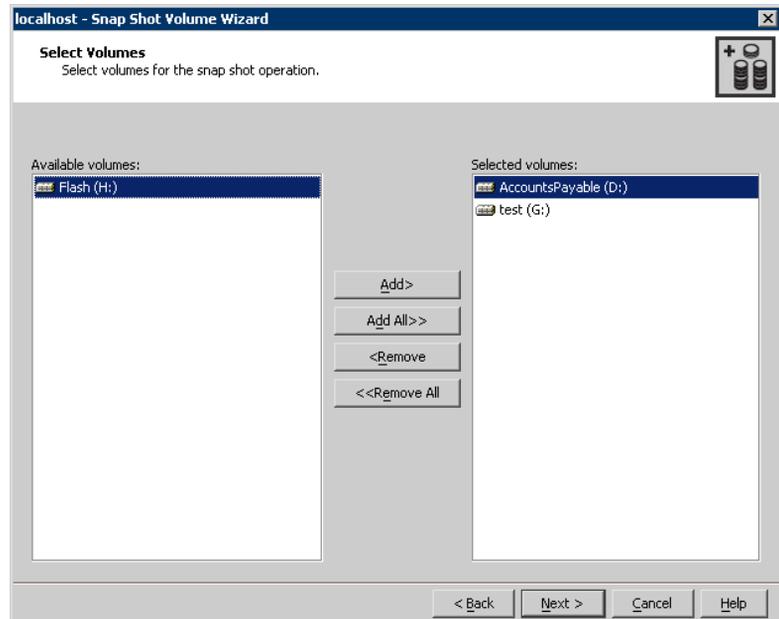
Snap shot

Snap Shot detaches the snapshot mirror and creates a new volume that is associated with that mirror. This process takes a relatively short time, typically less than a minute, during which users can be requested not to access the original volume. After the snapshot volume is created, it can be used for backup or other purposes. **Snap Shot** can also make snapshots of more than one volume at the same time.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Snap Shot** command.

To take a snapshot

- 1 Right-click on one of the volumes with a snapshot mirror. A context menu is displayed.
- 2 Select **Snap>Snap Shot**.
- 3 The Snap Shot Volume Wizard Welcome screen appears. Click **Next** to continue.



- 4 In the Select Volumes window that appears, select the volumes that you want to take a snapshot of by highlighting the volumes in the **Available**

volumes pane and clicking **Add**. Your selected volumes should appear in the **Selected volumes** pane.

You have the option of taking the snapshot with Volume Shadow Copy Service (VSS). The VSS snapshot method allows you to take snapshots of VSS-aware applications, such as Microsoft Exchange, while the application files are open. When VSS-aware applications do not exist, the snapshot is taken with the SFW FlashSnap method (VM method).

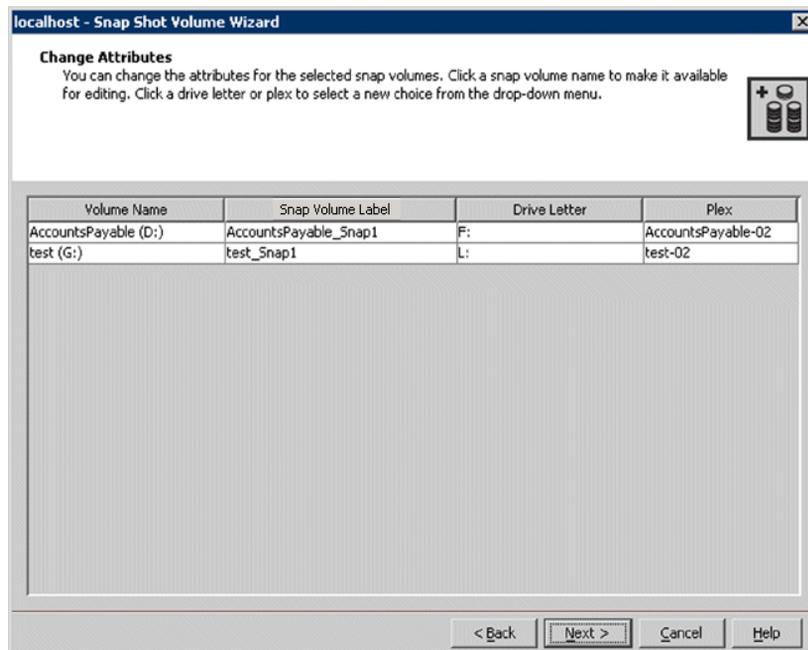
See “[Volume Shadow Copy Service \(VSS\)](#)” on page 617.

When the VSS snapshot method is used, snapshots can only be taken of read/write volumes and the resulting VSS snapshot is read only. The VM snapshot method may take snapshots of read/write or read only volumes and the resulting snapshots match the access mode of the original volume. However, when the VM snapshot method is used the Snap Shot Volume Wizard presents a **Force Read Only** checkbox to allow you to specify the resulting snapshot to have read only access.

You can set the snapshot process to use the VSS or the VM snapshot method by selecting Systems Settings on the VEA Control Panel and clicking the **Snap Shot** tab.

See “[System settings](#)” on page 126.

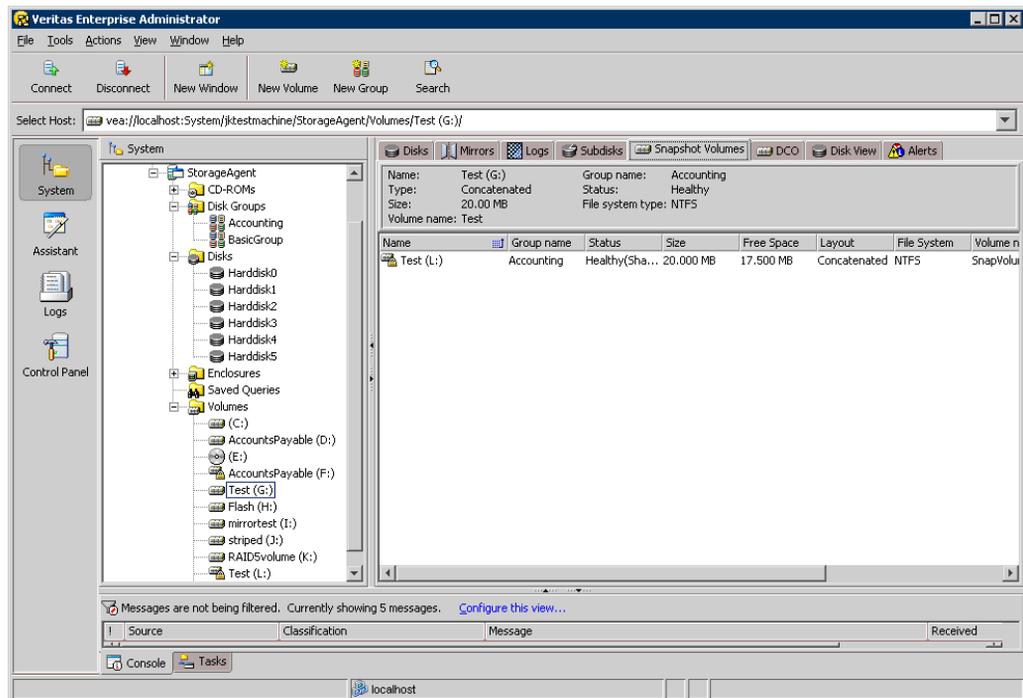
Click **Next** after selecting your volumes.



- 5 In the Change Attributes window that appears, you may edit the following attributes of the snapshot:
 - Snap Volume Label
(not available to be changed for read only snapshots)
 - Drive Letter
 - Plex

After editing the attributes, click **Next** to continue.

- 6 Click **Finish** in the final window to begin the Snap Shot process.
The snapshot mirror is detached from each of the original volumes, and new volumes are created that are associated with the snapshot mirrors. This process usually takes less than a minute.
The snapshot mirrors are no longer displayed on the **Mirrors** tab of the original volumes. The new snapshot volumes are displayed under the Volumes folder in the tree view. The program assigns them the next available drive letters (drive letters F and L in the tree view of the following sample screen).



You can now use the snapshot volume for backup or other purposes.

Snap back

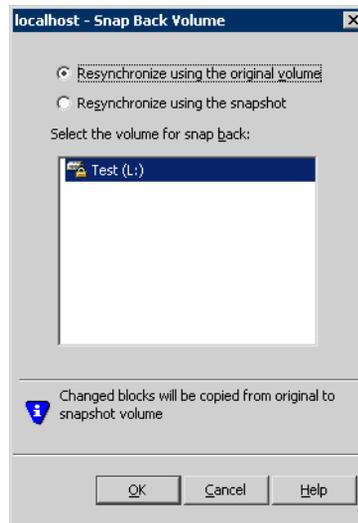
Snap Back reattaches a detached snapshot mirror to its original volume.

After you are done using the snapshot, you can reattach it to the volume, where it is resynchronized to the data store and continually updated. You can then get a current copy of the original volume, with minimal disruption to users, by issuing **Snap Shot** again.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Snap Back** command.

To reattach a snapshot mirror to the original volume

- 1 Right-click the snapshot volume whose snapshot mirror you want to reattach to its original volume.
A context menu is displayed.
- 2 Select **Snap>Snap Back**.
A dialog box appears with two options for resynching the snapshot, as shown in the screen that follows:



- 3 Specify whether the snapshot volume is to be resynchronized to match the original volume or the original volume is to be resynchronized to the snapshot volume, and click **OK**.

One situation where you might want to resynchronize using the snapshot volume rather than the original volume is when something has happened to the original volume so that its data integrity is no longer sound.

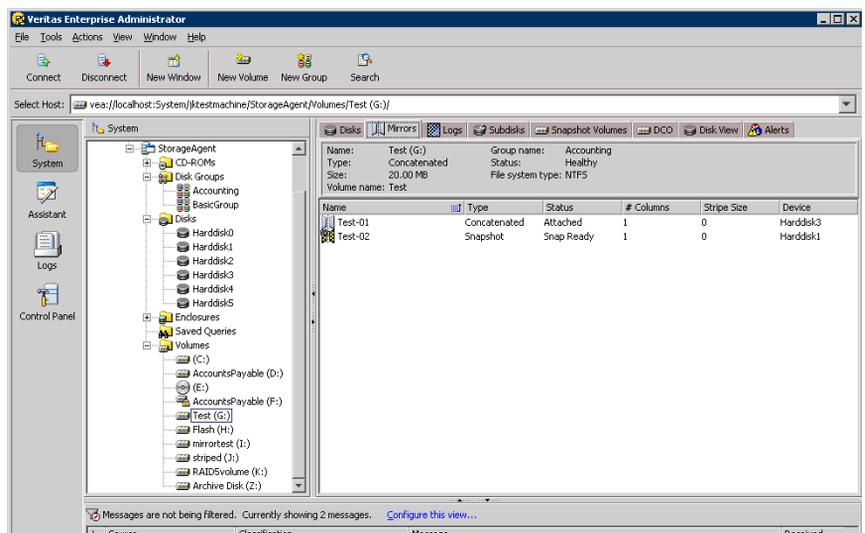
The middle of the screen displays a further explanation of the selected option.

The snapshot mirror is reattached to the original volume, and the snapshot volume is deleted if it is the last plex of the volume. (If the snapshot volume has other mirrors associated with it, it is not deleted.) As shown in the following figure, the snapshot volume, identified as L in the previous figure, is removed from the Volumes folder in the tree view, and the snapshot mirror is now shown on the **Mirrors** tab for the original volume. After the resynchronization, the original volume is now in a similar situation as it was after the first **Prepare** command, but any changes to it have been updated on the snapshot mirror.

Now it is possible to do another **Snapshot** command on the volume and repeat the process. If you are resynchronizing to the original volume, the resynchronization should take very little time because that volume was being constantly updated all the time.

Only the original synchronizing of the mirror in the original **Prepare** command takes the normal amount of time to create the snapshot mirror. Once you have completed the original **Prepare** command, the repeat procedure for **Snapshot** and **Snapshot Back** are very quick. You have to do the **Prepare** command only once.

Note that any mirrors added to the DCO volume of a snapshot volume are deleted when you snap back the snapshot volume.



Snap clear

Snap Clear permanently removes the link between a snapshot volume and its original volume. **Snap Clear** can be specified after the **Snap Shot** command has been issued. After a **Snap Clear**, the snapshot volume becomes an ordinary volume.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Snap Clear** command.

To change a snapshot volume to an ordinary volume

- 1 Right-click on the snapshot volume that you want to change to an ordinary volume. After the **Snap Clear** command is completed, the volume is no longer linked to its original volume.
- 2 Select **Snap>Snap Clear**.
A message box is displayed asking you to confirm the **Snap Clear** operation for the specified volume.
- 3 Click **Yes**.
The snapshot mirror becomes an ordinary volume. The original volume goes back to the state that it was in before the **Prepare** command.

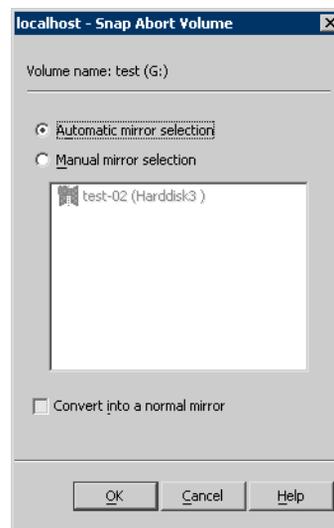
Snap abort

Snap Abort aborts the changes made by the **Prepare** or **Snap Back** command. In both these commands, a snapshot mirror plex is attached to a volume. **Snap Abort** either deletes this snapshot mirror plex or converts the snapshot mirror plex to an ordinary mirror. In cases where the deleted snap plex is the last snap plex and the resulting volume is simple or striped, the **Snap Abort** command deletes the DCO log volume also. The command cannot be done directly after a **Snap Shot** command.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the **Snap Abort** command.

To delete a snapshot mirror or change it into an ordinary mirror

- 1 Right-click the volume on which you want to abort the **Prepare** operation.
- 2 Select **Snap>Snap Abort** from the context menu that comes up.
- 3 Select the options in the Snap Abort Volume window that appears.



If you have only one mirror, you can leave the default setting of “Automatic mirror selection.” If there are multiple mirrors, you can manually select the mirrors to snap abort. If you click the checkbox **Convert into a normal mirror**, the selected mirror or mirrors become normal mirrors. Click **OK** when you are satisfied with your selections.

- 4 Respond to the message box asking you to confirm the **Snap Abort** operation for the specified volume. The snapshot mirror is deleted or converted. The DCO volumes are removed.

Using the Snapshot Scheduler wizard

You can use the Snapshot Scheduler wizard to add a snapshot schedule. The scheduling capability automates the process of taking snapshots. At the scheduled time, the specified volumes are automatically snapshotted. Once configured and applied, the schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background.

Note: Information about the operations performed by the schedule can be found by expanding the nodes under the Scheduled Tasks node in the tree-view of the GUI. Expand the appropriate application node to locate the schedules for that application. Right-click the node and select JobHistory to view information about the operations performed by the schedule.

Note: The Snapshot Scheduler only supports VSS snapshots (readonly snapshots).

Note: You must prepare the snapshot mirror with the Prepare command before running the Snapshot Scheduler wizard.

To create a scheule for snapshots

- 1 Right-click a volume in the tree-view.
- 2 Click Snap>Schedule SnapShot in the context menu.
- 3 In the wizard, review the Welcome page and click Next.
- 4 In the Select Volumes window that appears, select the volumes that you want to take a snapshot of.
Highlight the volumes in the Available volumes pane and click Add. Your selected volumes should appear in the Selected volumes pane.
Specify the snapshot set parameters as appropriate and then click Next

Directory	The wizard creates the snapshot set metadata XML file. The XMLmetadata file is stored by default in the directory shown on the screen.
Snapshot set	Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet.vol.timestamp".

- 5 In the Change Attributes window that appears, you may edit the following attributes as appropriate. Click Next to continue.
 - Drive Letter
 - Plex
- 6 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	Enter a unique name for the snapshot set schedule. This name identifies the snapshot schedule if you later want to view information about the snapshot status. A default name consists of a prefix, "Generic", and a numbered suffix that increments with each schedule.
Description of this schedule	Optionally, enter a description to help you identify the schedule when you view information about the snapshot status.
Start Time	The time of the day to begin taking snapshots.
End Time	The time of day to end taking snapshots. If a snapshot is in progress it is completed but a new one is not started after the end time.
Schedule takes effect on	The date on which the specified schedule takes effect. The default is the current date.
Restart task every	The interval between snapshots, in minutes. For example, if the interval is 360 minutes and you schedule a snapshot start time of 12 P.M. and an end time of 7 P.M, the snapshot occurs twice. If no interval is specified the snapshot occurs once.
Every	Enable the Every option to have the snapshot schedule continue to occur. Otherwise the schedule applies only for one day. Specify the number of days before restarting the snapshot schedule. For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.
Start On	If you enable the Every option, specify the starting date.

Pre Command	Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.
Post Command	Optionally, specify the full path of a command script to run after the snapshot is complete.

7 To specify run days for the schedule, make selections on the following tabs:

Days of Week	Select one or more days on one or more weeks of the month. You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.
Days of Month	Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.
Specific Dates	Select one or more specific dates to include in or to exclude from the schedule. Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.

If two schedules overlap for the same snapshot set, only one snapshot is taken. For example, if you select every Thursday plus the last day of the month, and the last day of the month occurs on Thursday, only one snapshot is taken on Thursday.

8 Click Next.

9 Review the specifications of the snapshot set and click Finish.

Displaying the status of the scheduled snapshot

If a scheduled snapshot fails for some reason, the scheduler process will attempt to rerun it. You may want to verify that scheduled snapshots completed successfully. From the VEA console, you can view snapshot results.

To view a scheduled snapshot status

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node and the Storage Agent node.
- 3 Click Scheduled Tasks.
- 4 Expand the Generic node. The scheduled snapshots are listed in the pane on the right.
All scheduled snapshots not associated with an Application are displayed under the Generic node.
- 5 Choose one of the following:
 - To view the status of all scheduled jobs, right-click Generic and click All Job History
 - To view the status of a particular schedule, right-click the snapshot schedule name and click Job History.
- 6 In the dialog box, view the schedule information.
You can sort listed schedules by clicking the column headings. The Status column shows if the snapshot completed successfully.

Deleting a schedule for a snapshot

The following is the procedure to delete a schedule.

Note: You cannot modify a schedule that has expired. You can also delete (but not modify) a schedule from the GUI console.

To delete a schedule with the GUI

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node and the Storage Agent node.
- 3 Click Scheduled Tasks.
- 4 Expand the Generic node for which you scheduled the snapshot. The scheduled snapshots are listed in the pane on the right.
- 5 Right-click the name of the snapshot schedule and click Delete Schedule.

Dynamic disk group split and join

This section on Dynamic Disk Group Split and Join has the following topics:

- [About dynamic disk group split and join](#)
- [Dynamic disk group split](#)
- [Recovery for the split command](#)
- [Dynamic disk group join](#)
- [Using dynamic disk group split and join with a cluster on shared storage](#)
- [Limitations when using dynamic disk group split and join with VVR](#)
- [DGSJ troubleshooting tips](#)

About dynamic disk group split and join

Dynamic Disk Group Split and Join (DGSJ) refers to two related commands—**Split Dynamic Disk Group** and **Join Dynamic Disk Group**. **Split Dynamic Disk Group** splits a dynamic disk group into two dynamic disk groups. **Join Dynamic Disk Group** joins two dynamic disk groups into one merged disk group. You can join two disk groups that were originally split apart with the **Split Dynamic Disk Group** command, but you can also join two dynamic disk groups that started out as separate disk groups.

DGSJ can be used for the FlashSnap process and to reorganize dynamic disk groups. DGSJ can be implemented through the VEA console or through the command line by using the `vxdg split` and `vxdg join` commands.

With the **Split Dynamic Disk Group** command, you can take some but not all disks from one dynamic disk group to another. The source dynamic disk group retains its identity as the original, while the other dynamic disk group, called the target disk group, becomes a new dynamic disk group. After the split operation, the target dynamic disk group is in the Imported state if you used the GUI to implement the command. If you used the command line to do the split, the target dynamic disk group is by default in the Deported state (though you can use the `-i` switch to have it remain in the Imported state). In both the GUI and the command line, the source dynamic disk group continues to remain online after the split operation.

Primary dynamic disk groups cannot be split because primary dynamic disk groups usually contain the computer's boot and system disks. Also, only healthy dynamic volumes can be transferred in the split operation. If you have dynamic disk groups created in Volume Manager 2.7 or earlier, you need to upgrade these disk groups to be compatible with Volume Manager 3.0 and 3.1 and SFW dynamic disk groups before you can use the DGSJ commands.

You can upgrade disk groups through the GUI.

See “[Upgrade a dynamic disk group version](#)” on page 199.

You can also upgrade disk groups through the command line.

See “[vxdg upgrade](#)” on page 312.

The **Split Dynamic Disk Group** command works on the premise that the split-off disk group should contain all disks that are needed to make the volumes in the new disk group complete. If the disks that you select to split the disk group result in incomplete volumes, the logic built into the command adds the remaining disk or disks needed to split the disk group with complete volumes. A screen is presented to you that lists the disks needed for the split. You can decide at that time whether you want to go ahead with the dynamic disk group split.

Thus, you are not able to split a dynamic disk group into two disk groups if any of the volumes allocated to either split disk group are incomplete.

The **Join Dynamic Disk Group** command allows you to combine dynamic disk groups. It does not require that the dynamic disk groups to be joined were previously split. When you join two dynamic disk groups, the dynamic disk group you designate as the source becomes the one that loses its identity in the merge. The target dynamic disk group is the one that remains after the join.

With the join command, all the disks of the source dynamic disk group are joined with all the disks of the target dynamic disk group. With Volume Manager 3.0 and 3.1, if some disks were missing or nonfunctional in the source dynamic disk group, the join command did not succeed. Veritas Storage Foundation for Windows now allows a partial join--that is, volumes in the source disk group can have missing or nonfunctional disks and the join command can still succeed. In this situation, you must click the **Allow Partial Join** checkbox to indicate that you want a partial join to take place. When the missing disk or disks come back to an online state, then you need to do another **Join Dynamic Disk Group** command to add the missing disk or disks to the target disk group.

Caution: If you have a partial join in place, you must wait until the missing disks or disks are joined to the target disk group before making the following configuration changes to either the source or target disk group: replace or evacuate disk, split or move a subdisk, extend a volume, add a mirror, and clear hot relocation. Doing so before all disks are joined can result in data loss.

The procedures in this section focus on the GUI commands related to Dynamic Disk Group Split and Join.

You can also perform Dynamic Disk Group Split and Join through the command line.

See “[vxdg](#)” on page 302.

Note: Microsoft Disk Management Disk Groups do not support Dynamic Disk Group Split and Join.

Dynamic disk group split

After a dynamic disk group is split with the GUI command, the target disk group is in an Imported state. If you want the dynamic disk group to be in a Deported state, use the CLI version of the command, `vxdg split`, in which the default state of the target disk group is Deported. However, you can also use the `-i` switch with `vxdg split` to have the target disk group be Imported.

With the GUI dynamic disk group split command, if the source disk group is a cluster disk group or a disk group with private dynamic disk group protection, the resulting target disk group becomes the same disk group type.

With the CLI disk group split command, these disk group types need additional parameters to ensure that they retain their respective disk group type.

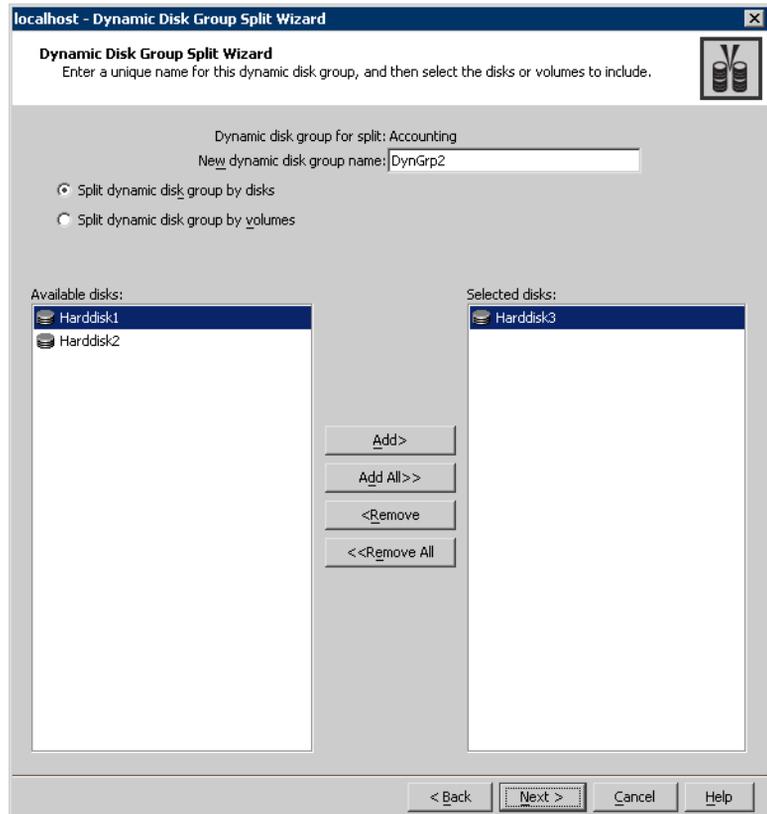
See “[vxdg split](#)” on page 316.

Note: Microsoft Disk Management Disk Groups do not support dynamic disk group split.

To split a dynamic disk group

- 1 Make sure that the volumes to be split are not in use and that they are healthy. Similarly, make sure that any disks that are split do not have a Missing status.
It is a good idea to use the Disk View to look at the disk group’s volumes and subdisks, so you can see which disks are appropriate to split. The disks in the new split-off disk group have to contain complete volumes.
If a volume is in use, an error message comes up, asking if you want to force the split operation.
See “[Error message about forcing a split or join operation](#)” on page 612.
- 2 Right-click a dynamic disk group, disk, or volume in the tree view of the VEA console, and click **Split Dynamic Disk Group** from the context menu. You can also select the command from the **Actions** menu on the VEA console menu bar.
- 3 The Dynamic Disk Group Split wizard appears. Click **Next** to continue.

- 4 In the screen that appears next, specify the information needed for splitting the disk group as follows:



- Enter the new dynamic disk group name.
The disk group name should be unique. The dynamic disk group name is limited to 18 characters. It cannot contain spaces or forward and backward slashes. Also, a period cannot be the first character of the name.
- Choose either the “Split dynamic disk group by disks” option or the “Split dynamic disk group by volumes” option.
When you choose to split by disks, disks appear in the panes in the lower section of the window. If you choose to split by volumes, volumes appear instead of disks.
- Select the disks or volumes that you wish to split.
The currently available disks or volumes in the specified disk group are displayed in the left pane, which is labeled “Available disks” or

“Available volumes.” You select disks or volumes in the left pane and then click the **Add** or **Add All** button to move them to the right pane, which is labeled “Selected disks” or “Selected volumes.”

The **Add All** button is provided for convenience in moving many disks at once. If all disks are moved, you need to move at least one of them back to the left pane, because you cannot split a dynamic disk group if you include all the disks in the target disk group.

The volumes and disks that belong to the source dynamic disk group and that are not being split remain accessible during the entire dynamic disk group split operation.

After entering the specifications, click **Next** to continue.

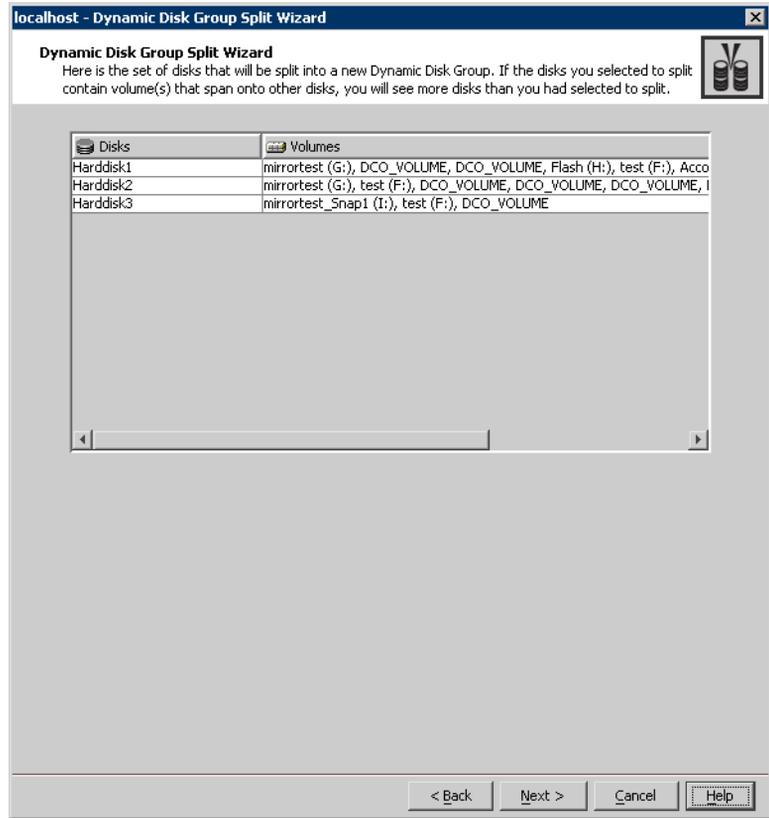
5 Verify the information for the dynamic disk group split.

The screen that follows shows the type of information you may see. The purpose of this screen is to allow you to confirm the disk group split.

The wizard shows the disks selected for the split in the left column and the volumes that are split in the right column. In this screen, you may see more disks than what you selected for the split. If the disks you have selected would result in a disk group with partial volumes, the program supplies the disks needed to ensure that the split-off dynamic disk group have complete volumes.

If you want to make the split-off dynamic disk group larger, you can click **Back** to go back and add more disks.

When you are satisfied that the information is correct, click **Next**.



- 6 Click **Finish** to confirm the dynamic disk group split.

If the dynamic disk group split is successful, you'll be able to view the new target dynamic disk group in the tree view and in the right pane of the console. By default, the new target disk group is in the Imported state if you are using the GUI to perform the split. If you use the command line to execute the split, the new target disk group is in the Deported state by default, because it assumes you want to deport the disk group and then import it on another computer. However, with the command line, you can use the `-i` switch with the `vxrdg split` command to have the disk group remain in the Imported state.

If the **Split Dynamic Disk Group** command fails, an error dialog box is displayed showing the reason for failure. The dynamic disk group split operation fails if the target disk group already exists or if a problem occurs when the split operation is taking place.

If the computer fails during the split operation, Veritas Storage Foundation for Windows provides a recovery process. The next section has the details on the recovery process.

Recovery for the split command

If disk and/or system failures occur during the disk group split operation, Veritas Storage Foundation for Windows generally performs any necessary recovery operations automatically. The recovery procedure performs any operations necessary to restore the disk group to a consistent state. On successful recovery, the disk groups are again available for use.

For example, if there is a power outage during the split operation, it results in incomplete information on the disk and in the disk group. The recovery mechanism ensures that when the host boots up the next time or if the disk group is imported on a host (the same host or another host), the inconsistencies in the information are removed. Depending on the amount of processing completed by the split operation at the time of the failure, the recovered disk group is either in the state it was in before the split operation or be successfully split into two disk groups.

Recovery has the following two modes:

■ **Automatic recovery**

If it is possible to reboot the system, Veritas Storage Foundation for Windows attempts automatic recovery after the reboot. If the automatic recovery process is able to detect sufficient information to perform the recovery, the recovery is successful and the disk group appears in a normal state after the automatic recovery process.

■ **Manual recovery**

In the following situations, it is necessary to do manual recovery:

- If the automatic recovery runs after the reboot and there is not sufficient information for recovery, the disk group is in a Deported state and displays an alert icon (a yellow caution icon).
- If you cannot reboot the system because it has failed completely, then you must move the disk group's disks to another system and then do a manual recovery. In this situation, it is recommended that you move the entire source disk group to another computer, rescan, and implement the recovery manually.
- It becomes clear that a disk group needs manual recovery after a split command when Veritas Storage Foundation for Windows does not allow imports of the disk group to succeed or it blocks the join of a disk group. You receive an error message indicating that the disk group needs recovery.

Recovery should be done as soon as possible to preserve the integrity of the data. You can perform manual recovery through the GUI as described in the following procedure.

You can also perform manual recovery through the command line.

See “[vxdg recover](#)” on page 319.

To manually recover the dynamic disk group

- 1 Right-click the disk group icon in the VEA GUI and select **Recover Dynamic Disk Group** from the context menu that appears.
- 2 In the dialog box that appears, make sure the proper disk group name is showing, and click **OK** to have Veritas Storage Foundation for Windows start the recovery process.



On the successful completion of the manual recovery operation, the user can perform all Veritas Storage Foundation for Windows operations. The only exception is that if a host crashes during a particular stage of the split operation, one or more of the disk group's disks and volumes may come up in an unhealthy state after recovery. In that situation, use the **Reactivate Disk** command on the unhealthy disks and then the **Reactivate Volume** command on each of the unhealthy volumes involved in the split command. After running these commands, the disk group's disks and volumes should be healthy.

See “[Reactivate disk command](#)” on page 491.

See “[Reactivate volume command](#)” on page 492.

Dynamic disk group join

This section describes the procedures for a dynamic disk group join operation.

When you join two dynamic disk groups, the disk group you designate as the source becomes the one that loses its identity in the merge. The target dynamic disk group is the one that remains after the merge.

With Volume Manager 3.0 and 3.1, if some disks were missing or nonfunctional in the source dynamic disk group, the join command did not succeed. Veritas Storage Foundation for Windows now allows a partial join—that is, volumes in the source disk group can have missing or nonfunctional disks and the join command can still succeed.

See “[About partial disk group join](#)” on page 608.

The disk group type after the join becomes the type of the target disk group. For example, if the target disk group before the join had private dynamic disk group protection, the combined disk group has private dynamic disk group protection after the join.

Note: A cluster dynamic disk group that is part of the cluster resources cannot be a source disk group for a join command. However, it can be a target disk group for the command.

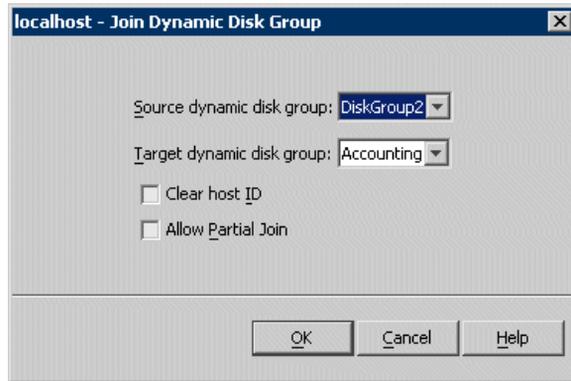
Note: It is possible to force the join command when a volume is in use or if disks from the source disk group’s disks are missing, but doing so is not recommended as a best practice.

Note: Microsoft Disk Management Disk Groups do not support dynamic disk group join.

To join two disk groups into one disk group:

- 1 Make sure that the volumes in the source dynamic disk group are not in use and are healthy.
- 2 Right-click the disk group object in the left pane of the VEA console, and then click the **Join Dynamic Disk Group** command, or select the **Join Dynamic Disk Group** command from the **Actions** menu on the VEA console menu bar.

The Join Dynamic Disk Group dialog box appears as shown:



- 3 In the Join Dynamic Disk Group dialog box, make sure the correct source and target disk groups are indicated. If necessary, use the drop-down lists to change the disk group names.

The **source dynamic disk group** is the disk group that is merged with the target dynamic disk group. The source disk group ceases to exist after the join.

The **target dynamic disk group** is the disk group that remains after the join. It retains its identity and becomes larger with the addition of the disks from the source disk group.

The **Clear host ID** checkbox should be used when you want to import a disk group from another node and that disk group was not properly deported. A host ID might not be cleared, for example, if the host computer became nonfunctional. When a host ID has not been cleared, SFW does not permit the join without the Clear host ID override. Use this override with care.

The **Allow Partial Join** checkbox can be used when you have a missing or nonfunctional disk or disks in the source disk group and you want SFW to allow the join to occur.

See “[About partial disk group join](#)” on page 608

- 4 Click **OK**.
If the join operation is successful, the source dynamic disk group merges into the target dynamic disk group. The changes in the target dynamic disk group are reflected in the VEA console tree view and right pane.
If a volume is in use, SFW displays an error message about forcing the join command.

See “[Error message about forcing a split or join operation](#)” on page 612.

If there is an error message about the disks not being ready, you can click the checkbox for the partial join to allow the command to complete.

If the join operation fails, an error dialog box is displayed, showing the reason for the failure.

The new dynamic disk group after the join command are of the same type as the target dynamic disk group. For example, if a cluster dynamic disk group is joined with a normal dynamic disk group, then the new dynamic disk group is a normal dynamic disk group.

About partial disk group join

With Volume Manager 3.0 and 3.1, if some disks were missing or nonfunctional in the source dynamic disk group, the join command did not work. Veritas Storage Foundation for Windows now allows a partial join—that is, volumes in the source disk group can have missing or nonfunctional disks and the join command still succeeds. However, you need to click the **Allow Partial Join** checkbox in the Join Dynamic Disk Group window for the join to take place. When the missing disk or disks come back to an Online state, then you need to do another **Join Dynamic Disk Group** command to add the missing disk or disks to the target disk group.

Caution: If you have a partial join in place, you must wait until the missing disks or disks are joined to the target disk group before making the following configuration changes to either the source or target disk group: replace or evacuate disk, split or move a subdisk, extend a volume, add a mirror, and clear hot relocation. Doing so before all disks are joined can result in data loss.

Using dynamic disk group split and join with a cluster on shared storage

This section describes the use of the Dynamic Disk Group Split and Join operations with SFW cluster disk groups on shared storage. SFW supports cluster dynamic disk groups with either Veritas Cluster Server (VCS) or Microsoft Clustering (Microsoft Cluster Service (MSCS) on Windows Server 2003; or the Failover Cluster feature on Windows Server 2008).

The section covers the following topics:

- [Using DGSJ with VCS or Microsoft Clustering](#)
- [Example of an off-host backup procedure using SFW and VCS or Microsoft Clustering](#)

Using DGSJ with VCS or Microsoft Clustering

If a disk group is under VCS or Microsoft Clustering control, SFW imposes certain conditions on the functioning of the Dynamic Disk Group Split and Join operations.

These conditions are the following:

- If a shared dynamic cluster disk group is joined to another (possibly shared) dynamic disk group and the source disk group is configured as a VCS or Microsoft Clustering resource, then the join operation fails.
- If a dynamic disk group (possibly shared) is joined to another shared cluster dynamic disk group and the target disk group is configured as a VCS or Microsoft Clustering resource, then the join operation is allowed to proceed.
- (VCS only) If a shared dynamic cluster disk group is split into another (possibly shared) disk group and the source disk group is configured as a VCS resource, then the split operation is not allowed to proceed, with one exception. The exception is that the split operation can proceed when the volumes selected to be split off are NOT configured under VCS. Thus, in this situation, if users want to split any volumes that are configured under VCS, they should remove the volumes from VCS monitoring and retry the split operation.
- (Microsoft Clustering only) If a shared dynamic cluster disk group is split into another (possibly shared) disk group and the source disk group is configured as an Microsoft Clustering resource, the split operation is allowed to proceed. However, before the command completes, a confirmation window appears to remind you that if you split a disk group resource so that a volume on which other cluster resources depend is moved to a new SFW cluster disk group, it is necessary to define the new cluster

disk group as a Microsoft Clustering resource and to modify the properties of dependent resources to reflect the change.

If necessary, use the Windows Server 2003 Cluster Administrator or Windows Server 2008 Failover Cluster Management to check and modify resource dependency fields as follows:

- Define the new cluster disk group as a Volume Manager cluster disk group resource.
Even though the name of the program has changed to Storage Foundation for Windows, the resource group is still named “Volume Manager.”
 - If the new disk group resource is in a different Microsoft Clustering group than the original cluster disk group resource, move all resources that depend on the new cluster disk group resource to the Microsoft Clustering group where it resides.
 - For each dependent resource, do the following:
 - Offline the resource.
 - Right-click on the resource and select **Properties**.
 - Select the **Dependencies** tab in the resource's Properties window.
 - If the resource lists the disk group that was the source of the split operation as a dependency, click the **Modify** button.
 - Move the new disk group from the **Available Resources** pane of the Modify Dependencies window to the **Dependencies** pane, and move the old disk group from the **Dependencies** pane to the **Available Resources** pane, if it appears in the **Dependencies** pane.
 - Online the resource.
- 5 (VCS only) If there is a hardware failure or a power failure during an ongoing disk group split operation and the disk group being split is configured under VCS, then VCS attempts to failover that disk group to another node in the cluster and brings the disk group online.
At that time, appropriate disk group split recovery is carried out as required to bring the disk group online.
See “[Recovery for the split command](#)” on page 604.
Manual intervention may or may not be required to recover the disk group.
- 6 If you are splitting a dynamic cluster disk group that contains the quorum volume, make sure that the quorum volume is not part of the target disk group after the split operation. If you fail to do so, the quorum volume is not able to function and the cluster fails.

Example of an off-host backup procedure using SFW and VCS or Microsoft Clustering

This section describes how to use SFW and VCS or Microsoft Clustering in a typical off-host backup procedure.

In the example, a disk group named “SQL” has volume “V” on which a SQL Server database is under heavy use by clients. This disk group is imported on one node of a cluster running VCS or Microsoft Clustering. VCS or Microsoft Clustering monitors the disk group as well as the volume, ensuring high availability.

In the off-host backup solution outlined below, the high availability of the volume V is not affected at all. While the successful backup is taking place, the SQL server provides uninterrupted service to its clients with minimum configuration changes on both nodes in the cluster.

The procedure is fully scriptable and thus can be automated to provide a backup on a hourly, daily, weekly, or monthly basis.

To implement off-host backup

- 1 Create a snapshot “V1” of the volume V with the snap commands in the VEA GUI or the CLI.
See “[Snapshot commands](#)” on page 577.
- 2 Split the dynamic disk group SQL into another dynamic disk group “Temp” so that V1 resides on the disks in the Temp disk group. Since VCS or Microsoft Clustering is monitoring V (and not V1), the split operation succeeds.
See “[Dynamic disk group split](#)” on page 600.
- 3 Deport the Temp disk group and import it on another node in the cluster.
See “[Importing and deporting dynamic disk groups](#)” on page 205.
- 4 Back up volume V1 on the second node, using the backup software.
- 5 After backup is complete, deport the Temp disk group on the second node.
- 6 Join the Temp disk group to the SQL disk group on the first node. Since the SQL disk group is a VCS or Microsoft Clustering resource (and the Temp disk group is not monitored), the join operation succeeds.
See “[Dynamic disk group join](#)” on page 606.
- 7 The snapshot volume V1 can then be snapped back to its parent volume V.
See “[Snap back](#)” on page 588.

Limitations when using dynamic disk group split and join with VVR

If you are using the Dynamic Disk Group Split and Join commands with volumes that are under Veritas Volume Replicator (VVR) control, the following limitations apply:

- A volume under replication cannot be part of the volumes split off to the target disk group. It can remain in the source disk group.
- A join operation is not allowed if the source disk group has any VVR objects.

DGSJ troubleshooting tips

This section provides information and workarounds for problems that might arise when using the Dynamic Disk Group Split and Join commands.

Error message, “The disk group requires recovery. please recover...”

This message can occur when you attempt to import a disk group or do a join command. The message indicates that the disk group needs recovery because of a problem that occurred during a disk group split operation.

See [“Recovery for the split command”](#) on page 604.

Error message, “One or more disk(s) in the source dynamic disk group are missing.”

This message can occur when you attempt a disk group split or join operation and a disk in the disk group is no longer functional or has gone offline. It is recommended that you rescan and then retry the disk operation. However, if one or more disks in the disk group is missing or nonfunctioning, you can click the **Allow Partial Join** checkbox to have the join command succeed even though one or more disks are missing.

See [“About partial disk group join”](#) on page 608.

Error message about forcing a split or join operation

If you attempt a dynamic disk group split or join command when a volume is in use, Veritas Storage Foundation for Windows puts up a message asking whether you want to force the split or join. If the volume is in use because it is selected in Windows Explorer, then you can force the split or join safely. However, if the volume is actually in use within an application, it is not recommended that you attempt to complete the command. If a volume is regenerating, resynching, or recovering, then even if you force the split or join, the operation is not successful.

CLI FlashSnap commands

SFW provides command line interface commands corresponding to the GUI FlashSnap commands presented in this chapter. The following table lists each GUI FlashSnap command with a cross reference to its corresponding CLI command. It also has some additional comments to clarify distinctions between the two CLI snapshot commands, `vxsnap` and `vxassist snapshot`.

Table 12-1 FlashSnap GUI and CLI Commands Correspondences

GUI Command	Corresponding CLI Command
FastResync	See “ <code>vxvol set fastresync=on off</code> ” on page 290.
Prepare	See “ <code>vxassist prepare</code> ” on page 363. Note: The Prepare command replaces the Snap Start command in the GUI. Both <code>prepare</code> and <code>start</code> keywords are available in the CLI, however <code>prepare</code> is the recommended keyword.
Snap Shot	There are two snapshot commands. The command <code>vxassist snapshot</code> allows snapshotting only a single volume at a time. The command <code>vxsnap</code> allows simultaneous, multiple snapshots. The <code>vxsnap</code> command integrates with VSS to enable VSS snapshots with Microsoft Exchange Server 2003.
Snap Back	See “ <code>vxassist snapback</code> ” on page 368.
Snap Clear	See “ <code>vxassist snapclear</code> ” on page 369.
Snap Abort	See “ <code>vxassist snapabort</code> ” on page 371.

Note: Refer to the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange* for detailed procedures on how to use FlashSnap with Microsoft Exchange Sever 2003 to perform snapshots and to implement recovery procedures.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the `vxassist prepare`, `vxassist snapshot`, `vxassist snapback`, `vxassist snapclear`, and `vxassist snapabort` commands.

Fast file resync

Fast File Resync (FFR) allows you to resynchronize one or more files in a snapshotted volume back to the original volume.

This section covers the following topics:

- [Overview](#)
- [Prerequisites](#)
- [Resynchronizing a file](#)
- [Possible error for small files](#)

Note: Fast File Resync requires the FlashSnap option be installed.

Overview

Fast File Resync uses Veritas FastResync technology to resynchronize selected files in a snapshotted volume to the original volume. Fast File Resync is designed for database applications using volumes with multiple database files and can be used to restore one or more corrupt files. A snapback command that resynchronizes the split-mirror snapshot back to the original files is performed *only* for the selected files. Other databases do not have to be off-lined during the Fast File Resync process, and the entire volume is not resynchronized. The Fast File Resync command restores the file or files on the original volume but does not bring the database to a current state.

In general, the FastResync technology used by Fast File Resync is more efficient for files greater than 50 MB, and the Windows Explorer copy function or Windows xcopy command is more efficient for files smaller than approximately 50 MB. Fast File Resync is unable to restore a file that has been deleted.

Also, it may not work on files smaller than 8 KB.

See “[Possible error for small files](#)” on page 616.

Caution: It is important to wait until the FFR process is complete before accessing and using the restored file. Data corruption can occur if the file is used before the resynchronization is complete.

The Fast File Resync command can be issued through the VEA or through a CLI command, `vxfsync`.

However, the CLI command does not support resynchronization of multiple files. It supports the resynchronization of one specified file at a time.

See “[vxfsync](#)” on page 455.

Note: Fast File Resync is not available through the VEA GUI of a SFW remote client connected to a SFW server.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support Fast File Resync.

Prerequisites

The following prerequisites must be met for a successful FFR resynchronization of a file:

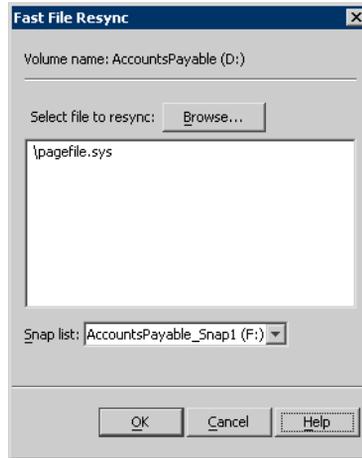
- The names and creation times of the snapshot and original files are identical.
- The file is formatted using NTFS.
- The file is not compressed.
- The file is not encrypted.
- There are no open handles on either file.

Resynchronizing a file

To resynchronize corrupted files

- 1 Right-click on the original volume containing the corrupted file and select **Fast File Resync**.

The Fast File Resync dialog box appears.



- 2 Click **Browse** and navigate to the file or files that you want to copy from the snapshot volume back to the original volume. Use the Control and Shift keys to select multiple files. Click **Select**.
- 3 Select the desired snapshot volume from the **Snap list**.

Note: A snapshot volume must have either a drive letter or a mount point assigned for it to be available for selection from the **Snap list** in the Fast File Resync window.

- 4 Click **OK**.

Possible error for small files

When using Fast File Resync to resynchronize files smaller than 8 KB, the file extents call to the operating system may fail and an error message notifies you that the call has failed and refer you to the trace for further information.

If this error occurs, use the Windows Explorer copy function or Windows xcopy command to copy the file.

The trace can be found at `\Veritas\Veritas Object Bus\logs\vxisis.log`. The error is prefixed by **vxffr**.

Volume Shadow Copy Service (VSS)

This section describes how Veritas Storage Foundation for Windows works with Volume Shadow Copy Service (VSS) to provide snapshots.

This section covers the following topics:

- [Overview](#)
- [VSS components](#)
- [Overview of VSS process for SFW snapshots](#)
- [VSS snapshot wizard for Microsoft Exchange, Microsoft SharePoint, and Microsoft SQL](#)

Overview

Volume Shadow Copy Service (VSS) is a Windows service that provides the capability of creating snapshots or volume shadow copies. A volume shadow copy is a volume that represents a duplicate of the state of the original volume at the time the copy began. Thus, through VSS, point-in-time copies of data can be saved and used for different purposes, such as backup or application testing.

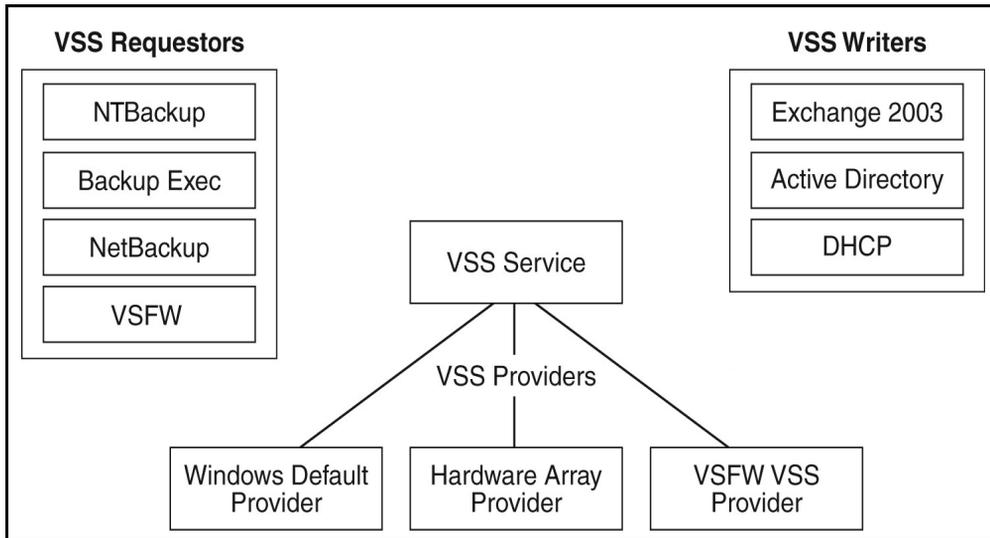
VSS snapshots represent an advance in snapshot technology because snapshots can be taken when application files are open. VSS interacts with an application (such as Microsoft Exchange) and can quiesce the application for the moment when the snapshot is created. VSS restarts the application immediately after the snapshot. VSS only takes snapshots of read/write volumes and the resulting volume shadow copy is a read only volume.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support the Volume Shadow Copy Service (VSS).

VSS components

VSS works through an infrastructure that coordinates the snapshot process by using software components from Microsoft itself and from various storage software and hardware vendors. The illustration below indicates the VSS service and the three key software components used in the VSS process—requestors, writers, and providers.

VSS components



1) Requestors

The software component that requests the creation of the snapshot is known as the requestor. NTBackup is the default requestor that comes with Windows. Veritas Backup Exec and NetBackup also have requestor components for VSS. In addition, SFW can function as a VSS requestor when the FlashSnap option is installed.

2) Writers

These are application-specific software components that ensure that the application data is quiesced and then restarted after the snapshot. Microsoft has provided the writer software component in Exchange 2003 and in the Active Directory and DHCP software features that are included in Windows.

3) Providers

Providers are the software components that implement the snapshots. Windows comes with a default provider. However, the SFW VSS provider and providers

from hardware array manufacturers offer enhanced functionality. For SFW to act as a provider, the FlashSnap option must be installed.

For the VSS process to work properly, the different software programs involved in the process need to be “VSS-aware” – that is, the necessary software components have been added to the programs so that they can participate. Again, it may take time for software and hardware vendors to provide the various VSS components with their products.

SFW as a VSS Provider and Requestor

An example in which SFW acts as a provider is a backup situation where Veritas Backup Exec is the requestor, initiating a snapshot of a SFW volume that is part of a Microsoft Exchange 2003 database. Microsoft Exchange is the VSS-aware writer.

As a VSS requestor, SFW with FlashSnap can initiate snapshots at any time. It is not dependent on a backup program to initiate the snapshot. Thus, SFW with FlashSnap integrates with VSS and is able to snapshot volumes associated with an Exchange 2003 storage group without taking the databases offline. The VSS process allows the databases of the storage group to be quiesced before the snapshot operation occurs and then reactivated immediately after it. This quiescing, supported by Exchange 2003 at the storage group level, allows for Microsoft supported and guaranteed persistent snapshots of your data.

Recovery

In addition to snapshots, SFW provides recovery support for Microsoft Exchange storage groups or individual databases within an Exchange storage group. Through SFW’s VSS Snapshot wizard or `vxsnap restore` command, the VSS snapshots can be used for a point-in-time recovery of the storage group or a roll-forward recovery to the point of failure of either the storage group or an individual database within it.

The point-in-time recovery restores the data to the point in time that the quick recovery image was last refreshed—that is, it restores all the data to what was recorded in the snapshot.

The point-of-failure recovery recovers the Exchange storage group by restoring the old image of the data volumes only and replaying the logs to accomplish a roll-forward recovery, provided that the log volume is intact.

For Exchange 2007, there is also an option to restore to a recovery storage group (RSG) rather than to the production store.

Refer to the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange Sever 2003* to perform snapshots and to implement recovery procedures.

Also see “[vxsnap](#)” on page 407.

Advantage of SFW Snapshots

The snapshots created with VSS through the Windows default provider are limited to copy-on-write snapshots. That is, the snapshot does not include a full copy of the original image but refers back to the original volume. For this reason, the default provider snapshots cannot be used for any procedures that involve off-host processing. The Veritas FlashSnap snapshot procedures produce independent split-mirror snapshot volumes that can be used for off-host processing. Thus, the FlashSnap snapshots implemented through SFW offer a definite advantage over snapshots created with the Windows default provider.

Overview of VSS process for SFW snapshots

The process for creating SFW snapshots with VSS can be done through the GUI, the command line, or a script with CLI commands.

Note: Snapshots can only be taken of read/write volumes when VSS is used. The resulting VSS snapshot is read only. The file system label of VSS snapshot volumes cannot be changed.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support snapshot or VSS related commands.

It is recommended that you use the GUI **Snap Back** command or `vxassist snapback` to reattach the snapshot mirror to its original volume. This enables you to update the snapshot mirror and make it available for more timely backups.

To create SFW snapshots with VSS

- 1 Use the **Prepare** command in the GUI or the `vxassist prepare` command to attach a snapshot mirror to a volume on the working server. Creating the snapshot mirror of the volume and resynchronizing it to the volume takes considerable time, but it only has to be done once for the initial setup.
The **Prepare** command replaces the **Snap Start** command in the GUI. Both `prepare` and `start` keywords are available in the CLI, however `prepare` is the recommended keyword.
- 2 Request a snapshot through a backup program (such as Veritas Backup Exec) or through SFW. In SFW, initiate a VSS snapshot through the GUI with the **Snap Shot** command. Be sure to enable the VSS snapshot method

in the Systems Settings in the VEA Control Panel. You can also use the `vxsnap` CLI command to take the snapshot.

If you are planning to use these snapshots to recover a Microsoft Exchange database, use the `vxsnap` command or the VSS Snapshot wizard.

See [“Using the VSS snapshot wizards with Microsoft Exchange”](#) on page 624.

The `vxsnap` command allows you to snapshot multiple volumes simultaneously; thus, you can snapshot all the volumes in a Microsoft Exchange storage group at one time. The VSS Snapshot wizard can also snapshot a storage group one at a time.

- 3 VSS interacts with a writer utility for the application to make sure that the application is momentarily quiesced for the snapshot.
- 4 VSS determines the appropriate provider for the snapshot. The Microsoft default provider is used only if another provider is not present. If a SFW dynamic volume is involved, then SFW would be selected as the provider.
- 5 After the snapshot is taken, the writer utility makes sure the application is restarted.
- 6 Once the snapshot takes place successfully, VSS communicates the successful result to the program with the requestor software.

VSS snapshot wizard for Microsoft Exchange, Microsoft SharePoint, and Microsoft SQL

Storage Foundation integrates with the Windows Volume Shadow Copy Service (VSS) as both a VSS Requestor and a VSS Provider. This integration is provided by FlashSnap.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support snapshot or VSS related commands.

FlashSnap integrates with VSS and uses the `vxsnap` command to provide the ability to detach multiple split-mirror snapshot volumes simultaneously. This allows you to snapshot all volumes associated with an Exchange storage group, SharePoint components, or SQL database at exactly the same point in time without taking the databases offline. When viewed all together these snapshots form a snapshot set of the storage group or database. These persistent FlashSnap snapshots, taken through VSS, can later be used for either a point-in-time recovery or a roll forward recovery to point of failure of the storage group or database.

FlashSnap calls VSS to perform a “copy backup” of Exchange, which does not truncate the transaction log files.

The following steps occur during the snapshot process:

- 1 Acting as a VSS Requestor, FlashSnap notifies the VSS coordinator service to prepare for a split-mirror snapshot of an Exchange storage group, Sharepoint components, or SQL database.
- 2 The VSS coordinator service calls the Exchange VSS Writer, Sharepoint VSS Writer, or SQL VSS Writer to find out which volumes contain the databases and transaction logs.
- 3 The VSS coordinator service notifies the FlashSnap VSS Provider to prepare for the snapshot.
- 4 Acting as a VSS Requestor, FlashSnap requests that the VSS coordinator service begin the snapshot call.
- 5 The VSS coordinator service notifies the Exchange VSS Writer, SharePoint Writer VSS, or SQL VSS Writer to quiesce the databases in preparation for the snapshot. When this is accomplished, the Exchange Writer, SharePoint VSS Writer, or SQL Writer informs the VSS coordinator service to proceed.
- 6 The VSS coordinator service calls the FlashSnap Provider to create the split-mirror snapshot by detaching the snapshot volume from the original volume. After the snapshot volume is detached, the FlashSnap Provider informs the VSS coordinator service to proceed.

- 7 The VSS coordinator service notifies the Exchange Writer, SharePoint Writer, or SQL Writer to resume normal I/O.

Using the VSS snapshot wizards with Microsoft Exchange

SFW provides support for taking snapshots of Microsoft Exchange 2003 and Exchange 2007 storage groups. FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with an Exchange storage group without taking the storage group's databases offline. The VSS Snapshot wizard uses VSS to take snapshots of storage groups. The VSS process allows the storage group's databases to be quiesced before the snapshot operation and reactivates them immediately after. The quiescing at the storage group level allows for Microsoft supported and guaranteed persistent snapshots of the data. A snapshot of a storage group can be reattached and resynchronized to match the current state of the storage group with the VSS Snapback wizard.

Note: Snapshots can only be taken of read/write volumes when VSS is used. The resulting VSS snapshot is read only. The file system label of VSS snapshot volumes cannot be changed.

SFW also provides a VSS Snapshot Scheduler wizard that can be used as an alternative to the VSS Snapshot wizard and the VSS Snapback wizard. It enables you to set up a schedule for taking the initial snapshots and for automating the snapback process. At the scheduled time for the snapshot, the snapshot volumes are automatically reattached, resynchronized, and then split again. The schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background.

SFW also provides recovery support for an Exchange storage group or a select database within a storage group. Using the VSS Restore wizard, the snapshots taken with the VSS Snapshot wizard can be used for a point-in-time recovery of the storage group or a roll-forward recovery to the point of failure of either the storage group or an individual database in the storage group.

The point-in-time recovery restores the data to the time that the snapshot set was last refreshed—that is, it restores all the data that was recorded in the snapshot.

The point-of-failure recovery recovers the Exchange storage group by restoring the old image of the data volumes only and replaying the logs to accomplish a roll-forward recovery, provided that the log volume is intact.

For Exchange 2007 only, if you have set up a recovery storage group (RSG), you have the option to restore to the RSG rather than to the production volume, leaving the production volume intact. Follow the Microsoft instructions in

creating the RSG. The database names in the recovery storage group must match those in the source storage group.

Refer to the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange* for additional information about how to use FlashSnap with Microsoft Exchange to perform and to implement recovery procedures.

This section covers the following topics:

- [Using the VSS Snapshot wizard](#)
- [Using the VSS Snapback wizard](#)
- [Using the VSS Snapshot Scheduler wizard](#)
- [Using the VSS Restore wizard](#)
- [Refreshing the snapshot set](#)

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support snapshot or VSS related commands.

Using the VSS Snapshot wizard

Creating a snapshot is a two-step process. The first step, prepare the volume for snapshot, creates snapshot mirrors attached to all the original volumes in the specified storage group. Depending on the size and number of volumes, the process of synchronizing the new snapshot mirrors with the original production volumes can take a long time. The second step uses the VSS Snapshot wizard to create the snapshot set by detaching the snapshot mirrors from the original volumes and creating separate on-host snapshot volumes as well as an XML file to store the Exchange and snapshot volume metadata. The VSS Snapshot wizard integrates with VSS to quiesce the databases and then simultaneously snapshot the volumes in the storage group. This snapshot is done while the databases are online and without disrupting the email flow. Once a snapshot set has been created, it can be reattached and resynchronized with the VSS Snapback wizard.

Creating the snapshot set

Note: You must prepare each volume for a snapshot before running the VSS Snapshot wizard.

To snapback a snapshot set

- 1 Close the database application GUI and all Explorer windows, applications, consoles (except the VEA console), or third-party system management tools that may be accessing the snapshot set.
- 2 From the VEA console URL bar, select the *<host name>* which is the system where the production volumes and snapshot mirrors are located, as the active host.
- 3 Expand the system node, the Storage Agent node, and the **Applications** node.
- 4 Right-click on the node of the application and click **VSS Snapback**.
- 5 Review the Welcome page and click **Next**.
- 6 Select the snapshot set you want to snapback and click **Next**.
The XML metadata file contains all required information needed to snapback the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**. This file is deleted after the snapback operation has completed successfully.
- 7 If a message appears that indicates some volumes have open handles, confirm that all open handles are closed and then click Yes to proceed.
- 8 Verify that the snapback specifications are correct and click **Finish**.

Using the VSS Snapback wizard

The VSS Snapback wizard reattaches and resynchronizes an existing snapshot set so that it matches the current state of its original Exchange storage group. The wizard is available in the context menu of the VSS Writer object.

Resynchronizing the snapshot set

To snapback a snapshot set

- 1 Close the database application GUI and all Explorer windows, applications, consoles (except the VEA console), or third-party system management tools that may be accessing the snapshot set.
- 2 From the VEA console URL bar, select the *<host name>* which is the system where the production volumes and snapshot mirrors are located, as the active host.
- 3 Expand the system node, the Storage Agent node, and the **Applications** node.
- 4 Right-click on the node of the application and click **VSS Snapback**.
- 5 Review the Welcome page and click **Next**.
- 6 Select the snapshot set you want to snapback and click **Next**.
The XML metadata file contains all required information needed to snapback the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**. This file is deleted after the snapback operation has completed successfully.
- 7 If a message appears that indicates some volumes have open handles, confirm that all open handles are closed and then click Yes to proceed.
- 8 Verify that the snapback specifications are correct and click **Finish**.

Using the VSS Snapshot Scheduler wizard

You can use the VSS Snapshot Scheduler wizard to add a snapshot schedule.

The scheduling capability automates the process of refreshing snapshot sets. At the time scheduled for the snapshot, the snapshot volumes are automatically reattached, resynchronized, and then split again. Once configured and applied, the schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background. In a clustered server environment, ensure that the scheduler service is configured on each node with domain administrator privileges so that any node in the cluster can run the schedule after a failover.

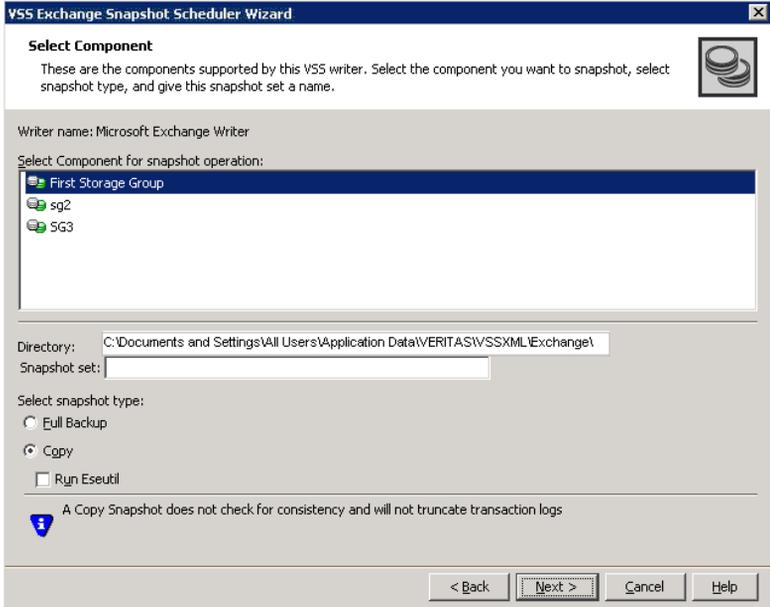
The VSS Snapshot Scheduler wizard does not prepare the snapshot mirror. Prepare the snapshot mirror with the **Prepare** command before running the VSS Snapshot Scheduler wizard.

Note: The **Prepare** command replaces the **Snap Start** command in the GUI.

To schedule a snapshot

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node, the Storage Agent node, and the **Applications** node.
- 3 Right-click **Exchange** and click **Schedule VSS Exchange Snapshot**.
- 4 Choose one of the following:
 - Right-click **Exchange** and select **VSS Exchange Snapshot**.
 - Optionally, if replication is enabled in an Exchange 2010 DAG and you want to create a schedule on the replication node, right-click **Exchange Replica** and click **Schedule VSS Exchange Snapshot**.
- 5 In the Welcome panel, review the information and click **Next**.

6 Specify the snapshot set parameters as follows and then click **Next**:



Select component for snapshot operation	<p>Select the component for the snapshot set.</p> <p>For Exchange 2003 or 2007, the component is a storage group.</p> <p>For Exchange 2010, the component is a mailbox database.</p>
Directory	<p>Accept or enter a directory location for the XML file.</p> <p>The XML file is stored by default in the directory shown on the screen.</p> <p>Note: The XML file for the snapshot must be stored separately from the volumes that are included in the snapshots, otherwise a restore will fail.</p> <p>In a clustered server environment, the XML file must be saved on shared storage to be available from all nodes in the cluster. To accomplish this, either edit the directory path in the Directory field for this wizard screen or use a text editor to create a text file named <code>redirect.txt</code>. This text file should contain a single text line specifying the full path to the location of the XML file, for example, <code>G:\BackupSets</code>. Save the <code>redirect.txt</code> file in the default directory <code>C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML</code> on each node of the cluster.</p> <p>Note: You must not use the volume name or volume path in the <code>redirect.txt</code> file that is involved in the snapshot. If the volume name or path for the snapshot is used, then a restore will fail.</p> <p>Note that if your Exchange 2010 mailbox database is configured under a VCS cluster, then you can store the snapshot set metadata file in a file share path by configuring a file share resource. You can also specify the file share path in the <code>redirect.txt</code> file.</p>
Snapshot set	<p>Enter a name for the snapshot set.</p>

Select snapshot type

Select the snapshot type.

Full Backup is typically used for backup to tape or other storage media. It does the following:

- Creates a copy of the selected component
- Runs **Eseutil** to check for consistency before truncating the logs
- Truncates the transaction logs

Copy is typically used for Quick Recovery. It creates a copy of the storage group, but does not truncate the transaction logs. Optionally, check **Run Eseutil** with the **Copy** option to check the snapshot for consistency.

You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a database.

- 7 In the Change Attributes panel, optionally change the attributes for the snapshot volumes and click **Next**:

Snapshot Volume Label

Displays the read-only label for the snapshot volume.

Drive Letter

Optionally, click a drive letter and select a new choice from the drop-down menu.

The drive letters specified may not be available when the snapshot is taken. When this occurs, the snapshot operation is performed, but no drive letters are assigned.

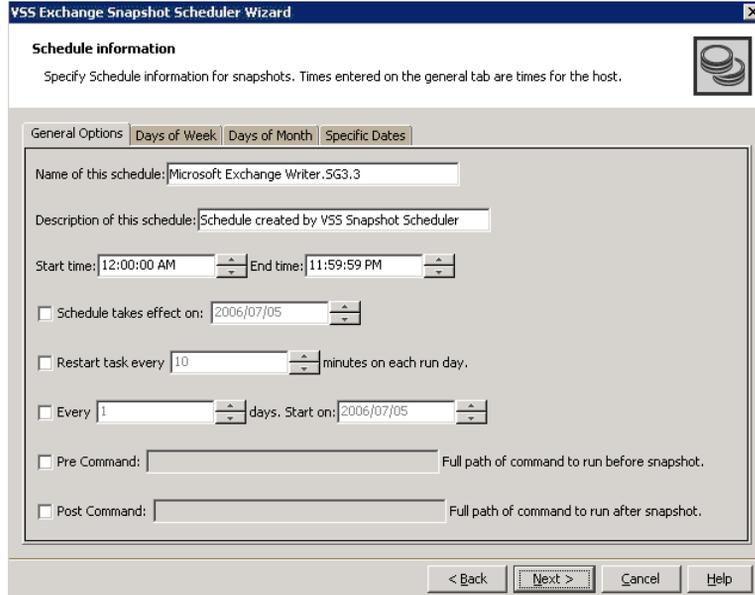
Plex

Optionally, click a plex and select a new choice from the drop-down menu.

- 8 Optionally, in the Synchronized Snapshot panel (VVR only), select the secondary hosts for which you want to create synchronized snapshots. Either double-click on the host name or click the **Add** option to move the host into the Selected Secondary Hosts pane. To select all the available hosts, click the **Add All** option. The VSS wizard creates synchronized snapshots on all the selected secondary hosts. This panel is displayed only in an environment using Veritas Volume Replicator (VVR). Otherwise, you will be directly taken to the Schedule Information panel.

See *Veritas Volume Replicator Administrator's Guide*.

- 9 In the Schedule Information panel, on the General Options tab, specify the following:



- | | |
|------------------------------|--|
| Name of this schedule | Enter a unique name for the snapshot set schedule.
This name identifies the snapshot schedule if you later want to view information about the snapshot status. A default name consists of the VSS writer name, the component name and a numbered suffix that increments with each schedule. |
| Description of this schedule | Optionally, enter a description to help you identify the schedule when you view information about the snapshot status |
| Start Time | The time of the day to begin taking snapshots. |
| End Time | The time of day to end taking snapshots.
If a snapshot is in progress it is completed but a new one is not started after the end time. |
| Schedule takes effect on | The date on which the specified schedule takes effect. The default is the current date. |

Restart task every	<p>The interval between snapshots, in minutes.</p> <p>For example, if the interval is 360 minutes and you schedule a snapshot start time of 12 P.M. and an end time of 7 P.M, the snapshot occurs twice.</p>
Every	<p>Enable the Every option to have the snapshot schedule continue to occur. Otherwise the schedule applies only for one day.</p> <p>Specify the number of days before restarting the snapshot schedule.</p> <p>For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.</p>
Start On	<p>If you enable the Every option, specify the starting date.</p>
Pre Command	<p>Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.</p> <p>Note: Precommands which launch windows or any other GUI related entities are not allowed in the Scheduler.</p>
Post Command	<p>Optionally, specify the full path of a command script to run after the snapshot is complete.</p> <p>Note: Postcommands which launch windows or any other GUI related entities are not allowed in the Scheduler.</p>

10 To specify run days for the schedule, make selections on the following tabs:

Days of Week	<p>Select one or more days on one or more weeks of the month.</p> <p>You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.</p>
Days of Month	<p>Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.</p>

Specific Dates

Select one or more specific dates to include in or to exclude from the schedule.

Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.

If two schedules overlap for the same snapshot set, only one snapshot is taken. For example, if you select every Thursday plus the last day of the month, and the last day of the month occurs on Thursday, only one snapshot is taken on Thursday.

11 Click **Next**.

12 Review the snapshot set and schedule details and click **Finish**.

Displaying the status of the scheduled VSS Exchange snapshot

If a scheduled snapshot fails for some reason, the scheduler process will attempt to rerun it. You may want to verify that scheduled snapshots completed successfully. From the VEA console, you can view snapshot results.

To view a scheduled snapshot status

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node and the Storage Agent node.
- 3 Click **Scheduled Tasks** to view all the applications that have schedules.
- 4 Select the application for which you scheduled the snapshot. The scheduled snapshots are listed in the pane on the right.
If you have just configured the schedules and they are not yet displayed, right-click the Storage Agent node and click **Refresh** to update the display.
- 5 Choose one of the following:
 - To view the status of all scheduled jobs, right-click the selected application and click **All Job History**.
 - To view the status of a particular schedule, right-click the snapshot schedule name and click **Job History**.
- 6 In the Job History dialog box, view the schedule information.
You can sort listed schedules by clicking the column headings. The Status column shows if the snapshot completed successfully.

Deleting a schedule for a VSS Exchange snapshot

Note: You cannot modify a schedule that has expired.

You can also delete (but not modify) a schedule from the VEA console.

Note: The VEA can delete snapshot schedules only; it does not delete mirror preparation scheduled with the Quick Recovery Configuration Wizard. In addition, deleting a snapshot schedule using the VEA does not update template settings created with the Quick Recovery Configuration Wizard.

To delete a schedule from the VEA

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the **System** node and **StorageAgent** node. Select and click to expand the **Scheduled Tasks > Exchange** node.
The scheduled snapshots are listed on the right pane.
- 3 Right-click the name of the snapshot schedule and select **Delete Schedule**.

Using the VSS Restore wizard

SFW provides recovery support for an Exchange storage group or a select database within a storage group. Using the VSS Restore wizard, the snapshots created with the VSS Snapshot wizard can be used for a point-in-time recovery of the storage group or a roll-forward recovery to the point of failure of either the storage group or an individual database in the storage group.

The point-in-time recovery restores the data to the time that the snapshot set was last refreshed—that is, it restores all the data that was recorded in the snapshot.

The point-of-failure recovery restores the old image of the data volumes only and then replays the logs to accomplish a roll-forward recovery, provided that the log volume is intact.

Note: After completing a point of failure (POF) recovery of a single database, Symantec recommends using the VSS Snapback wizard to reattach and resynchronize the other databases in the storage group and to use the VSS Snapshot wizard to create a new snapshot set.

For Exchange 2007, there is also an option to restore to a recovery storage group (RSG) rather than to the production store.

Note: COW snapshots are not supported when restoring to a recovery storage group (RSG).

Restoring the snapshot set

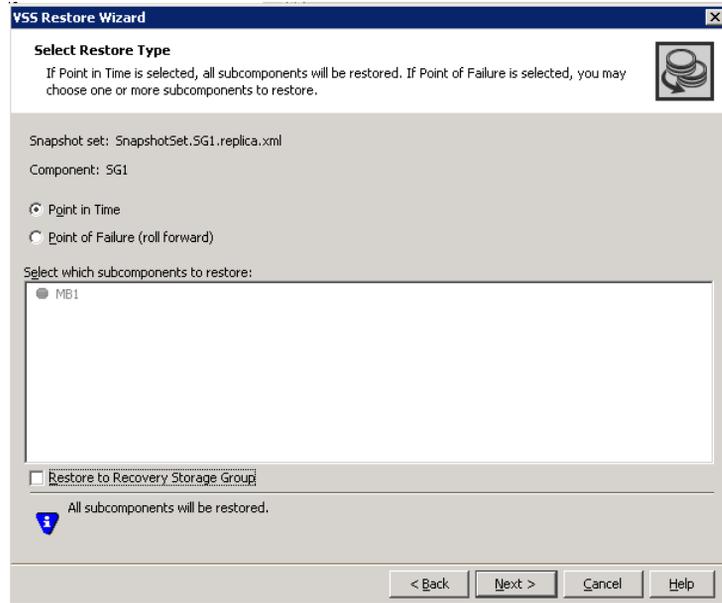
To restore to the point in time of the snapshot set

- 1 Close the database application GUI and all Explorer windows, applications, consoles (except the VEA console), or third-party system management tools that may be accessing the volumes.
- 2 From the VEA console, navigate to the system where the production volumes and snapshot set are located.
- 3 Expand the system icon and the **Applications** node.
- 4 Right-click **Exchange** and click **VSS Restore**.
- 5 Review the Welcome page and click **Next**.
- 6 Select the snapshot set you wish to restore and click **Next**.

The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs

volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**.

- 7 In the Select Restore Type panel, select Point in Time. Point in Time restores to the point in time that the snapshot set was created or refreshed based on the information contained in the metadata file.



Click **Next**

- 8 Verify that the restore specifications are correct and click **Finish**.
- 9 Mount all the databases (stores) in the Exchange storage group.
- 10 To refresh the snapshot set use the VSS Exchange Snapshot Wizard or `vxsnap create` command to create a new snapshot set of all the volumes in the storage group.

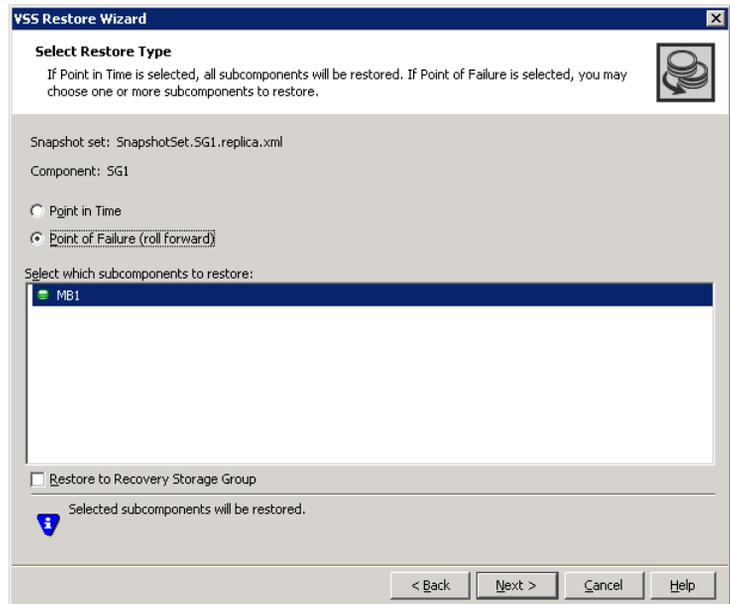
To perform a roll-forward recovery of one or more databases to the point of failure

- 1 Dismount all the databases (stores) in the Exchange storage group:
 - For Exchange 2003, you can use the Exchange System Manager.
 - For Exchange 2007, you can use the Exchange Management Console.
- 1 Close the database application GUI and all Explorer windows, applications, consoles (except the VEA console), or third-party system management tools that may be accessing the volumes.

- 2 From the VEA console, navigate to the system where the production volumes and snapshot set are located.
- 3 Expand the system icon and the **Applications** node.
- 4 Right-click **Exchange** and click **VSS Restore**.
- 5 Review the Welcome page and click **Next**.
- 6 Select the name of the metadata file for the snapshot set you wish to restore and click **Next**.

The XML metadata file contains all required information about the Exchange storage group, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by File Name or Creation Time.

- 7 In the Select Restore Type panel, select Point of Failure and select one or more subcomponents (databases). Do not select the transaction logs volume.



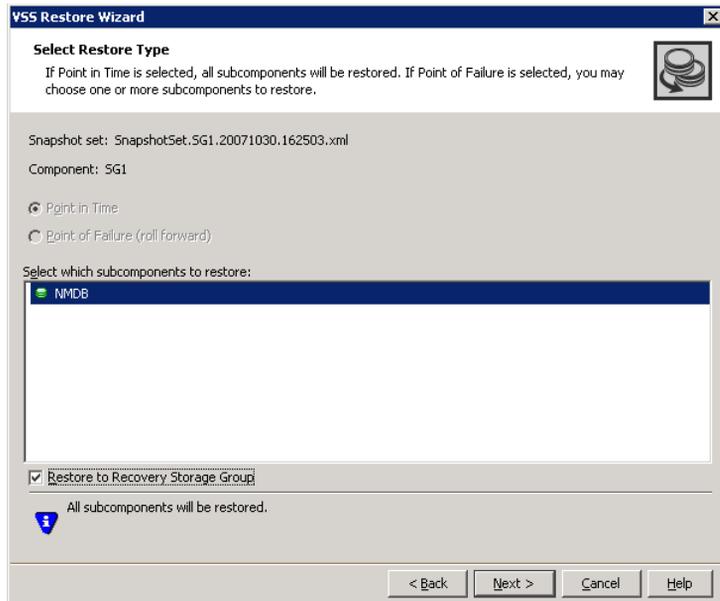
Click **Next**

- 8 Verify that the restore specifications are correct and click **Finish**.
- 9 Mount all databases (stores) in the Exchange storage group; the transaction logs will roll forward to the point of failure. This action can be observed in the Event Viewer Application log.
- 10 To refresh the snapshot set at this point, snapback any remaining database volumes and the transaction logs volume using either the VSS Snapback

wizard or the `vxsnap reattach` command. Then use the VSS Exchange Snapshot wizard or `vxsnap create` command to create a new snapshot set of the storage group.

To restore to a recovery storage group (Exchange 2007 only)

- 1 Close the database application GUI and all Explorer windows, applications, consoles (except the VEA console), or third-party system management tools that may be accessing the volumes.
- 2 From the VEA console, navigate to the system where the production volumes and snapshot set are located.
- 3 Expand the system icon and the **Applications** node.
- 4 Right-click **Exchange** and click **VSS Restore**.
- 5 Review the Welcome page and click **Next**.
- 6 Select the snapshot set you wish to restore and click **Next**.
The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**.
- 7 In the Select Restore Type panel, select Restore to Recovery Storage Group and select one or more subcomponents.



Click **Next**

- 8 Verify that the restore specifications are correct and click **Finish**.
- 9 Mount all the databases (stores) in the Exchange storage group.

Refreshing the snapshot set

The VSS Refresh command available in the context menu of the VSS Writer object refreshes the VEA display of the VSS Writer and components. It does not refresh the snapshot set.

To refresh the snapshot set, either use the VSS Snapback Wizard for a one-time refresh or set up a schedule using the VSS Snapshot Scheduler Wizard.

Supporting replication in Exchange 2007

SFW provides support for snapshots when the Local Continuous Replication (LCR) and Cluster Continuous Replication (CCR) features of Exchange 2007 are enabled.

The following topics describe various notes about support of replication in Exchange 2007.

VEA GUI

If replication for Exchange 2007 is enabled, then the display of the Microsoft Exchange Replication Service instance of the Microsoft Exchange Writer is enabled and displayed in the VEA GUI. It appears as the Microsoft Exchange Writer Replica and is displayed in the tree view of the VEA subordinate to the VSS Writers node.

Right-clicking the Microsoft Exchange Writer Replica node displays a context menu that shows VSS Snapshot, VSS Snapback, and VSS Refresh selections. Restoring the replica with the VSS Restore operation and the Schedule VSS Snapshot operation for the replica are not supported.

Note: The Prepare command is required before using VSS Snapshot.

Microsoft Clustering environment

In a Microsoft Clustering environment, you have to manually set the dependency of the Microsoft Exchange database instance to the Volume Manager Disk group resource so that it fails over in the correct sequence.

vxsnap CLI command

SFW provides a `vxsnap` CLI command option to take a snapshot of a Microsoft Exchange Writer Replica (Microsoft Exchange Replication Service instance of

the Microsoft Exchange writer) or of a Microsoft Exchange Writer (Microsoft Exchange Service instance of the Microsoft Exchange writer).

In the command, you can specify the replica store writer to take the snapshot of the replica or the active store writer to take the snapshot of the active store. If the replica store writer or the active store writer is not specified, then "Microsoft Exchange Writer" is used as a default.

For example:

```
vxsnap -x snapdata.xml create writer="Microsoft Exchange  
Writer Replica" component=SG1 backupType=COPY -E -O
```

specifies that the VSS Writer, Microsoft Exchange Writer Replica, is used to take a snapshot of the replica.

Note: The Prepare operation must be completed on the volumes that contain the replica before taking a snapshot of a replica. This can be done using the VEA GUI or the `vxsnap prepare` CLI command. When using the CLI, the `vxsnap prepare` command must specify the Microsoft Exchange Writer Replica.

For example:

```
vxsnap prepare component=SG1/writer="Microsoft Exchange  
Writer Replica" source=L:/harddisk=harddisk2
```

See "[vxsnap](#)" on page 407.

Using a Snapshot of a Replica for Database Recovery

A snapshot of a replica can be used to restore an Exchange database to the point of failure (POF) or be used to restore a complete Exchange storage group to a point in time (PIT).

Taking a snapshot of a replica can be done with the VEA GUI by using the VSS snapshot wizard or with the `vxsnap` CLI command. Taking a snapshot of a replica automatically takes a snapshot of all the volumes that the replica uses.

To restore the database from a snapshot of a replica, you must first manually perform a "Restore-StorageGroupCopy" on the storage group, and then perform the restore on the active writer. (The restore operation on the replica store writer is not supported.)

Originally, a manual dismount of the database was required before the restore operation. Now SFW performs the dismount of the database automatically as a part of the restore operation.

Note: In a VCS environment, the database is automatically dismounted and the database is set for overwrite by restore as a part of the restore operation. However in a Microsoft Clustering environment, a manual dismount of the database and manually setting the database for overwrite by restore are both required.

Note: When SFW fails to automatically dismount the database during a restore operation, the restore operation fails. The restore operation can be performed again after manually dismounting the databases and manually setting the databases for overwrite by restore. If LCR is enabled in a non-Microsoft Clustering environment or if CCR is enabled in a Microsoft Clustering environment, suspend LCR/CCR. Then repeat the restore operation. If you suspended LCR/CCR, re-enable it after the restore operation.

To perform the restore on the active writer, use the Exchange Management shell to execute the following cmdlets:

■ Dismount Database cmdlet

```
dismount-Database -Identity <DatabaseIdParameter>  
[-DomainController <Fqdn>]
```

■ RestoreStorageGroupCopy cmdlet

```
Restore-StorageGroupCopy  
-Identity:<Server>\<StorageGroupName>  
-ReplaceLocations
```

Additional considerations when running the RestoreStorageGroupCopy cmdlet:

- The LCR is automatically disabled when running the Restore-StorageGroupCopy cmdlet
- If a schedule for snapshots exists for the active store, running the RestoreStorageGroupCopy cmdlet makes the schedule invalid. The schedule becomes invalid because it no longer has updated volume/plex information to take the snapshot. In this situation, the user must delete the invalid schedule before performing the restore operation.

For more information about the Exchange Management shell and cmdlets, refer to the Microsoft Exchange 2007 product information at

<http://www.microsoft.com>.

After completing the "Restore-StorageGroupCopy" on the storage group, you would use the VSS restore wizard or the vxsnap restore command to complete the recovery operation.

Note: Although SFW allows you to restore the database from a snapshot, restoring just the database log files is not supported.

An example of a PIT recovery procedure from a snapshot of a replica of an Exchange storage group, SG1, that contains two databases, DB1 and DB2, on an Exchange server, TestExch, would be as follows:

- 1 Run Dismount Database cmdlet on DB1 and DB2 databases.
`Dismount-database -Identity TestExch\SG1\DB1`
`Dismount-database -Identity TestExch\SG1\DB2`
- 2 Run RestoreStorageGroupCopy cmdlet on SG1 storage group.
`Restore-StorageGroupCopy -Identity TestExch\SG1`
`-ReplaceLocations`
- 3 Run Mount Database cmdlet on DB1 and DB2 databases.
`Mount-database -Identity TestExch\SG1\DB1`
`Mount-database -Identity TestExch\SG1\DB2`
- 4 Perform refresh.
`vxsnap refresh`
- 5 Perform VSS restore operation using snapshot of replica.
`vxsnap -x snapdata.xml restore RestoreType=PIT`
`writer="Microsoft Exchange Writer"`

Note: For this example, assume that the snapshot of the replica was performed with

```
vxsnap -x snapdata.xml create writer="Microsoft  
Exchange Writer Replica" component=SG1 backupType=COPY  
-E -O
```

For a Microsoft Clustering environment, there are additional considerations when restoring the database.

- After performing the refresh operation, the user must manually dismount the databases before performing the restore operation.
- If CCR is enabled, then the user must disable the circular logging feature and suspend CCR before restoring the database.

Using the VSS snapshot wizards with Microsoft SharePoint

SFW provides support for taking snapshots of Microsoft SharePoint components.

FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with a SharePoint component without taking the component's databases offline. The VSS Snapshot wizard uses VSS to take snapshots of components. The VSS process allows the component's databases to be quiesced before the snapshot operation and reactivates them immediately after. The quiescing at the component level allows for Microsoft supported and guaranteed persistent snapshots of the data. A snapshot of a component can be reattached and resynchronized to match the current state of the component with the VSS Snapback wizard.

Note: When creating SharePoint components, ensure that the names of the components are unique. Performing operations on components with names that are not unique may cause unpredictable results.

Using the VSS SharePoint Snapshot wizard

Creating a snapshot is a two-step process. The first step, prepare the volume for snapshot, creates snapshot mirrors attached to all the original volumes of the specified component. Depending on the size and number of volumes, the process of synchronizing the new snapshot mirrors with the original production volumes can take a long time. The second step uses the VSS SharePoint Snapshot wizard to create the snapshot set by detaching the snapshot mirrors from the original volumes and creating separate on-host snapshot volumes as well as an XML file to store the component and snapshot volume metadata. The VSS SharePoint Snapshot wizard integrates with VSS to quiesce the component and then while the component is online and without disrupting processing. Once a snapshot set has been created, it can be reattached and resynchronized with the VSS SharePoint Snapback wizard.

Note: To enable the restore of a single SharePoint component from a snapshot, components should be configured to reside on individual volumes so that a snapshot of a volume contains a single component.

Note: After performing operations for snapshots, the VEA GUI may not be updated to reflect the results of the operation. Use the VSS Refresh command to update the VEA GUI.

Preparing the snapshot set

The following is the procedure to prepare a snapshot.

To prepare the snapshot set

- 1 From the VEA console, navigate to the SharePoint sever.
- 2 Expand the system node, the Storage Agent node, and the Applications node.
- 3 Expand the SharePoint node.
- 4 Right-click the SharePoint component and click SharePoint Prepare.
- 5 In the wizard, review the Welcome page and click Next.
- 6 Select the component to prepare for the snapshot and click Next.
- 7 Review the components for the prepare operation and click Next.
- 8 Review the specifications for the prepare operation and click Finish.

Creating the snapshot set

The following is the procedure to create a snapshot set.

To create the snapshot set

- 1 From the VEA console, navigate to the SharePoint sever.
- 2 Expand the system node, the Storage Agent node, and the Applications node.
- 3 Expand the SharePoint node.
- 4 Right-click the SharePoint component and click SharePoint Snapshot.
- 5 In the wizard, review the Welcome page and click Next.
- 6 Specify the snapshot set parameters and then click Next.

Select Component for snapshot set Select the component for the snapshot set

Directory	<p>The wizard creates the snapshot set metadata XML file. The XMLmetadata file is stored by default in the directory shown on the screen.</p> <p>There are two ways to change the XML file location.</p> <p>First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named redirect.txt. This text file should contain a single text line specifying the full path to the location of the XML file, for example,</p> <p>G:\BackupSets. Save the redirect.txt file in the default directory C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML.</p> <p>If SFW/SFWHA is installed on the D drive, then the path will be the same as above, but on the D drive.</p>
Snapshot set	<p>Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, date, and time.</p>
Select snapshot type	<p>Select the snapshot type.</p> <p>You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a SharePoint component. However, if you want to replay logs in as a part of restoring a component, a Full backup needs to have been created earlier. When replaying logs, you can replay from the time of the last Full backup. A Copy backup does not affect this sequence of log replay and therefore is often used as an "out of band" copy for purposes such as testing or data mining.</p>

- 7 Review the components for the snapshot operation and click Next.
- 8 Review the specifications of the snapshot set and click Finish.

Note: When taking a snapshot of the SharePoint Osearch component, ensure to include the index component in the snapshot operation.

Using the VSS SharePoint Snapshot Scheduler wizard

You can use the VSS SharePoint Snapshot Scheduler wizard to add a snapshot schedule.

The scheduling capability automates the process of refreshing snapshots sets. At the time scheduled for the snapshot, the snapshot volumes are automatically reattached, resynchronized, and then split again. Once configured and applied, the schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background. In a clustered server environment, ensure that the scheduler service is configured on each node with domain administrator privileges so that any node in the cluster can run the schedule after a failover.

Note: Information about the operations performed by the schedule can be found by expanding the nodes under the Scheduled Tasks node in the tree-view of the GUI. Expand the appropriate application node to locate the schedules for that application. Right-click the node and select JobHistory to view information about the operations performed by the schedule.

The VSS SharePoint Snapshot Scheduler wizard does not prepare the snapshot mirror. Prepare the snapshot mirror with the SharePoint Prepare command before running the VSS SharePoint Snapshot Scheduler wizard.

To schedule a snapshot for a selected component

- 1 From the VEA console, navigate to the SharePoint server.
- 2 Expand the system node, the Storage Agent node, and the Applications node.
- 3 Expand the SharePoint node.
- 4 Right-click the SharePoint component and click SharePoint Scheduler.
- 5 In the wizard, review the Welcome page and click Next.
- 6 Specify the snapshot set parameters and then click Next.

Select the component for the snapshot set operation

Directory The wizard creates the snapshot set metadata XML file. The XMLmetadata file is stored by default in the directory shown on the screen.

There are two ways to change the XML file location.

First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named redirect.txt. This text file should contain a single text line specifying the full path to the location of the XML file, for example,

G:\BackupSets. Save the redirect.txt file in the default directory C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML.

If SFW/SFWHA is installed on the D drive, then the path will be the same as above, but on the D drive.

Snapshot set Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, date, and time.

Select snapshot type Select the snapshot type.

You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a SharePoint component. However, if you want to replay logs in as a part of restoring a component, a Full backup needs to have been created earlier. When replaying logs, you can replay from the time of the last Full backup. A Copy backup does not affect this sequence of log replay and therefore is often used as an "out of band" copy for purposes such as testing or data mining.

- 7 Review the components for the snapshot operation and click Next.
- 8 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	<p>Enter a unique name for the snapshot set schedule.</p> <p>This name identifies the snapshot schedule if you later want to view information about the snapshot status. A default name consists of the VSS writer name, the component name and a numbered suffix that increments with each schedule.</p>
Description of this schedule	<p>Optionally, enter a description to help you identify the schedule when you view information about the snapshot status.</p>
Start Time	<p>The time of the day to begin taking snapshots.</p>
End Time	<p>The time of day to end taking snapshots.</p> <p>If a snapshot is in progress it is completed but a new one is not started after the end time.</p>
Schedule takes effect on	<p>The date on which the specified schedule takes effect. The default is the current date.</p>
Restart task every	<p>The interval between snapshots, in minutes.</p> <p>For example, if the interval is 360 minutes and you schedule a snapshot start time of 12 P.M. and an end time of 7 P.M, the snapshot occurs twice. If no interval is specified the snapshot occurs once.</p>
Every	<p>Enable the Every option to have the snapshot schedule continue to occur. Otherwise the schedule applies only for one day.</p> <p>Specify the number of days before restarting the snapshot schedule.</p> <p>For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.</p>
Start On	<p>If you enable the Every option, specify the starting date.</p>
Pre Command	<p>Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.</p>
Post Command	<p>Optionally, specify the full path of a command script to run after the snapshot is complete.</p>

9 To specify run days for the schedule, make selections on the following tabs:

Days of Week	<p>Select one or more days on one or more weeks of the month.</p> <p>You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.</p>
Days of Month	<p>Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.</p>
Specific Dates	<p>Select one or more specific dates to include in or to exclude from the schedule.</p> <p>Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.</p>

If two schedules overlap for the same snapshot set, only one snapshot is taken. For example, if you select every Thursday plus the last day of the month, and the last day of the month occurs on Thursday, only one snapshot is taken on Thursday.

10 Click Next.

11 Review the snapshot set and schedule details and click Finish.

Using the VSS SharePoint Snapback wizard

The VSS SharePoint Snapback wizard reattaches and resynchronizes an existing snapshot set so that it matches the current state of its original SharePoint component. The wizard is available in the context menu of the VSS Writer object.

The following is the procedure to resynchronize (snapback) a snapshot set.

To snapback a snapshot set

- 1** Close the database application GUI and all Explorer windows, applications, consoles (except the VEA console), or third-party system management tools that may be accessing the snapshot set.

- 2 From the VEA console URL bar, select the <host name> which is the system where the production volumes and snapshot mirrors are located, as the active host.
- 3 Expand the system node, the Storage Agent node, and the Applications node.
- 4 Right-click the SharePoint Server node and click SharePoint Snapback.
- 5 Review the Welcome page and click Next.
- 6 Select the snapshot set you want to snapback and click Next.
TheXMLmetadata file contains all required information needed to snapback the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by File Name or CreationTime. This file is deleted after the snapback operation has completed successfully.
- 7 Verify that the snapback specifications are correct and click Finish.

Using the VSS SharePoint Restore wizard

SFW provides recovery support for SharePoint components. Using the VSS SharePoint Restore wizard, the snapshots created with the VSS SharePoint Snapshot wizard can be used to restore the components without logs.

Restoring the component without logs (recovery and no log replay) restores the database and the transaction log volumes. No other logs are applied. This leaves the component in an online state.

Note: After restoring an Osearch index and database, the Office SharePoint Server Search service needs to be restarted. Open the service manager and locate/restart Office SharePoint Server Search. You also need to do an incremental crawl to keep the index and database up to date.

Restoring the component database with recovery without logs

The following is the procedure to restore the component database with recovery without logs.

To recover a component database without log replay

- 1 Close the SQL GUI and all Explorer windows, applications, consoles, or third-party system management tools that may be accessing the volumes. It is also recommended to bring the database offline.

- 2 Using the GUI, navigate to the system where the SharePoint component volumes are located.
- 3 Expand the system node, the Storage Agent node, Applications node, and the SharePoint node.
- 4 Right-click the SharePoint Server and click SharePoint Restore.
- 5 Review the Welcome page and click Next.
- 6 Select the snapshot set XML metadata file to be used for this operation and click Next.
The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by File Name or Creation Time.
- 7 On the Select Restore Type panel, click Recovery. and select a component. If one or more original volumes are missing, you can check the checkbox for a Recovery with missing original volumes.
- 8 You may receive a message "Some volumes in this component have open handles. Do you want to override these handles and do this restore? Click Yes to proceed." Click No, close any open handles and retry the command.
- 9 Verify the restore specifications and click Finish.
The database is restored to the time the snapshot set was created or last refreshed. If you took it offline earlier, bring it back online.
- 10 The restore operation leaves the snapshot volumes snapped back to the production volumes. To ensure that another split-mirror snapshot set is immediately available, use the VSS Snapshot Wizard to create a new snapshot of all the volumes in the SharePoint component.

Restoring the database with no recovery

The following is the procedure to restore the component database with the No Recovery option.

To restore using the No Recovery option

- 1 Ensure that you have backed up the transaction logs within SQL Server using the "overwrite existing media" option to create uniquely-named backup files.
- 2 Close the SQL GUI and all Explorer windows, applications, consoles, or third-party system management tools that may be accessing the database volumes. It is also recommended to bring the database offline.

- 3 From the VEA console, navigate to the system where the database volumes are located.
- 4 Expand the system node, the Storage Agent node, the Applications node and the SharePoint node.
- 5 Right-click the SharePoint Server and click SharePoint Restore.
- 6 Review the Welcome page and click Next.
- 7 Select the snapshot set XML metadata file to be used for this operation and click Next.
The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by File Name or Creation Time.
- 8 On the Select Restore Type panel, click NoRecovery and select a component.
- 9 You may receive a message "Some volumes in this component have open handles. Do you want to override these handles and do this restore? Click Yes to proceed." Click No, close any open handles and retry the command.
- 10 Verify the restore specifications and click Finish.
- 11 Use your preferred method to manually restore the backup transaction logs to the desired point in time and then bring the database back online.
- 12 The restore operation leaves the snapshot volumes snapped back to the production volumes. To ensure that another split-mirror snapshot set is immediately available, use the VSS Snapshot Wizard to create a new snapshot of all the volumes in the SharePoint component.

Using the VSS snapshot wizards with Enterprise Vault

SFW provides support for taking snapshots of Enterprise Vault components. FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with a Enterprise Vault component without taking the component's databases offline. The Enterprise Vault Snapshot wizard uses VSS to take snapshots of components. The VSS process allows the component's databases to be quiesced before the snapshot operation and reactivates them immediately after. The quiescing at the component level allows for supported and guaranteed persistent snapshots of the data. A snapshot of a component can be reattached and resynchronized to match the current state of the component with the Enterprise Vault Snapback wizard. SFW also provides recovery support for Enterprise Vault components. Using the Enterprise Vault Restore wizard, the snapshots taken with the Enterprise Vault Snapshot wizard can be used for a recovery of the component. The following describes the Enterprise Vault components that SFW supports

Directory database	The Enterprise Vault Directory database holds configuration information for each site in the Directory (EnterpriseVaultDirectory).
Monitoring database	Enterprise Vault has a Monitoring agent on each Enterprise Vault server. The Monitoring agents collect monitoring data at scheduled intervals, usually every few minutes, and store it in the Enterprise Vault Monitoring database. If multiple Enterprise Vault sites share a Directory database, then they must also share a Monitoring database (EnterpriseVaultMonitoring).
Reporting database	The Reporting database stores reporting information that is generated from the collected Monitoring data. There is one Reporting database named EnterpriseVaultFSAReporting corresponding to the Directory Database.
Auditing database	The Auditing database stores audit information. There is one Auditing database named EnterpriseVaultAudit corresponding to the Directory database

Site	A site comprises one or more Enterprise Vault servers running one or more Enterprise Vault services and tasks to archive items from specified targets. A site also contains a collection of vault stores, archiving policies that define how and when items are to be archived, and Retention Categories that define how long items are to be stored before being deleted.
Index	The Indexing Service indexes items as they are archived. There is one Index for each archive
Vault Store Group	A Vault Store Group (VSG) is a collection of Vault Stores that are configured to share data.
Fingerprintdatabase	A Vault Store Group contains one or more Fingerprint Catalog databases (FDB) to hold a shared item's metadata.
Vault Store	Enterprise Vault organizes archives in entities called Vault Stores. Vault Stores contain one or more Enterprise Vault Partitions. A Partition can reside on any of the supported storage media.
VaultStoredatabase	The Vault StoreSQLdatabases contain information about every archive operation processed for all archives within a Vault Store. Both the Vault Store's database and the Vault Store's files must be complete to be able to retrieve messages from an archive.
Open Partition	In each Vault Store, there can be only one Open Partition. This is the Partition in which Enterprise Vault archives data. An Open Partition is the current active Partition in which Enterprise Vault data is being written.
Ready Partition	Each Vault Store can have a number of Ready Partitions. A Ready Partition is the next available partition to be used.
Closed Partition	Each Vault Store can have any number of Closed Vault Store Partitions. Enterprise Vault does not archive content into Partitions that are closed.

Using the Enterprise Vault Snapshot wizard

Creating a snapshot is a two-step process. The first step, prepare the volume for snapshot, creates snapshot mirrors attached to all the original volumes of the specified component. Depending on the size and number of volumes, the process of synchronizing the new snapshot mirrors with the original production

volumes can take a long time. The second step uses the Enterprise Vault Snapshot wizard to create the snapshot set by detaching the snapshot mirrors from the original volumes and creating separate on-host snapshot volumes as well as an XML file to store the component and snapshot volume metadata. The Enterprise Vault Snapshot wizard integrates with VSS to quiesce the component and then simultaneously snapshot the volumes in the component. This snapshot is done while the component is online and without disrupting processing. Once a snapshotset has been created, it can be reattached and resynchronized with the Enterprise Vault Snapback wizard.

Note: After performing operations for snapshots, the VEA GUI may not be updated to reflect the results of the operation. Use the VSS Refresh command to update the VEA GUI.

Preparing for Enterprise Vault snapshots

After completing Enterprise Vault installation tasks, and before taking Enterprise Vault snapshots, you must invoke the Enterprise Vault Management Shell to register PowerShell snap-ins, set the execution policy and then configure the Veritas Scheduler Service. The Enterprise Vault Management Shell can be invoked either prior to or after performing the Prepare operation for snapshot mirrors.

Setting the execution policy with the Enterprise Vault Management Shell

You must invoke the Enterprise Vault Management Shell to set the execution policy to unrestricted.

You need to invoke the Enterprise Vault Management Shell only once on a host where you will be performing the snapshot command. As a best practice, it is recommended that you invoke the shell once on all the hosts in the Enterprise Vault configuration.

To set the execution policy with the Enterprise Vault Management Shell

1 Click Start>AllPrograms>EnterpriseVault>EnterpriseVaultManagement Shell

2 Run the following command to set the execution policy.

```
set-executionpolicy unrestricted
```

Caution: Setting the execution policy to unrestricted may be a potential security risk. This setting allows any (untrusted) script to be invoked.

Configuring the Veritas Scheduler Service

Configure the Veritas Scheduler Service with administrative privileges on all nodes where you have configured the Enterprise Vault Server.

Perform the following to configure the service.

To configure the Veritas Scheduler Service

- 1 Launch the Veritas Scheduler Service Administrative tool by clicking Start>All Programs>Administrative Tools>Services>Veritas Scheduler Service.
- 2 From the Veritas Scheduler Service Properties dialog, perform the following settings:
 - Select Log On.
 - Disable the Local System account option.
 - Enable the This account option.
 - Ensure that the user name is set up with administrative privileges.
- 3 Click OK to complete the configuration.

Preparing an Enterprise Vault snapshot mirror

Preparing Enterprise Vault (EV) for a snapshot involves preparing all the dependent components of Enterprise Vault. The snapshot prepare operation can be performed at the Enterprise Vault farm, site, VaultStore Group, VaultStore, or the component level. When you right-click an Enterprise Vault object and select the Enterprise Vault Prepare operation from the menu option, related Enterprise Vault sites, components, etc. within (subordinate to) the Enterprise Vault object are prepared for snapshot mirrors.

Note: You can have only one snapshot volume on a disk for particular production volume.

Note: If a volume is used for more than one component, it will be snapshot prepared only once when all the components are specified in a vxsnap prepare CLI command or in the Enterprise Vault Prepare wizard. If several components share the same volume and these components are each prepared separately for snapshot mirrors, then the volume will be prepared many times (once for every component).

The snapshot mirrors remain attached to the original volumes and continue to be updated until you use the Enterprise Vault Snapshot Wizard, the vxsnap

create command, or the Enterprise Vault Snapshot Scheduler Wizard to create the snapshot set.

Please note the following:

- When an Enterprise Vault site is Prepared, the Directory database is also Prepared implicitly by the system along with the Enterprise Vault site components.
- When a Vaultstore database of a VaultStore is prepared, the Open Partition of that VaultStore is also prepared implicitly by the system.
- When an Open Partition of a VaultStore is prepared, the VaultStore database of that VaultStore is also prepared implicitly by the system.
- Upon completion of the operation, the status (success/failure) of the selected components is recorded in a log, %VMPATH%\logs\EVStatus.log. The log contains information about the success or failure of the operation for the components. In the event that the prepare of a volume for a component fails, the operation continues to prepare the remaining volumes of the component and any other requested components. If the operation succeeds for all the volumes of a component, then the status of the component is logged as a success. If the operation fails for any one of the volumes of the component, then the status of the component is logged as a failure along with the cause of failure.

You can also use the vxsnap prepare CLI command to prepare volumes as snapshot mirrors.

To prepare an Enterprise Vault snapshot mirror

- 1 On the VEA console, navigate to the Storage Agent in the tree-view and expand the Enterprise Vault nodes, under Applications.
- 2 Right-click the desired Enterprise Vault node and click Enterprise Vault Prepare on the context menu.
- 3 In the wizard, review the Welcome page and click Next.
- 4 In the Select Component dialog, select the Enterprise Vault components (sites, VaultStoreGroups, VaultStores, or partitions) that you want to snapshot prepare. Review the specifications for the prepare operation and click Finish.

Creating the snapshot set

SFW provides support for creating snapshots for the Enterprise Vault (EV) farm, sites, VaultStore Groups, VaultStores, and components. The Enterprise Vault Snapshot Wizard integrates with Microsoft Volume Shadow Copy Service (VSS) to allow you to create snapshots of all volumes associated with Enterprise Vault components and volumes without taking the databases offline and disrupting

database operations. It also allows the Enterprise Vault Powershell cmdlet to put Enterprise Vault into backup mode. Backup mode ensures that there are no write operations involving any Enterprise Vault components and helps avoid disruption.

The resulting snapshot set provides a complete picture of the database at a point in time the snapshot was taken. You can take a snapshot with the Enterprise Vault Snapshot Wizard or the vxsnap create CLI command.

Note: The Enterprise Vault Snapshot Wizard and vxsnap utility can be invoked from any node that has the Directory service running.

The snapshot operation can be performed at the Enterprise Vault farm, site, VaultStore Group, VaultStore, or component levels. When you right-click an Enterprise Vault object and click Enterprise Vault Snapshot from the context menu, the Enterprise Vault objects and components within (subordinate to) the selected Enterprise Vault object are all included in the snapshot. You can also add more Enterprise Vault objects from the objects shown in the Enterprise Vault Snapshot wizard.

Please note the following:

- When an Enterprise Vault site is snapshotted, the Directory database is also snapshotted implicitly by the system along with the Enterprise Vault site components.
- When a Vaultstore database is snapshotted, the Open Partition of that VaultStore is also snapshotted implicitly by the system.
- When an Open Partition of a VaultStore is snapshotted, the Vaultstore database of that VaultStore is also snapshotted implicitly by the system.
- Upon completion of the operation, the status (success/failure) of the selected components is recorded in a log, %VMPATH%\logs\EVStatus.log. The log contains information about the success or failure of the operation for the components. In the event that the snapshot of a volume for a component fails, the operation does not snapshot the remaining volumes of the component nor any other requested components that are remaining. If the operation succeeds for all the volumes of a component, then the status of the component is logged as SUCCESS. If the operation fails for any one of the volumes of the component, then the status of all the components of that EnterpriseVault server is logged as FAILED along with the cause of the failure. The status of all components that had been already snapshotted earlier before the failed component are logged as SUCCESS, and the status of the remaining components that had not been snapshotted are logged as SKIPPED.

Review the following before proceeding with the snapshot operation for Enterprise Vault:

- Ensure that the execution policy is set to unrestricted. You can use the Enterprise Vault Management Shell to set the execution policy.
- Ensure that the Veritas Scheduler Service is configured for all Enterprise Vault servers in the Enterprise Vault configuration.
- Ensure that the component volumes or database and partition volumes have been snapshot prepared as snapshot mirrors.

The following is the procedure to create a snapshot set.

To create the snapshot set

- 1 Using the VEA console, navigate to the Storage Agent node in the tree-view and expand the Enterprise Vault nodes under Applications.
- 2 Navigate to the desired Enterprise Vault node. Right-click the Enterprise Vault node and click Enterprise Vault Snapshot in the context menu.
- 3 In the wizard, review the Welcome page and click Next.
- 4 Specify the snapshot set parameters and then click Next

Select component for snapshot operation Select the component for the snapshot set

Directory

The wizard creates the snapshot set metadata XML file. The XMLmetadata file is stored by default in the directory shown on the screen.

There are two ways to change the XML file location. First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named redirect.txt. This text file should contain a single text line specifying the full path to the location of the XML file, for example,

G:\BackupSets. Save the redirect.txt file in the default directory C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML.

If SFW/SFWHA is installed on the D drive, then the path will be the same as above, but on the D drive.

- Snapshot set** Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, date, and time. If multiple components are selected, "EV" is used in the default snapshot set name instead of the component name.
- Select snapshot type** Select the snapshot type.
- You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a Enterprise Vault component. However, if you want to replay logs in as a part of restoring a component, a Full backup needs to have been created earlier. When replaying logs, you can replay from the time of the last Full backup. A Copy backup does not affect this sequence of log replay and therefore is often used as an "out of band" copy for purposes such as testing or data mining.

- 5 Review the specifications of the snapshot set and click Finish.

Using the Enterprise Vault Snapback wizard

The Enterprise Vault Snapback Wizard reattaches and resynchronizes an existing snapshot set so that it matches the current set of its original database.

Note: Upon completion of the operation, the status (success/failure) of the selected components is recorded in a log, %VMPATH%\logs\EVStatus.log. The log contains information about the success or failure of the operation for the components. In the event that the reattach of a volume for a component fails, the operation continues to reattach the remaining volumes of the component and any other requested components. The components that successfully complete the operation are removed from the snapshot set. If the operation succeeds for all the volumes of a component, then the status of the component is logged as a success. If the operation fails for any one of the volumes of the component, then the status of the component is logged as a failure along with the cause of failure.

To snapback an Enterprise Vault snapshot set

- 1 Except for the VEA GUI, close all windows, applications, or third-party system management tools that may be accessing the snapshot set.

- 2 Using the VEA console, navigate to the Storage Agent node in the tree-view and expand the Enterprise Vault nodes under Applications.
- 3 Right-click the Enterprise Vault node and click Enterprise Vault Snapback in the context menu.
- 4 In the wizard, review the Welcome page and click Next
- 5 Select the snapshot set and specify the parameters and then click Next.

Directory	Specify the path of the directory where the snapshot set is located.
Snapshot Sets	The XML metadata file contains all required information needed to snapback the snapshot set, including the names of the database and transaction log volumes. Click the appropriate header to sort the list of available files by File Name or Creation Time. This file is deleted after the snapback operation has completed successfully.

- 6 On the Select Components page, select the components to be reattached or snapbacked. Click Next to continue.
- 7 Review the specifications of the snapback and click Finish.

Using the VSS Enterprise Vault Snapshot Scheduler wizard

Before you run the Enterprise Vault Snapshot Scheduler Wizard to schedule a snapshot set for a database, you must prepare a snapshot mirror for each of the volumes in the database.

You can then use the Enterprise Vault Snapshot Scheduler Wizard to schedule the initial snapshot set and to set up the schedule for keeping it refreshed.

The scheduling of snapshots can be done at the Enterprise Vault (EV) farm, sites, VaultStore Groups, Vault Stores, Partitions, or any component level. The Schedule Enterprise Vault Snapshot Wizard can be launched from any component of Enterprise Vault configuration.

When the scheduled snapshots occur, the snapshot mirrors are detached from the original volumes, creating separate on-host snapshot volumes as well as an XML file to store the snapshot volume metadata. The scheduled process integrates with VSS to quiesce the database and then simultaneously snapshot the volumes for Enterprise Vault components. This snapshot is done while the Enterprise Vault components are online and without disrupting the operations. It also allows the Enterprise Vault PowerShell cmdlet to put Enterprise Vault

into backup mode. Backup mode ensures that no writes happen on Enterprise Vault components.

To schedule a snapshot for a selected component

- 1 Using the VEA console, navigate to the Storage Agent node in the tree-view and expand the Enterprise Vault nodes under Applications.
- 2 Right-click the appropriate Enterprise Vault node and click Schedule Enterprise Vault Snapshot in the context menu.
- 3 In the wizard, review the Welcome page and click Next.
- 4 On the Select Components page, select the Enterprise Vault components you want to snapshot. Select the snapshot type and give it a name.

Specify the following and click Next to continue.

Select component for snapshot operation Select the EV components you want to snapshot. You can select EV Farm, sites, Vault StoreGroups, Vault Stores, partitions or any component.

Additionally, you can also use the keyboard shortcuts to select EV components. Ctrl+ A selects the entire EV farm along with sites and components. Use Ctrl+Click to select EV components of your choice.

Use Ctrl+Shift+Arrow Up, Down keys to select components located at the upper and lower hierarchies in the EV farm.

Directory	<p>The XML file is stored by default in the directory shown on the screen.</p> <p>In a clustered server environment, the XML file must be saved on shared storage to be available from all nodes in the cluster.</p> <p>Note: Note: The XML file for the snapshot must be stored separately from the volumes that are included in the snapshots, otherwise a restore will fail.</p> <p>There are two ways to change the XML file location.</p> <p>First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named <code>redirect.txt</code>. This text file should contain a single text line specifying the full path to the location of the XML file, for example, <code>G:\BackupSets</code>. Save the <code>redirect.txt</code> file in the default directory</p> <p><code>C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML.</code></p> <p>If SFW/SFW HA is installed on the D drive, then the path will be the same as above, but on the D drive.</p> <p>Note: You must not use the volume name or volume path in the <code>redirect.txt</code> file that is involved in the snapshot. If the volume name or path for the snapshot is used, then a restore will fail.</p>
Snapshot set	<p>Enter a name for the snapshot set, for example, <code>billing</code> or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, date, and time. Example: <code>SnapshotSet.EV.20091001.124837</code>.</p> <p>Note: If multiple components are selected, "EV" is used in the default snapshot set name instead of the component name.</p>

Select snapshot type Select the snapshot type.

You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a Enterprise Vault component.

■ Full Backup

A full snapshot affects the sequence of backups and is used when replay logs are needed while restoring.

If you want to replay logs in SQL Server as part of restoring a database, a Full backup needs to have been created earlier. When replaying logs, you can replay from the time of the last Full backup.

■ Copy

A Copy backup does not affect this sequence of log replay and therefore is often used as an "out of band" copy for purposes such as testing or data mining.

5 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	Enter a unique name for the snapshot set schedule. This name identifies the snapshot schedule if you later want to view information about the snapshot status. A default name consists of the VSS writer name, the component name and a numbered suffix that increments with each schedule.
Description of this schedule	Optionally, enter a description to help you identify the schedule when you view information about the snapshot status.
Start Time	The time of the day to begin taking snapshots.
End Time	The time of day to end taking snapshots. If a snapshot is in progress it is completed but a new one is not started after the end time.
Schedule takes effect on	The date on which the specified schedule takes effect. The default is the current date.

Restart task every	The interval between snapshots, in minutes. For example, if the interval is 360 minutes and you schedule a snapshot start time of 12 P.M. and an end time of 7 P.M, the snapshot occurs twice. If no interval is specified the snapshot occurs once.
Every	Enable the Every option to have the snapshot schedule continue to occur. Otherwise the schedule applies only for one day. Specify the number of days before restarting the snapshot schedule. For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.
Start On	If you enable the Every option, specify the starting date.
Pre Command	Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.
Post Command	Optionally, specify the full path of a command script to run after the snapshot is complete.

6 To specify run days for the schedule, make selections on the following tabs:

Days of Week	Select one or more days on one or more weeks of the month. You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.
Days of Month	Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.
Specific Dates	Select one or more specific dates to include in or to exclude from the schedule. Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9

If two schedules overlap for the same snapshot set, only one snapshot is taken. For example, if you select every Thursday plus the last day of the month, and the last day of the month occurs on Thursday, only one snapshot is taken on Thursday.

- 7 Click Next.
- 8 Review the snapshot set and schedule details and click Finish.

Using the Enterprise Vault Restore wizard

SFW provides recovery support for Enterprise Vault components. Using the Enterprise Vault Restore wizard, the snapshots created with the Enterprise Vault Snapshot wizard can be used to restore the components without logs.

Restoring the component without logs (recovery and no log replay) restores the database and the transaction log volumes. No other logs are applied. This leaves the component in an online state.

Note: Upon completion of the operation, the status (success/failure) of the selected components is recorded in a log, %VMPATH%\logs\EVStatus.log. The log contains information about the success or failure of the operation for the components. In the event that the restore of a volume for a component fails, the operation continues to restore the remaining volumes of the component and any other requested components. The components that successfully complete the operation are removed from the snapshot set. If the operation succeeds for all the volumes of a component, then the status of the component is logged as a success. If the operation fails for any one of the volumes of the component, then the status of the component is logged as a failure along with the cause of failure.

Recovering using snapshots without log replay

The following procedure uses the Recovery option. It restores the component database from the snapshot set volumes to the time of the snapshot set. The component database and transaction log volumes are restored but no additional transaction logs are applied.

Note: The Recovery option is applicable only for Enterprise Vault database components and not for Enterprise Vault Index and Partitions.

To recover EV components without log replay using the VEA

- 1 Except for the VEA GUI, close all windows, applications, or third-party system management tools that may be accessing the Enterprise Vault component volumes. It is also recommended to bring the database offline.
- 2 Using the VEA console, navigate to the Storage Agent node in the tree-view and expand the Enterprise Vault nodes under Applications
- 3 Right-click the Enterprise Vault node and click Enterprise Vault Restore in the context menu.
- 4 In the wizard, review the Welcome page and click Next.
- 5 Select the snapshot set XML metadata file to be used for this operation and click Next. The XML metadata file contains all required information needed to restore the snapshot set. Click the appropriate header to sort the list of available files by File Name or Creation Time.
- 6 On the Select Enterprise Vault components for Restore operation page, select the component or components that you want to restore using the Recovery option. The original volumes of the selected components are restored from the snapshot volumes.
- 7 On the Select Restore Type panel, select Recovery and specify options.

Recovery with missing original volumes	Enable this checkbox if one or more original volumes are missing.
Forcefully close any open handles	Enable this checkbox if any Enterprise Vault component volumes have open handles. This option forcefully closes any open handles of the volumes to be restored.

Click Next to continue.

- 8 Verify the snapshot restore specifications on the summary page and click Finish.
The database is restored to the time the snapshot set was created or last refreshed. Bring the database back online, if needed.

Restoring snapshots and manually applying logs

The following procedure uses the No Recovery option to restore the component database from the component database and log snapshot volumes. Selecting this option leaves the component database in a loading state. You can then manually

apply backed up transaction logs to recover the component database to the desired point in time.

Note: The No Recovery option is applicable only for Enterprise Vault database components and not for Enterprise Vault Index and Partitions.

Warning: Before you begin, use your preferred method to backup the transaction logs within SQL Server. You must use the “overwrite existing media” option to create uniquely-named backup files.

To restore EV components using the No Recovery option

- 1 Ensure that you have backed up the transaction logs within the SQL Server using the “overwrite existing media” option to create uniquely-named backup files.
- 2 Except for the VEA GUI, close all windows, applications, or third-party system management tools that may be accessing the Enterprise Vault component volumes. It is also recommended to bring the database offline.
- 3 Using the VEA console, navigate to the Storage Agent node in the tree-view and expand the Enterprise Vault nodes under Applications
- 4 4 Right-click the Enterprise Vault node and click Enterprise Vault Restore in the context menu.
- 5 5 In the wizard, review the Welcome page and click Next.
- 6 6 Select the snapshot set XML metadata file to be used for this operation and click Next. The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction log volumes. Click the appropriate header to sort the list of available files by File Name or Creation Time.
- 7 7 On the Select Enterprise Vault components for Restore operation page, select the Enterprise Vault component or components that you want to restore. The original volumes of selected components are restored from the snapshot volumes.
- 8 8 On the Select Restore Type panel, selectNoRecovery and specify any options.

Forcefully close any open handles Enable this checkbox if any Enterprise Vault component volumes have open handles. This option forcefully closes any open handles of the volumes to be restored.

Click **Next** to continue.

- 9** Verify the snapshot restore specifications on the summary page and click **Finish**.

The component database and log snapshot volumes are restored and the component database is left in a loading state.

- 10** Use your preferred method to manually restore the backup transaction logs to the desired point in time and then bring the component database back online.

Using the VSS snapshot wizards with Microsoft SQL

SFW provides support for taking snapshots of Microsoft SQL databases. FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with an SQL database without taking the database offline. The VSS Snapshot wizard uses VSS to take snapshots of the database. The VSS process allows the database to be quiesced before the snapshot operation and reactivates it immediately after. The quiescing of the database and guarantees persistent snapshots of the data. A snapshot of a database can be reattached and resynchronized to match the current state of the database with the VSS Snapback wizard.

Note: Snapshots can only be taken of read/write volumes when VSS is used. The resulting VSS snapshot is read only. The file system label of VSS snapshot volumes cannot be changed.

SFW also provides a VSS Snapshot Scheduler wizard that can be used as an alternative to the VSS Snapshot wizard and the VSS Snapback wizard. It enables you to set up a schedule for taking the initial snapshots and for automating the snapback refresh process. At the scheduled time for the snapshot, the snapshot volumes are automatically reattached, resynchronized, and then split again. The schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background.

SFW also provides recovery support for a SQL database. Using the VSS Restore wizard, the snapshots taken with the VSS Snapshot wizard can be used for a recovery of the database with or without logs.

Refer to the *Veritas Storage Foundation and High Availability Solutions 5.1 Solutions Guide for Microsoft SQL* for additional information about how to use FlashSnap with Microsoft SQL to perform and to implement recovery procedures.

This section covers the following topics:

- [Using the VSS Snapshot wizard](#)
- [Using the VSS Snapback wizard](#)
- [Using the VSS Snapshot Scheduler wizard](#)
- [Using the VSS Restore wizard](#)

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support snapshot or VSS related commands.

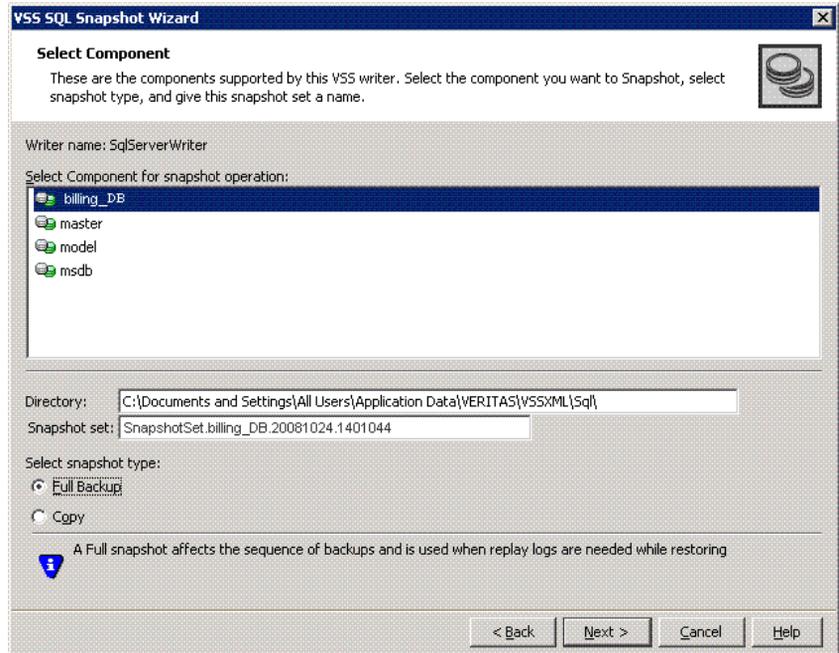
Using the VSS Snapshot wizard

Creating a snapshot is a two-step process. The first step, prepare the volume for snapshot, creates snapshot mirrors attached to all the original volumes in the specified database. Depending on the size and number of volumes, the process of synchronizing the new snapshot mirrors with the original production volumes can take a long time. The second step uses the VSS Snapshot wizard to create the snapshot set by detaching the snapshot mirrors from the original volumes and creating separate on-host snapshot volumes as well as an XML file to store the database and snapshot volume metadata. The VSS Snapshot wizard integrates with VSS to quiesce the database and then simultaneously snapshot the volumes in the database. This snapshot is done while the database is online and without disrupting processing. Once a snapshot set has been created, it can be reattached and resynchronized with the VSS Snapback wizard.

Creating the snapshot set

To create the snapshot set from the VEA console

- 1 From the VEA console, navigate to the system where the production volumes and snapshots mirrors are located.
- 2 Expand the system node, the Storage Agent node, and the **Applications** node. If the SQL node is not shown, start the SQL Server VSS Writer service and then select the Storage Agent node and refresh the VEA display (**Actions > Refresh**).
- 3 Expand the **SQL** node.
- 4 Right-click the instance and click **VSS Snapshot**.
- 5 In the wizard, review the Welcome page and click **Next**.

6 Specify the snapshot set parameters as follows and then click **Next**:

Select Component for
snapshot operation

Directory

Select the database for the snapshot set.

The wizard creates the snapshot set metadata XML file. The XML metadata file is stored by default in the directory shown on the screen.

There are two ways to change the XML file location.

First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named `redirect.txt`. This text file should contain a single text line specifying the full path to the location of the XML file, for example, `G:\BackupSets`. Save the `redirect.txt` file in the default directory `C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML`.

If SFW/SFW HA is installed on the D drive, then the path will be the same as above, but on the D drive.

Snapshot set Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, date, and time.

Select snapshot type Select the snapshot type.
You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a database. However, if you want to replay logs in SQL Server as part of restoring a database, a Full backup needs to have been created earlier. When replaying logs, you can replay from the time of the last Full backup. A Copy backup does not affect this sequence of log replay and therefore is often used as an "out of band" copy for purposes such as testing or data mining.

7 In the Change Attributes panel, optionally change the attributes for the snapshot volumes and click **Next**:

Snapshot Volume Label Displays the read-only label for the snapshot volume.

Drive Letter Optionally, click a drive letter and select a new choice from the drop-down menu.

Plex Optionally, click a plex and select a new choice from the drop-down menu.

8 On the Synchronized Snapshot panel (VVR only), select the secondary hosts for which you want to create synchronized snapshots. Either double-click on the host name or click the **Add** option to move the host into the Selected Secondary Hosts pane. To select all the available hosts, click the **Add All** option. The VSS wizard creates synchronized snapshots on all the selected secondary hosts.

This panel is displayed only in an environment using Veritas Volume Replicator (VVR). Otherwise, you will be directly taken to the Schedule Information panel.

See *Veritas Volume Replicator Administrator's Guide*.

9 Review the specifications of the snapshot set and click **Finish**.

Using the VSS Snapback wizard

The VSS Snapback wizard reattaches and resynchronizes an existing snapshot set so that it matches the current state of its original SQL database. The wizard is available in the context menu of the VSS Writer object.

Resynchronizing the snapshot set

To snapback a snapshot set

- 1 Close the database application GUI and all Explorer windows, applications, consoles (except the VEA console), or third-party system management tools that may be accessing the snapshot set.
- 2 From the VEA console URL bar, select the *<host name>* which is the system where the production volumes and snapshot mirrors are located, as the active host.
- 3 Expand the system node, the Storage Agent node, and the **Applications** node.
- 4 Right-click on the node of the application and click **VSS Snapback**.
- 5 Review the Welcome page and click **Next**.
- 6 Select the snapshot set you want to snapback and click **Next**.
The XML metadata file contains all required information needed to snapback the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**. This file is deleted after the snapback operation has completed successfully.
- 7 If a message appears that indicates some volumes have open handles, confirm that all open handles are closed and then click Yes to proceed.
- 8 Verify that the snapback specifications are correct and click **Finish**.

Using the VSS Snapshot Scheduler wizard

You can use the VSS Snapshot Scheduler wizard to add a snapshot schedule.

The scheduling capability automates the process of refreshing snapshot sets. At the time scheduled for the snapshot, the snapshot volumes are automatically reattached, resynchronized, and then split again. Once configured and applied, the schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background. In a clustered server environment, ensure that the scheduler service is configured on each node with domain administrator privileges so that any node in the cluster can run the schedule after a failover.

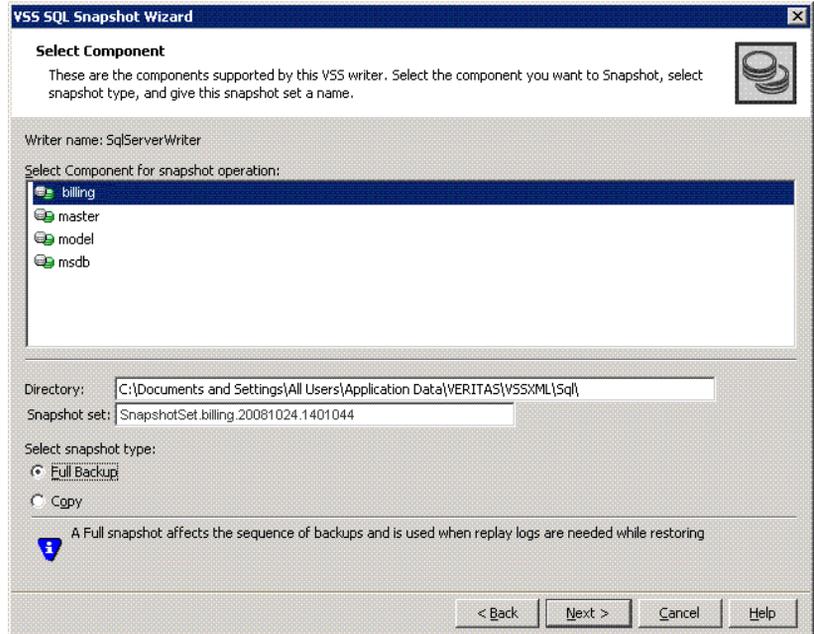
The VSS Snapshot Scheduler wizard does not prepare the snapshot mirror. Prepare the snapshot mirror with the **Prepare** command before running the VSS Snapshot Scheduler wizard.

Note: The **Prepare** command replaces the **Snap Start** command in the GUI.

To schedule a snapshot for a selected component

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node, the Storage Agent node, and the **Applications Node**. If the SQL node is not shown, start the SQL Server VSS Writer service and then select the Storage Agent node and refresh the VEA display (**Actions > Refresh**).
- 3 Expand the **SQL** node.
- 4 Right-click the instance, and click **Schedule VSS Snapshot**.
- 5 In the Welcome panel, review the information and click **Next**.

6 Specify the snapshot set parameters as follows and then click **Next**:



Select component for snapshot operation	Select the database for the snapshot set.
Directory	<p>The XML file is stored by default in the directory shown on the screen.</p> <p>In a clustered server environment, the XML file must be saved on shared storage to be available from all nodes in the cluster.</p> <p>There are two ways to change the XML file location.</p> <p>First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named <code>redirect.txt</code>. This text file should contain a single text line specifying the full path to the location of the XML file, for example, <code>G:\BackupSets</code>. Save the <code>redirect.txt</code> file in the default directory <code>C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML</code>.</p> <p>If SFW/SFW HA is installed on the D drive, then the path will be the same as above, but on the D drive</p>
Snapshot set	Enter a name for the snapshot set, for example, <code>billing</code> or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, date, and time.
Select snapshot type	<p>Select the snapshot type.</p> <p>You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a database. However, if you want to replay logs in SQL Server as part of restoring a database, a Full backup needs to have been created earlier. When replaying logs, you can replay from the time of the last Full backup. A Copy backup does not affect this sequence of log replay and therefore is often used as an "out of band" copy for purposes such as testing or data mining.</p>

- 7 In the Change Attributes panel, optionally change the attributes for the snapshot volumes and click **Next**:

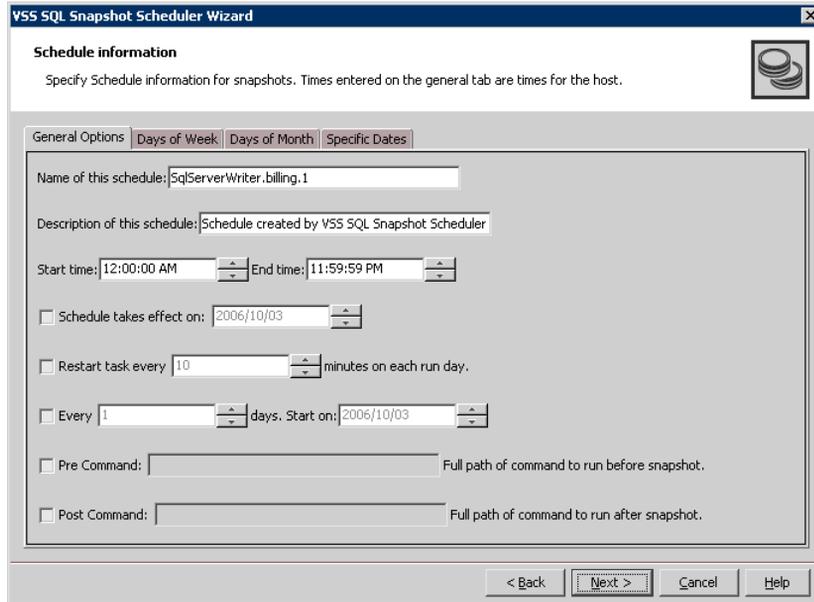
Snapshot Volume Label	Displays the read-only label for the snapshot volume.
Drive Letter	Optionally, click a drive letter and select a new choice from the drop-down menu. The drive letters specified may not be available when the snapshot is taken. When this occurs, the snapshot operation is performed, but no drive letters are assigned.
Plex	Optionally, click a plex and select a new choice from the drop-down menu.

- 8 Optionally, in the Synchronized Snapshot panel (VVR only), select the secondary hosts for which you want to create synchronized snapshots. Either double-click on the host name or click the **Add** option to move the host into the Selected Secondary Hosts pane. To select all the available hosts, click the **Add All** option. The VSS wizard creates synchronized snapshots on all the selected secondary hosts.

This panel is displayed only in an environment using Veritas Volume Replicator (VVR). Otherwise, you will be directly taken to the Schedule Information panel.

See *Veritas Volume Replicator Administrator's Guide*.

- 9 In the Schedule Information panel, on the General Options tab, specify the following:



- | | |
|------------------------------|---|
| Name of this schedule | Enter a unique name for the snapshot set schedule. This name identifies the snapshot schedule if you later want to view information about the snapshot status. A default name consists of the VSS writer name, the component name and a numbered suffix that increments with each schedule. |
| Description of this schedule | Optionally, enter a description to help you identify the schedule when you view information about the snapshot status. |
| Start Time | The time of the day to begin taking snapshots. |
| End Time | The time of day to end taking snapshots. If a snapshot is in progress it is completed but a new one is not started after the end time. |
| Schedule takes effect on | The date on which the specified schedule takes effect. The default is the current date. |

Restart task every	<p>The interval between snapshots, in minutes.</p> <p>For example, if the interval is 360 minutes and you schedule a snapshot start time of 12 P.M. and an end time of 7 P.M, the snapshot occurs twice. If no interval is specified the snapshot occurs once.</p>
Every	<p>Enable the Every option to have the snapshot schedule continue to occur. Otherwise the schedule applies only for one day.</p> <p>Specify the number of days before restarting the snapshot schedule.</p> <p>For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.</p>
Start On	<p>If you enable the Every option, specify the starting date.</p>
Pre Command	<p>Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.</p>
Post Command	<p>Optionally, specify the full path of a command script to run after the snapshot is complete.</p>

10 To specify run days for the schedule, make selections on the following tabs:

Days of Week	<p>Select one or more days on one or more weeks of the month.</p> <p>You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.</p>
Days of Month	<p>Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.</p>
Specific Dates	<p>Select one or more specific dates to include in or to exclude from the schedule.</p> <p>Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.</p>

If two schedules overlap for the same snapshot set, only one snapshot is taken. For example, if you select every Thursday plus the last day of the month, and the last day of the month occurs on Thursday, only one snapshot is taken on Thursday.

- 11 Click **Next**.
- 12 Review the snapshot set and schedule details and click **Finish**.

Displaying the status of the scheduled VSS SQL snapshot

If a scheduled snapshot fails for some reason, the scheduler process will attempt to rerun it. You may want to verify that scheduled snapshots completed successfully. From the VEA console, you can view snapshot results.

To view a scheduled snapshot status

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node and the Storage Agent node.
- 3 Click **Scheduled Tasks** to view all the applications that have schedules.
- 4 Select the application for which you scheduled the snapshot. The scheduled snapshots are listed in the pane on the right.
If you have just configured the schedules and they are not yet displayed, right-click the Storage Agent node and click **Refresh** to update the display.
- 5 Choose one of the following:
 - To view the status of all scheduled jobs, right-click the selected application and click **All Job History**.
 - To view the status of a particular schedule, right-click the snapshot schedule name and click **Job History**.
- 6 In the Job History dialog box, view the schedule information.
You can sort listed schedules by clicking the column headings. The Status column shows if the snapshot completed successfully.

Deleting a schedule for a VSS SQL snapshot

Note: You cannot modify a schedule that has expired.

You can also delete (but not modify) a schedule from the VEA console.

Note: The VEA can delete snapshot schedules only; it does not delete mirror preparation scheduled with the Quick Recovery Configuration Wizard. In addition, deleting a snapshot schedule using the VEA does not update template settings created with the Quick Recovery Configuration Wizard.

To delete a schedule from the VEA

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the **System** node and **StorageAgent** node. Select and click to expand the **Scheduled Tasks > Exchange** node.
The scheduled snapshots are listed on the right pane.
- 3 Right-click the name of the snapshot schedule and select **Delete Schedule**.

Using the VSS Restore wizard

SFW provides recovery support for a SQL database. Using the VSS Restore wizard, the snapshots created with the VSS Snapshot wizard can be used to restore the database with or without logs.

Restoring the database with logs (recovery and log replay) restores the database and the transaction log volumes. Backup transaction logs are also applied. This leaves the database in an online state.

Restoring the database without logs (recovery and no log replay) restores the database and the transaction log volumes. No other logs are applied. This leaves the database in an online state.

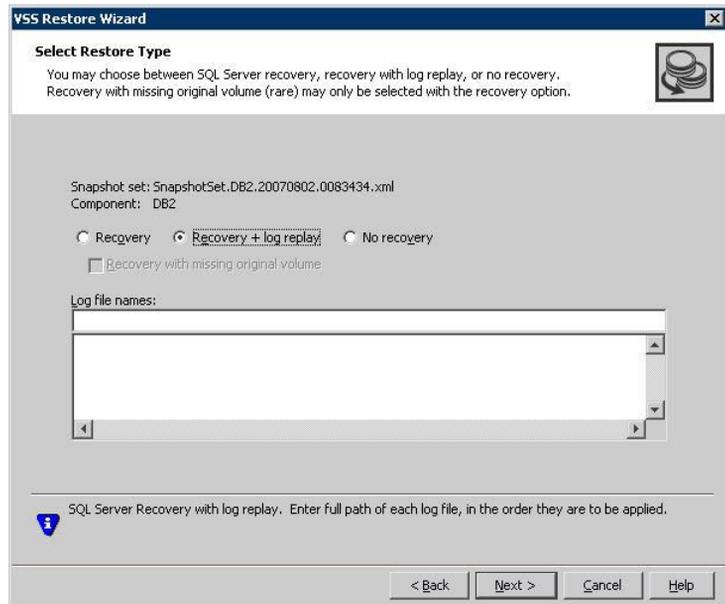
Restoring the database with no recovery (no recovery and no log replay) restores the database and the transaction log volumes. However no logs are applied. This leaves the database in a loading state and ready for backup transaction logs to be applied.

Restoring the database with recovery and logs

To use log replay for an automatic roll-forward recovery to a point of failure using the VEA

- 1 Ensure that you have backed up the transaction logs within SQL Server using the “overwrite existing media” option to create uniquely-named backup files.
- 2 Close the SQL GUI and all Explorer windows, applications, consoles (except the VEA), or third-party system management tools that may be accessing the volumes. It is also recommended to bring the database offline.
- 3 From the VEA console, navigate to the system where the database volumes are located.
- 4 Expand the system node, the Storage Agent node, and the **Applications** node
- 5 Right-click **SQL** and click **VSS Restore**.
- 6 Review the Welcome page and click **Next**.
- 7 Select the snapshot set XML metadata file to be used for this operation and click **Next**.
The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**.
- 8 On the Select Restore Type panel, do the following and click Next:
 - Click **Recovery + Log replay**.

- Enter the full path of each log file, in the order they are to be applied.



- 9 You may receive a message “Some volumes in this component have open handles. Do you want to override these handles and do this restore? Click **Yes** to proceed.” Click **No**, close any open handles and retry the command.
- 10 Verify the restore specifications and click **Finish**.
After the most recent backup log is replayed, the SQL Server database is closed and left in an operational state. If you took it offline earlier, bring it back online.
- 11 The restore operation leaves the snapshot volumes snapped back to the production volumes. To ensure that another split-mirror snapshot set is immediately available, use the VSS SQL Snapshot Wizard to create a new snapshot of all the volumes in the database.

Restoring the database with recovery without logs

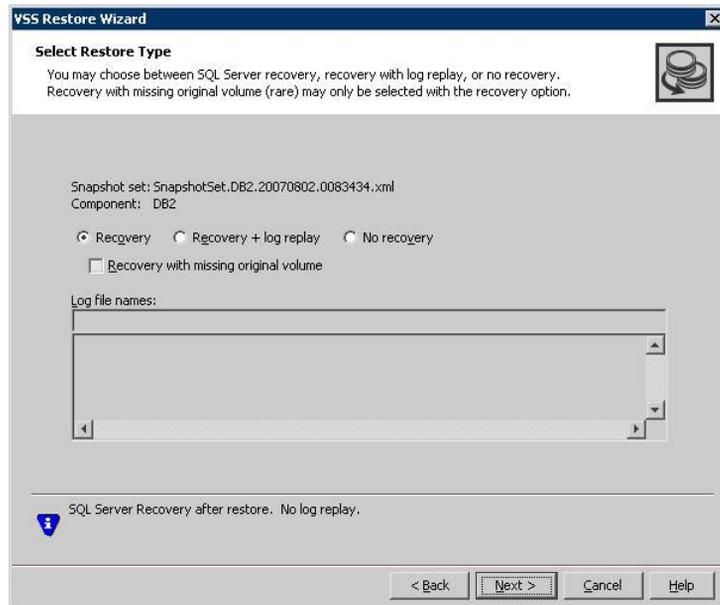
To recover a database without log replay using the VEA

- 1 Close the SQL GUI and all Explorer windows, applications, consoles (except the VEA), or third-party system management tools that may be accessing the volumes. It is also recommended to bring the database offline.

- 2 From the VEA console, navigate to the system where the database volumes are located.
- 3 Expand the system node, the Storage Agent node, and the **Applications node**.
- 4 Right-click **SQL** and click **VSS Restore**.
- 5 Review the Welcome page and click **Next**.
- 6 Select the snapshot set XML metadata file to be used for this operation and click **Next**.

The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**.

- 7 On the Select Restore Type panel, click **Recovery**.



- 8 You may receive a message “Some volumes in this component have open handles. Do you want to override these handles and do this restore? Click **Yes** to proceed.” Click **No**, close any open handles and retry the command.
- 9 Verify the restore specifications and click **Finish**.
The database is restored to the time the snapshot set was created or last refreshed. If you took it offline earlier, bring it back online.

- 10 The restore operation leaves the snapshot volumes snapped back to the production volumes. To ensure that another split-mirror snapshot set is immediately available, use the VSS SQL Snapshot Wizard to create a new snapshot of all the volumes in the database.

Restoring the database with one or more missing volumes

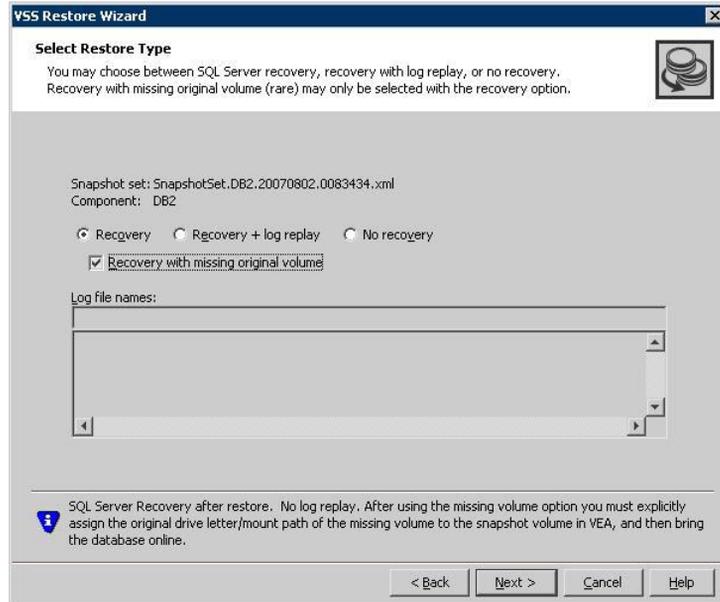
Note: COW snapshots are not supported for recovery with missing volumes.

To recover a database with one or more missing volumes using the VEA

- 1 Close the SQL GUI and all Explorer windows, applications, consoles (except the VEA), or third-party system management tools that may be accessing the volumes. It is also recommended to bring the database offline.
- 2 From the VEA console, navigate to the system where the database volumes are located.
- 3 Expand the system node, the Storage Agent node, and the **Applications** node.
- 4 Right-click **SQL** and click **VSS Restore**.
- 5 Review the Welcome page and click **Next**.
- 6 Select the snapshot set XML metadata file to be used for this operation and click **Next**.

The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**.

- 7 On the Select Restore Type panel, click **Recovery** and select **Recovery with missing original volume**.



- 8 You may receive a message “Some volumes in this component have open handles. Do you want to override these handles and do this restore? Click **Yes to proceed**.” Click **No**, close any open handles and retry the command.
- 9 Verify the restore specifications and click **Finish**.
The snapshot of the missing volume is changed from a read-only volume to a read-write volume.
- 10 If you have not already done so, in the VEA, ensure that the drive letter or mount path of the missing production volume is assigned to the snapshot volume.
- 11 Bring the database online.
If the production volume was missing, the snapshot volume is now changed to the production volume. The database is restored to the time the snapshot set was created or last refreshed.
- 12 To ensure that another split-mirror snapshot set is immediately available, use the VSS SQL Snapshot Wizard to create a new snapshot of all the volumes in the database.

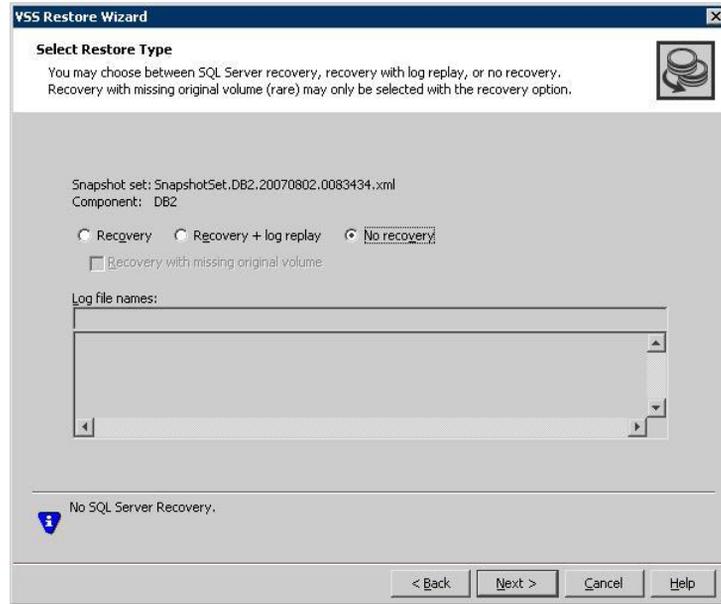
Restoring the database with no recovery

To restore using the No Recovery option in the VEA

- 1 Ensure that you have backed up the transaction logs within SQL Server using the “overwrite existing media” option to create uniquely-named backup files.
- 2 Close the SQL GUI and all Explorer windows, applications, consoles (except the VEA console), or third-party system management tools that may be accessing the database volumes. It is also recommended to bring the database offline.
- 3 From the VEA console, navigate to the system where the database volumes are located.
- 4 Expand the system node, the Storage Agent node, and the **Applications** node
- 5 Right-click **SQL** and click **VSS Restore**.
- 6 Review the Welcome page and click **Next**.
- 7 Select the snapshot set XML metadata file to be used for this operation and click **Next**.

The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**.

- 8 On the Select Restore Type panel, click **No Recovery** and click **Next**.



- 9 You may receive a message “Some volumes in this component have open handles. Do you want to override these handles and do this restore? Click **Yes to proceed**.” Click **No**, close any open handles and retry the command.
- 10 Verify the restore specifications and click **Finish**.
The database and log snapshot volumes are restored and the SQL Server database is left in a loading state.
- 11 Use your preferred method to manually restore the backup transaction logs to the desired point in time and then bring the database back online.
- 12 The restore operation leaves the snapshot volumes snapped back to the production volumes. To ensure that another split-mirror snapshot set is immediately available, use the VSS SQL Snapshot Wizard to create a new snapshot of all the volumes in the database.

Copy on Write (COW)

This section describes how Veritas Storage Foundation for Windows works with Microsoft Copy on Write (COW) to provide snapshots.

Overview

SFW supports Microsoft Copy on Write (COW) snapshots. The SFW GUI or the vxsnap CLI utility can be used to take COW snapshots. Microsoft COW snapshots are faster than full snapshots and take up less storage space.

A COW snapshot creates a shadow copy that is differential. When a change to the original volume occurs, the block that is about to be modified is read and then written to a “differences area”, which preserves a copy of the data block before it is overwritten with the change. This approach stores a copy of the block before it is changed. Using the blocks in the differences area and unchanged blocks in the original volume, a copy of the volume can be constructed that represents the volume in the state before any changes occurred.

The benefit of the COW snapshot is that it creates shadow copies very rapidly because it is only writing changed blocks at a given time.

Note: COW snapshots are supported in a VCS environment running only on Windows Server 2008 x86 and Windows Server 2008 x64. COW snapshots are not supported in a Microsoft Clustering environment.

SFW VSS COW snapshot process

The process for creating COW snapshots with VSS is a two step process. The first step is to create a Shadow Storage area (differences area). A Shadow Storage area must exist before taking a COW snapshot to preserve data blocks before they are overwritten. The second step is to create the COW snapshot.

The process for creating COW snapshots with VSS can be done with the GUI or the command line.

For more information about the command line operations, see the vxsnap CLI command.

Managing Shadow Storage

With the Shadow Storage dialog, you may add, remove, or specify another size for the Shadow Storage area.

- Add Shadow Storage allows you to add a shadow storage area for a volume.

Note: Note: Shadow storage areas are supported only on NTFS volumes.

- Remove Shadow Storage allows you to remove the shadow copy storage area for a volume.
- Resize Shadow Storage allows you to update the shadow copy storage area maximum size for a volume. This dialog allows you to specify an unlimited or exact volume size.

To add Shadow Storage

- 1 Right-click the volume you want to add shadow storage.
- 2 Click Shadow Storage> Add in the context menu.
- 3 Select the volume to store shadow copies and the disk space size.
 - Choose the No limit option to specify that unlimited disk space can be used to store shadow copies.
 - Choose the Use limit option to set the maximum amount of disk space allowed to store shadow copies. Also specify the exact amount of disk space (MB) to be used.
- 4 Click OK to complete the settings.

Note: The vxsnap diffarea command can also be used to create the Shadow Storage area.

Note: A basic volume cannot be used as a Shadow Storage area.

To resize Shadow Storage

- 1 Right-click the volume that contains the shadow storage you want to resize.
- 2 Click Shadow Storage>Resize in the context menu.
- 3 Choose the disk space size.
 - Choose the No limit option to specify that unlimited disk space can be used to store shadow copies.
 - Choose the Use limit option to set the maximum amount of disk space allowed to store shadow copies. Also specify the exact amount of disk space (MB) to be used.
- 4 Click OK to complete the command.

To remove Shadow Storage

- 1 Right-click the volume that contains the shadow storage you want to remove.
- 2 Click Shadow Storage>Remove in the context menu.
- 3 Click Yes to complete the command.

Using the VSS COW Snapshot wizard

Perform a COW snapshot with the COWSnap Shot wizard.

To create VSS COW snapshots

- 1 Right-click a volume in the tree-view.
- 2 Click COW>Snap Shot in the context menu.
- 3 In the wizard, review the Welcome page and click Next.
- 4 In the Select Volumes window that appears, select the volumes that you want to take a snapshot of.

Highlight the volumes in the Available volumes pane and click Add. Your selected volumes should appear in the Selected volumes pane.

The list of available volumes is a list of all volumes that have a shadow storage area and are in the same disk group of the selected volume.

Specify the snapshot set parameters as appropriate and then click Next.

Directory	The wizard creates the snapshot set metadata XML file. The XML metadata file is stored by default in the directory shown on the screen.
Snapshot set	Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet.cow.ID_number", date, and time.
5	Review the specifications of the snapshot set and click Finish.

Note: You can also use the vxsnap create CLI command to take the snapshot.

Using the VSS COW Snapshot Scheduler wizard

You can use the VSS COW Snapshot Scheduler wizard to add a snapshot schedule.

The scheduling capability automates the process of taking snapshots. At the scheduled time, the specified volumes are automatically snapshotted. A new snapshot set is made every time the schedule calls for a snapshot to be taken. In this way, a series of snapshot sets can be made with the scheduler. Once configured and applied, the schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background.

Note: Information about the operations performed by the schedule can be found by expanding the nodes under the Scheduled Tasks node in the tree-view of the GUI. Expand the Generic node to locate the schedules for snapshots of volumes. Right-click the node and select Job History to view information about the operations performed by the schedule.

Note: You must create a shadow storage area before running the VSS COW Snapshot Scheduler wizard.

To create a schedule for VSS COW snapshots

- 1 Right-click a volume in the tree-view.
- 2 Click COW>ScheduleCOWSnapShot in the context menu.
- 3 In the wizard, review the Welcome page and click Next.
- 4 In the Select Volumes window that appears, select the volumes that you want to take a snapshot of.
Highlight the volumes in the Available volumes pane and click Add. Your selected volumes should appear in the Selected volumes pane.
The list of available volumes is a list of all volumes that have a shadow storage area and are in the same disk group of the selected volume.
Specify the snapshot set parameters as appropriate and then click Next

Directory	The wizard creates the snapshot set metadata XML file. The XML metadata file is stored by default in the directory shown on the screen.
Snapshot set	Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet.cow" date, and time. Every time the a snapshot is taken, a unique snapshot set name is generated.

5 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	<p>Enter a unique name for the snapshot set schedule.</p> <p>This name identifies the snapshot schedule if you later want to view information about the snapshot status. A default name consists of the VSS writer name, the component name and a numbered suffix that increments with each schedule.</p>
Description of this schedule	<p>Optionally, enter a description to help you identify the schedule when you view information about the snapshot status.</p>
Start Time	<p>The time of the day to begin taking snapshots.</p>
End Time	<p>The time of day to end taking snapshots.</p> <p>If a snapshot is in progress it is completed but a new one is not started after the end time.</p>
Schedule takes effect on	<p>The date on which the specified schedule takes effect. The default is the current date.</p>
Restart task every	<p>The interval between snapshots, in minutes.</p> <p>For example, if the interval is 360 minutes and you schedule a snapshot start time of 12 P.M. and an end time of 7 P.M, the snapshot occurs twice. If no interval is specified the snapshot occurs once.</p>
Every	<p>Enable the Every option to have the snapshot schedule continue to occur. Otherwise the schedule applies only for one day.</p> <p>Specify the number of days before restarting the snapshot schedule.</p> <p>For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.</p>
Start On	<p>If you enable the Every option, specify the starting date.</p>
Pre Command	<p>Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.</p>
Post Command	<p>Optionally, specify the full path of a command script to run after the snapshot is complete.</p>

6 To specify run days for the schedule, make selections on the following tabs:

Days of Week	Select one or more days on one or more weeks of the month. You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.
Days of Month	Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.
Specific Dates	Select one or more specific dates to include in or to exclude from the schedule. Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.

If two schedules overlap for the same snapshot set, only one snapshot is taken. For example, if you select every Thursday plus the last day of the month, and the last day of the month occurs on Thursday, only one snapshot is taken on Thursday.

7 Click **Next**.

8 Review the specifications of the snapshot set and click **Finish**.

Displaying the status of the scheduled VSS COW snapshot

If a scheduled snapshot fails for some reason, the scheduler process will attempt to rerun it. You may want to verify that scheduled snapshots completed successfully. From the VEA console, you can view snapshot results.

To view a scheduled snapshot status

- 1** From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2** Expand the system node and the Storage Agent node.
- 3** Click **Scheduled Tasks**.

- 4 Expand the Generic node. The scheduled snapshots are listed in the pane on the right.
All scheduled snapshots not associated with an Application are displayed under the Generic node.
- 5 Choose one of the following:
 - To view the status of all scheduled jobs, right-click Generic and click All Job History
 - To view the status of a particular schedule, right-click the snapshot schedule name and click Job History.
- 6 In the dialog box, view the schedule information.
You can sort listed schedules by clicking the column headings. The Status column shows if the snapshot completed successfully.

Deleting a schedule for a VSS COW snapshot

The following is the procedure to delete a schedule.

You can also delete (but not modify) a schedule from the GUI console.

To delete a schedule with the GUI

- 1 From the VEA console, navigate to the system where the production volumes are located.
- 2 Expand the system node and the Storage Agent node.
- 3 Click Scheduled Tasks.
- 4 Expand the Generic node for which you scheduled the snapshot. The scheduled snapshots are listed in the pane on the right.
- 5 Right-click the name of the snapshot schedule and click Delete Schedule.

Using the VSS COW Restore wizard

Uses the snapshot volume in a snapshot set created s by VSS COW snapshot to restore data, for example, after an original volume has become corrupted.

To restore a volume with COW snapshot

- 1 Right-click a volume or a component of an application in the tree-view.
- 2 Click COW>Restore in the context menu.
- 3 In the wizard, review the Welcome page and click Next.
- 4 Select the snapshot set XML metadata file to be used for this operation and click Next.

The XML metadata file contains all required information needed to restore the volume.

- 5 In the Select Volumes window that appears, select the volumes that you want to restore.
Highlight the volumes in the Available volumes pane and click Add. Your selected volumes should appear in the Selected volumes pane.
- 6 Review the specifications of the snapshot set and click Finish.

Additional information about COW snapshots

Since COW snapshots rely on a Shadow Storage area, COW snapshots have the following constraints:

- COW snapshots are developed by keeping track of blocks that have changed. If the original volume that the COW snapshot is based upon becomes unavailable or corrupted, then the COW snapshot cannot be used to restore the snapshotted volume.
- After restoring the original volume with a COW snapshot, any subsequent COW snapshots taken after that snapshot are automatically deleted by Windows.
- The number of COW snapshots for a volume is limited by the size of the shadow storage area allocated. When the shadow storage area has reached its capacity, then older snapshots are deleted to make room for new snapshots. In addition, 512 COW snapshots is the maximum number allowed per volume.
- During a restore operation, a forced dismount of the original volume or the volume containing the shadow storage area may result in I/O corruption and the loss of COW snapshots.
- Due to the incremental nature of COW snapshots, COW snapshots can only be used to restore the snapshotted volume to a point in time.
- For every write operation on a new block of the snapshotted volume, a read operation is performed to allow the COW snapshot to store the block in the shadow storage area. As a result, a COW snapshot may impact the I/O performance of the snapshotted volume.
- SFW only supports COW snapshots of dynamic volumes.
- Both the shadow storage area and the snapshotted volume must reside in the same dynamic disk group.
- If a volume containing a shadow storage area is a part of a snapshot set and the shadow storage area volume is restored, then all snapshots that were stored on that volume are deleted automatically by Windows. Make sure that

volumes containing shadow storage areas for other volumes are not part of the same snapshot set. Otherwise COW snapshots may automatically get deleted during a restore operation, resulting in a snapshot not found error.

After performing operations for COW snapshots or operations on the Shadow Storage area, the VEA GUI may not be updated to reflect the results of the operation. Use the VSS Refresh command to update the VEA GUI.

Using the VSS COW snapshot wizards with Microsoft Exchange

SFW provides support for taking VSS COW snapshots of Microsoft Exchange 2003 and Exchange 2007 storage groups. FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with an Exchange storage group without taking the storage group's databases offline. The VSS COW Snapshot wizard uses VSS to take snapshots of storage groups. The VSS process allows the storage group's databases to be quiesced before the snapshot operation and reactivates them immediately after.

SFW also provides a VSS COW Snapshot Scheduler wizard that can be used as an alternative to the VSS COW Snapshot wizard. It enables you to set up a schedule for taking the snapshots at the specified times. The schedule is maintained by a scheduler service, `VxSchedService.exe`, that runs in the background.

Using the VSS COW Snapshot wizard

Creating a snapshot is a two-step process. The first step, creating a shadow storage area for the snapshot, creates a differences area to store blocks of data before they are changed. The second step uses the VSS COW Snapshot wizard to take the snapshot and create an XML file to store the Exchange and snapshot volume metadata. The VSS COW Snapshot wizard integrates with VSS to quiesce the databases and then simultaneously snapshot the volumes in the storage group. This snapshot is done while the databases are online and without disrupting the email flow.

Note: You must create a shadow storage area before running the VSS COW Snapshot wizard.

Note: After performing COW related operations with the Windows GUI, the VEA GUI may not be updated to reflect the results of the operation. Use the VSS Refresh command to update the VEA GUI.

Creating the snapshot set

The following is the procedure to create a snapshot set.

Note: You must create a shadow storage area before running the VSS COW Snapshot wizard.

To create the snapshot set using the GUI

- 1 From the VEA console, navigate to the system where the production volumes are located.
- 2 Expand the system node, the Storage Agent node, and the Applications node.
- 3 Right-click Exchange and click VSSCOWSnapshot
- 4 In the wizard, review the Welcome page and click Next.
- 5 Specify the snapshot set parameters as follows and then click Next

Select Component for snapshot operation	Select the component for the snapshot set For Exchange, the component is a storage group.
Directory	The snapshot set metadata XML file is stored under this name. The XML file is stored by default in the directory shown on the screen. However, in a clustered server environment, the XML file must be saved on shared storage to be available from all nodes in the cluster. To accomplish this, use a text editor to create a text file named "redirect.txt." This text file should contain a single text line specifying the full path to the location of the metadata file, for example, G:\BackupSets. Save the redirect.txt file in the default directory C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML on each node of the cluster.
Snapshot set	Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, identification number, date, and time.

Select snapshot type Select the snapshot type.

Full Backup is typically used for backup to tape or other storage media. It does the following:

- Creates a copy of the selected component
- Runs Eseutil to check for consistency before truncating the logs
- Truncates the transaction logs

Copy is typically used for Quick Recovery. It creates a copy of the storage group, but does not truncate the transaction logs. Optionally check Run Eseutil with the Copy option to check the snapshot for consistency.

6 Review the specifications of the snapshot set and click Finish

Using the VSS COW Snapshot Scheduler wizard

You can use the VSSCOWSnapshot Scheduler wizard to add a snapshot schedule.

The scheduling capability automates the process of taking snapshots. At the scheduled time, the specified volumes are snapshotted automatically. Once configured and applied, the schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background. In a clustered server environment, ensure that the scheduler service is configured on each node with domain administrator privileges so that any node in the cluster can run the schedule after a failover.

Note: Information about the operations performed by the schedule can be found by expanding the nodes under the Scheduled Tasks node in the tree-view of the GUI. Expand the appropriate application node to locate the schedules for that application. Right-click the node and select JobHistory to view information about the operations performed by the schedule.

Note: You must create a shadow storage area before running the VSS COW Snapshot wizard.

To schedule a snapshot for a selected component

1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.

- 2 Expand the system node, the Storage Agent node, and the Applications node.
- 3 Right-click the Exchange storage group, and click Schedule VSSCOW Snapshot.
- 4 In the Welcome panel, review the information and click Next.
- 5 Specify the snapshot set parameters as follows and then click Next:

Select component for snapshot operation Select the component for the snapshot set.

Directory	<p>The XML file is stored by default in the directory shown on the screen.</p> <p>In a clustered server environment, the XML file must be saved on shared storage to be available from all nodes in the cluster.</p> <p>There are two ways to change the XML file location.</p> <p>First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named <code>redirect.txt</code>. This text file should contain a single text line specifying the full path to the location of the XML file, for example, <code>G:\BackupSets</code>. Save the <code>redirect.txt</code> file in the default directory <code>C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML</code>.</p> <p>If SFW/SFW HA is installed on the D drive, then the path will be the same as above, but on the D drive.</p> <p>Note: When a COW snapshot is scheduled, a snapshot is taken at the specified time and a new xml file is generated for each snapshot.</p>
Snapshot set	<p>Enter a name for the snapshot set, for example, <code>billing</code> or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, identification number, date, and time.</p>
Select the snapshot type.	<p>You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a database.</p>

6 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	Enter a unique name for the snapshot set schedule. This name identifies the snapshot schedule if you later want to view information about the snapshot status. A default name consists of the application name and a numbered suffix that increments with each schedule.
Description of this schedule	Optionally, enter a description to help you identify the schedule when you view information about the snapshot status.
Start Time	The time of the day to begin taking snapshots.
End Time	The time of day to end taking snapshots. If a snapshot is in progress it is completed but a new one is not started after the end time.
Schedule takes effect on	The date on which the specified schedule takes effect. The default is the current date.
Restart task every	The interval between snapshots, in minutes. For example, if the interval is 360 minutes and you schedule a snapshot start time of 12 P.M. and an end time of 7 P.M, the snapshot occurs twice. If no interval is specified the snapshot occurs once.
Every	Enable the Every option to have the snapshot schedule continue to occur. Otherwise the schedule applies only for one day. Specify the number of days before restarting the snapshot schedule. For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.
Start On	If you enable the Every option, specify the starting date.
Pre Command	Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.
Post Command	Optionally, specify the full path of a command script to run after the snapshot is complete.

7 To specify run days for the schedule, make selections on the following tabs:

Days of Week	<p>Select one or more days on one or more weeks of the month.</p> <p>You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row.</p> <p>For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.</p>
Days of Month	<p>Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.</p>
Specific Dates	<p>Select one or more specific dates to include in or to exclude from the schedule.</p> <p>Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.</p>

If two schedules overlap for the same snapshot set, only one snapshot is taken. For example, if you select every Thursday plus the last day of the month, and the last day of the month occurs on Thursday, only one snapshot is taken on Thursday.

- 8 Click Next.
- 9 Review the snapshot set and schedule details and click Finish.

Displaying the status of the scheduled VSS COW snapshot

If a scheduled snapshot fails for some reason, the scheduler process will attempt to rerun it. You may want to verify that scheduled snapshots completed successfully. From the VEA console, you can view snapshot results.

To view a scheduled snapshot status

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node and the Storage Agent node.
- 3 Click **Scheduled Tasks** to view all the applications that have schedules.

- 4 Select the application for which you scheduled the snapshot. The scheduled snapshots are listed in the pane on the right.
If you have just configured the schedules and they are not yet displayed, right-click the Storage Agent node and click **Refresh** to update the display.
- 5 Choose one of the following:
 - To view the status of all scheduled jobs, right-click the selected application and click **All Job History**.
 - To view the status of a particular schedule, right-click the snapshot schedule name and click **Job History**.
- 6 In the Job History dialog box, view the schedule information.
You can sort listed schedules by clicking the column headings. The Status column shows if the snapshot completed successfully.

Note: All scheduled snapshots associated with Exchange are displayed under the Exchange node.

Deleting a schedule for a VSS COW Snapshot

The following is the procedure to delete a schedule.

Note: You cannot modify a schedule that has expired.

You can also delete (but not modify) a schedule from the VEA console.

Note: The VEA can delete snapshot schedules only; it does not delete mirror preparation scheduled with the Quick Recovery Configuration Wizard. In addition, deleting a snapshot schedule using the VEA does not update template settings created with the Quick Recovery Configuration Wizard.

To delete a schedule from the VEA

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the **System** node and **StorageAgent** node. Select and click to expand the **Scheduled Tasks > Exchange** node.
The scheduled snapshots are listed on the right pane.
- 3 Right-click the name of the snapshot schedule and select **Delete Schedule**.

Using the VSS COW snapshot wizards with Microsoft SQL

SFW provides support for taking VSS COW snapshots of Microsoft SQL databases. FlashSnap integrates with the Microsoft Volume Shadow Copy Service (VSS) to allow snapshots to be taken of all volumes associated with an SQL database without taking the database offline. The VSS COW Snapshot wizard uses VSS to take snapshots of the database. The VSS process allows the database to be quiesced before the snapshot operation and reactivates it immediately after.

SFW also provides a VSS COW Snapshot Scheduler wizard that can be used as an alternative to the VSS COW Snapshot wizard. It enables you to set up a schedule for taking the snapshots. The schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background.

Using the VSS COW Snapshot wizard

Creating a snapshot is a two-step process. The first step, create a shadow storage area for the snapshot, creates a differences area to store blocks of data before they are changed. The second step uses the VSS Snapshot wizard to create on-host snapshot volumes as well as an XML file to store the database and snapshot volume metadata. The VSS Snapshot wizard integrates with VSS to quiesce the database and then simultaneously snapshot the volumes in the database. This snapshot is done while the database is online and without disrupting processing.

Note: Note: You must create a shadow storage area before running the VSS COW Snapshot wizard.

Note: After performing COW related operations with the Windows GUI, the VEA GUI may not be updated to reflect the results of the operation. Use the VSS Refresh command to update the VEA GUI.

Creating the snapshot set

The following is the procedure to create a snapshot set.

To create the snapshot set

- 1 From the VEA console, navigate to the system where the production volumes are located.

- 2 Expand the system node, the Storage Agent node, Applications node, and SQL node.
- 3 Right-click the SQL instance node and click VSSCOWSnapshot.
- 4 In the wizard, review the Welcome page and click Next.
- 5 Specify the snapshot set parameters as follows and then click Next:

Select Component for snapshot operation Select the database for the snapshot set.

Directory The wizard creates the snapshot set metadataXMLfile. The XML metadata file is stored by default in the directory shown on the screen.

There are two ways to change the XML file location. First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named redirect.txt. This text file should contain a single text line specifying the full path to the location of the XML file, for example, G:\BackupSets. Save the redirect.txt file in the default directory C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML. If SFW/SFW HA is installed on the D drive, then the path will be the same as above, but on the D drive.

Snapshot set Enter a name for the snapshot set, for example, billing or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, identification number, date, and time.

Select the snapshot type. Select the snapshot type. You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a database. However, if you want to replay logs in SQL Server as part of restoring a database, a Full backup needs to have been created earlier. When replaying logs, you can replay from the time of the last Full backup. A Copy backup does not affect this sequence of log replay and therefore is often used as an "out of band" copy for purposes such as testing or data mining.

- 6 Review the specifications of the snapshot set and click Finish.

Using the VSS COW Snapshot Scheduler wizard

You can use the VSS COW Snapshot Scheduler wizard to add a snapshot schedule.

The scheduling capability automates the process of taking snapshots. At the scheduled time, the specified volumes are automatically snapshotted. Once configured and applied, the schedule is maintained by a scheduler service, VxSchedService.exe, that runs in the background. In a clustered server environment, ensure that the scheduler service is configured on each node with domain administrator privileges so that any node in the cluster can run the schedule after a failover.

Note: Information about the operations performed by the schedule can be found by expanding the nodes under the Scheduled Tasks node in the tree-view of the GUI. Expand the appropriate application node to locate the schedules for that application. Right-click the node and select JobHistory to view information about the operations performed by the schedule.

Note: You must create a shadow storage area before running the VSS COW Snapshot wizard.

To schedule a snapshot for a selected component

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node, the Storage Agent node, Applications node, and SQL node.
- 3 Right-click the SQL instance, and click Schedule VSSCOWSnapshot.
- 4 In the Welcome panel, review the information and click Next.
- 5 Specify the snapshot set parameters as follows and then click Next:

Select component for snapshot operation Select the database for the snapshot set.

Directory	<p>The XML file is stored by default in the directory shown on the screen.</p> <p>In a clustered server environment, the XML file must be saved on shared storage to be available from all nodes in the cluster.</p> <p>There are two ways to change the XML file location.</p> <p>First, edit the directory path in the Directory field for this wizard screen. Second, change the XML file location. Use a text editor to create a text file named <code>redirect.txt</code>. This text file should contain a single text line specifying the full path to the location of the XML file, for example, <code>G:\BackupSets</code>. Save the <code>redirect.txt</code> file in the default directory <code>C:\Program Files\Veritas\Veritas Volume Manager 5.1\VSSXML</code>.</p> <p>If SFW/SFW HA is installed on the D drive, then the path will be the same as above, but on the D drive.</p> <p>Note: When a COW snapshot is scheduled, a snapshot is taken at the specified time and a new xml file is generated for each snapshot.</p>
Snapshot set	<p>Enter a name for the snapshot set, for example, <code>billing</code> or accept the default name. The wizard generates a default snapshot set name that includes the term "SnapshotSet", component name, identification number, date, and time.</p>
Select snapshot type	<p>Select the snapshot type.</p> <p>You can specify that snapshots be created as either a Full backup or Copy backup type. Either type can be used to restore a database. However, if you want to replay logs in SQL Server as part of restoring a database, a Full backup needs to have been created earlier. When replaying logs, you can replay from the time of the last Full backup. A Copy backup does not affect this sequence of log replay and therefore is often used as an "out of band" copy for purposes such as testing or data mining.</p>

- 6 In the Schedule Information panel, on the General Options tab, specify the following:

Name of this schedule	<p>Enter a unique name for the snapshot set schedule.</p> <p>This name identifies the snapshot schedule if you later want to view information about the snapshot status. A default name consists of the application name, the component name and a numbered suffix that increments with each schedule.</p>
Description of this schedule	<p>Optionally, enter a description to help you identify the schedule when you view information about the snapshot status.</p>
Start Time	<p>The time of the day to begin taking snapshots.</p>
End Time	<p>The time of day to end taking snapshots.</p> <p>If a snapshot is in progress it is completed but a new one is not started after the end time.</p>
Schedule takes effect on	<p>The date on which the specified schedule takes effect. The default is the current date.</p>
Restart task every	<p>The interval between snapshots, in minutes.</p> <p>For example, if the interval is 360 minutes and you schedule a snapshot start time of 12 P.M. and an end time of 7 P.M, the snapshot occurs twice. If no interval is specified the snapshot occurs once.</p>
Every	<p>Enable the Every option to have the snapshot schedule continue to occur. Otherwise the schedule applies only for one day.</p> <p>Specify the number of days before restarting the snapshot schedule.</p> <p>For example, 1 day would mean the schedule takes effect daily, 2 days would mean every other day.</p>
Start On	<p>If you enable the Every option, specify the starting date.</p>
If you enable the Every option, specify the starting date.	<p>Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.</p>
Post Command	<p>Optionally, specify the full path of a command script to run before the scheduled snapshot occurs.</p>

7 To specify run days for the schedule, make selections on the following tabs:

Days of Week	<p>Select one or more days on one or more weeks of the month.</p> <p>You can click a button at the top of the column to select the entire column or a button to the left of a row to select the entire row. For example, clicking First schedules the snapshots to occur on the first occurrence of all the week days for the month.</p>
Days of Month	<p>Select one or more days of the month. You can also check the Last Day checkbox to schedule the snapshot for the last day of each month.</p>
Specific Dates	<p>Select one or more specific dates to include in or to exclude from the schedule.</p> <p>Excluding a date takes precedence over days scheduled on the other tabs. For example, if you schedule every Monday on the Days of Week tab, and you exclude Monday October 9 on the Specific Dates tab, the snapshots are not taken on October 9.</p>

If two schedules overlap for the same snapshot set, only one snapshot is taken. For example, if you select every Thursday plus the last day of the month, and the last day of the month occurs on Thursday, only one snapshot is taken on Thursday.

- 8 Click **Next**.
- 9 Review the snapshot set and schedule details and click **Finish**.

Displaying the status of the scheduled VSS COW snapshot

If a scheduled snapshot fails for some reason, the scheduler process will attempt to rerun it. You may want to verify that scheduled snapshots completed successfully. From the VEA console, you can view snapshot results.

To view a scheduled snapshot status

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the system node and the Storage Agent node.
- 3 Click **Scheduled Tasks** to view all the applications that have schedules.
- 4 Select the application for which you scheduled the snapshot. The scheduled snapshots are listed in the pane on the right.

If you have just configured the schedules and they are not yet displayed, right-click the Storage Agent node and click **Refresh** to update the display.

- 5 Choose one of the following:
 - To view the status of all scheduled jobs, right-click the selected application and click **All Job History**.
 - To view the status of a particular schedule, right-click the snapshot schedule name and click **Job History**.
- 6 In the Job History dialog box, view the schedule information. You can sort listed schedules by clicking the column headings. The Status column shows if the snapshot completed successfully.

Note: All scheduled snapshots associated with SQL are displayed under the SQL node.

Deleting a schedule for a VSS COW snapshot

The following is the procedure to delete a schedule.

Note: You cannot modify a schedule that has expired.

You can also delete (but not modify) a schedule from the VEA console.

Note: The VEA can delete snapshot schedules only; it does not delete mirror preparation scheduled with the Quick Recovery Configuration Wizard. In addition, deleting a snapshot schedule using the VEA does not update template settings created with the Quick Recovery Configuration Wizard.

To delete a schedule from the VEA

- 1 From the VEA console, navigate to the system where the production volumes and snapshot mirrors are located.
- 2 Expand the **System** node and **StorageAgent** node. Select and click to expand the **Scheduled Tasks > Exchange** node. The scheduled snapshots are listed on the right pane.
- 3 Right-click the name of the snapshot schedule and select **Delete Schedule**.

Dynamic multi-pathing software

- [Dynamic multi-pathing overview](#)
- [DMP DSMs](#)

Dynamic multi-pathing overview

This section provides a general overview of the Veritas Dynamic Multi-pathing software option.

This section covers the following topics:

- [About dynamic multi-pathing](#)
- [Major features of dynamic multi-pathing](#)
- [Active/Active and Active/Passive settings](#)
- [Active/Active and Active/Passive settings in a cluster environment](#)

For information on installing Veritas Dynamic Multi-pathing, refer to the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

About dynamic multi-pathing

The Veritas Dynamic Multi-pathing option adds additional fault tolerance to disk storage by making use of multiple paths between a computer and a disk in a storage array. A path is a connection between the computer and the storage array's disks and consists of a host adapter and a SCSI bus connection to one or more SCSI disks or a fiber optic channel connected to a hub, switch, or array. Thus, multiple paths are made possible by connecting two or more host bus adapters with either SCSI or fiber optic cabling to the storage array. The Dynamic Multi-pathing software manages the multiple paths so that the data on each of the array's disks is accessible to the host computer. If a path to a disk fails, Dynamic Multi-pathing automatically transmits data to and from the disk over an alternate path.

The paths on an array are set up to work in two ways—either in Active/Active mode, which provides load balancing of the data between multiple paths, or in Active/Passive mode, in which only one path is active and any remaining paths are backups.

SFW offers Dynamic Multi-pathing as DMP DSMs (DMP Device Specific Modules).

DMP DSMs are designed to support a multipath disk storage environment set up with the Microsoft multipath input/output (Microsoft MPIO) solution. DMP DSMs work effectively with Windows to provide a fault tolerant multipath disk storage environment. DMP DSMs have the following benefits:

- Windows Server 2003 and Windows Server 2008 support (32-bit, x64, and IA64)
- Fiber Channel StorPort Miniport HBA Driver support

- iSCSI HBA support
- Microsoft iSCSI Software Initiator support
- Boot from SAN support
- Active/Active Dynamic Multi-pathing with clustering support
- DMP DSMs load balancing support
 - Dynamic Least Queue Depth load balancing support
 - Round Robin with Subset load balancing support
 - Least Blocks load balancing support
 - Weighted Paths load balancing support
 - Balanced Path load balancing support

Basic disks are supported if SCSI-3 registry support is not enabled for DMP DSMs. If SCSI-3 registry is enabled for DMP DSMs for an attached array, then existing basic disks should be upgraded to dynamic disks before placing them under control of DMP DSMs. For DMP DSMs, Boot and data volumes are supported on the same bus/HBAs for non-clustered servers if the Boot from SAN recommendations from Microsoft are followed. DMP DSMs are not supported with fibre channel port drivers, fibre channel SCSI Miniport drivers or boot/cluster disks on the same bus/HBAs.

Major features of dynamic multi-pathing

The major features of Dynamic Multi-pathing are the following:

- **Fault tolerance**
Provides fault tolerance to a disk system by using multiple paths to each disk. If the primary path fails, either at the card level or in the cabling from the card to the disk, a secondary path is automatically utilized.
- **Load balancing in Active/Active configurations**
When a system is configured as Active/Active, Dynamic Multi-pathing makes use of all the paths to a disk for the transfer of I/O to and from the disk.
- **Support for multiple paths**
With DMP DSMs, the maximum number of I/O paths you can have is 16.
- **Dynamic recovery**
If an active path to a disk fails, Dynamic Multi-pathing automatically flags the failed path and no longer attempts to transfer data on it. The failed path is monitored and is automatically restored to service when Dynamic Multi-pathing detects that the path is functioning correctly. Dynamic Multi-pathing automatically updates path status on the user display when a path fails or is restored to service.
- **Dynamic path recognition**
If you add a new path to your Dynamic Multi-pathing configuration, running a rescan or rebooting your system causes Dynamic Multi-pathing to detect the new path and display its status. If a failed or disabled path is restored to service, Dynamic Multi-pathing automatically detects the status change and updates the display.

Active/Active and Active/Passive settings

Dynamic Multi-pathing has two modes of operation for an array's paths, Active/Active and Active/Passive.

These modes also apply to the array's disks and are defined as follows:

■ **Active/Active**

The mode in which Dynamic Multi-pathing allocates the data transfer across all the possible paths, thus enabling the desirable feature of load balancing. With this mode, Dynamic Multi-pathing implements a round-robin algorithm, selecting each path in sequence for each successive data transfer to or from a disk. For example, if you have two paths active, A and B, the first disk transfer occurs on path A, the next on path B, and the next on path A again.

In addition to the round-robin algorithm, DMP DSMs offer the following load balancing options:

■ **Dynamic Least Queue Depth**

Selects the path with the least number of I/O requests in its queue for the next data transfer.

For example, if you have two active paths, path A with one I/O request and path B with none, DMP DSMs would select the path with the least number of I/O requests in its queue, path B, for the next data transfer.

■ **Balanced Path**

This policy is designed to optimize the use of caching in disk drives and RAID controllers. The size of the cache depends on the characteristics of the particular hardware. Generally, disks and LUNs are logically divided into a number of regions or partitions. I/O to and from a given region is sent on only one of the active paths. Adjusting the region size to be compatible with the size of the cache is beneficial so that all the contiguous blocks of I/O to that region use the same active path. The value of the partition size can be changed by adjusting the value of the tunable parameter, Block Shift.

Block Shift represents the number of contiguous I/O blocks that are sent along a path to an Active/Active array before switching to the next available path. The Block Shift value is expressed as the integer exponent of a power of 2. For example, the Block Shift value of 11 represents 2^{11} or 2048 contiguous blocks of I/O.

The benefit of this policy is lost if the value is set larger than the cache size. The benefit is also lost when the active path fails. In this situation, the I/O is automatically redistributed across the remaining paths.

The default value of the Block Shift parameter is set to 11 so that 2048 blocks (1MB) of contiguous I/O are sent over a path before switching to

a different path. Depending on your hardware, adjusting this parameter may result in better I/O throughput. Refer to your hardware documentation for more information.

Note: Block Shift only affects the behavior of the balanced path policy. A value of 0 disables multipathing for the policy unless the `vxdmadm` command is used to specify a different partition size for an array.

- **Weighted Paths**

Uses the path with the lowest numerical weight. Each path is assigned a weight by the user to designate which path is favored for data transfer. If two or more paths have the same weight and are the lowest weight of all paths, then these paths are used each in turn, in round-robin fashion, for the data transfer.

For example, if you have three active paths, path A with weight of 0, path B with weight of 0, and path C with weight of 9, DMP DSMs would use path A for one data transfer and then use path B for the next. Path C is in standby mode and is used if path A or path B fails.

- **Round Robin with Subset**

Uses a subset of paths, each in turn, in round-robin fashion. The user specifies the paths for data transfer that make up the subset. The remaining paths are in standby mode.

For example, if you have three active paths, path A, path B, and path C and you specify the subset to contain path A and path B, then DMP DSMs would use path A for one data transfer and then use path B for the next. Path C is in standby mode and is used if path A or path B fails.

- **Least Blocks**

Selects the path with the least number of blocks of I/O in its queue for the next data transfer.

For example, if you have two active paths, path A with one block of I/O and path B with none, DMP DSMs would select the path with the least number of blocks of I/O in its queue, path B, for the next data transfer.

- **Active/Passive**

A mode in which a path designated as the “Preferred Path” or “Primary Path” is always active and the other path or paths act as backups (standby paths) that are called into service if the current operating path fails.

The modes of operation—Active/Active and Active/Passive—are shown as options in the Load Balancing section of the program’s Array Settings and Device Settings windows. The Active/Active mode enables load balancing, but the Active/Passive mode does not provide load balancing.

Note: If a storage array cannot transfer data on one of the path configurations, the Load Balancing options appear grayed out on the screen and you cannot access these settings.

You configure the load balancing settings for the paths at the array level through the Array Settings screen, or you can accept the default setting. The default setting is dependent on the particular array. Consult the documentation for your storage array to determine the default setting of the array and any additional settings it supports.

After the appropriate array setting is made, all the disks in an array have the same load balancing setting as the array. If the array is set to Active/Active, you can use the Device Settings screen to change the setting on an individual disk so that it has a different load balancing setting than the array. When an array is set to Active/Passive, no load balancing is enabled and data transfer is limited to the one preferred or primary path only.

Note: If you are using a demo license to try out Dynamic Multi-pathing, please refer to the section "[When a dynamic multi-pathing license is no longer valid](#)" on page 508.

Active/Active and Active/Passive settings in a cluster environment

This section covers information about settings for DMP DSMs along with information about enabling or disabling SCSI-3 PGR.

DMP DSMs

For DMP DSMs in a cluster environment, either Active/Active or Active/Passive load balance settings can be used. DMP DSMs automatically set the load balancing to Active/Passive for disks under SCSI-2 reservation. For Active/Active load balancing in a cluster environment, the array must be enabled for SCSI-3 Persistent Group Reservations (SCSI-3 PGR).

Note: Veritas maintains a Hardware Compatibility List (HCL) for Veritas Storage Foundation & High Availability Solutions 5.1 for Windows Products on the Symantec Support web site. The HCL gives information on HBAs, firmware, and switches that have been tested with each supported array. Check the HCL for details about your hardware before using DMP DSMs.

Note: Storage arrays may require additional configuration steps or updates to work with Veritas Storage Foundation for Windows and MPIO. Contact the manufacturer of the storage array for details.

SCSI-3 PGR technology

SCSI-3 PGR supports multiple nodes accessing a device while at the same time blocking access to other nodes. SCSI-3 PGR supports multiple paths from a host to a disk and SCSI-3 PGR reservations are persistent across SCSI bus resets.

By contrast, SCSI-2 reservations can only be used by one host, with one path. This means if there is a need to block access for data integrity concerns, only one host and one path remain active. This limits access to the device to only one path and prevents the use of multiple paths even if they are available.

SCSI-3 PGR uses a concept of registration and reservation. Systems accessing a device register a key with a SCSI-3 device. Each system registers its own key. Multiple systems registering keys form a membership. Registered systems can then establish a reservation. The reservation type is set to "Exclusive Access - Registrants Only". This means that only some commands are allowed and there is only one persistent reservation holder. With SCSI-3 PGR technology, blocking write access can be done by removing a registration from a device.

In the Veritas Storage Foundation for Windows implementation, a node registers the same key for all paths to the device.

For DMP DSMs, the Active/Active setting is implemented by translating SCSI reserve/release commands to SCSI-3 PGR commands.

Enabling SCSI-3 PGR

You must enable SCSI-3 PGR before using the Active/Active setting for DMP DSMs. (SCSI-3 PGR is disabled by default.)

The files in the following table are provided to enable or disable SCSI-3 PGR for the type of storage array supported. The files are located on the product CD at `..\Tools\storage_foundation_for_windows\DMP_DSM_SCSI3_reg`

Copy the files to your system and run the appropriate `.reg` for your storage array.

Note: You must ensure that your storage array supports SCSI-3 PGR before using the Active/Active setting for DMP DSMs. Also check to see if your array manufacturer requires any special settings for a LUN to be enabled for SCSI-3 PGR.

Table 13-1 Files to Enable/Disable SCSI-3 PGR

Array Type	Enable SCSI-3 PGR	Disable SCSI-3 PGR
<ul style="list-style-type: none"> ■ EMC Symmetrix 8000 Series ■ EMC Symmetrix DMX Series 	EnableSupportSCSI3EMC.reg	DisableSupportSCSI3EMC.reg
<ul style="list-style-type: none"> ■ IBM TotalStorage™ ESS800/ESS750 ■ IBM TotalStorage™ DS8000 	EnableSupportSCSI3IBMDS.reg	DisableSupportSCSI3IBMDS.reg

Table 13-1 Files to Enable/Disable SCSI-3 PGR

Array Type	Enable SCSI-3 PGR	Disable SCSI-3 PGR
<ul style="list-style-type: none"> ■ Hitachi TagmaStore Universal Storage Platform (USP100, USP600, and USP1100) ■ Hitachi TagmaStore Network Storage Controller (NSC55) ■ Hitachi TagmaStore Adaptable Modular Storage (AMS200 and AMS500) ■ Hitachi TagmaStore Workgroup Modular Storage (WMS100) ■ Hitachi Hitachi 9900 Lightning Series (9900 and 9900V) ■ Sun StorEdge SE9900 Series (SE9910, SE9960, SE9970V, SE9980V, and SE9990) 	EnableSupportSCSI3HDS.reg	DisableSupportSCSI3HDS.reg
<ul style="list-style-type: none"> ■ HP StorageWorks XP128 Disk Array ■ HP StorageWorks XP1024 Disk Array ■ HP StorageWorks XP10000/XP12000 Disk Array 	EnableSupportSCSI3HPXP.reg	DisableSupportSCSI3HPXP.reg

Table 13-1 Files to Enable/Disable SCSI-3 PGR

Array Type	Enable SCSI-3 PGR	Disable SCSI-3 PGR
<ul style="list-style-type: none"> ■ HP StorageWorks Enterprise Virtual Array (EVA4000, EVA6000, and EVA8000) 	EnableSupportSCSI3HPEVA.reg	DisableSupportSCSI3HPEVA.reg
<ul style="list-style-type: none"> ■ Network Appliance F800 Series ■ Network Appliance FAS200 Series (FAS250 and FAS270) ■ Network Appliance FAS900 Series (FAS920, FAS940, FAS960, and FAS980) ■ Network Appliance FAS3000 Series (FAS3020 and FAS3050) ■ Network Appliance NearStore Series ■ NetApp V-Series (GF980c, GF960c, V3050c, V3020c, and GF270c) <p>Note: The only Network Appliance arrays that are supported are those that are configured as an Active/Active hardware type (cfmode: standby for each Network Appliance filer).</p>	EnableSupportSCSI3NETAPP.reg	DisableSupportSCSI3NETAPP.reg

DMP DSMs

This section describes support for the Microsoft multipath input/output solution (Microsoft MPIO). The support is provided by Veritas DMP DSMs.

This section covers the following topics:

- [DMP DSMs menus](#)
- [Add and remove paths](#)
- [Specify load balancing settings and the primary path](#)
- [View array, disk, and path status](#)

DMP DSMs menus

This section on DMP DSMs menus has the following topics:

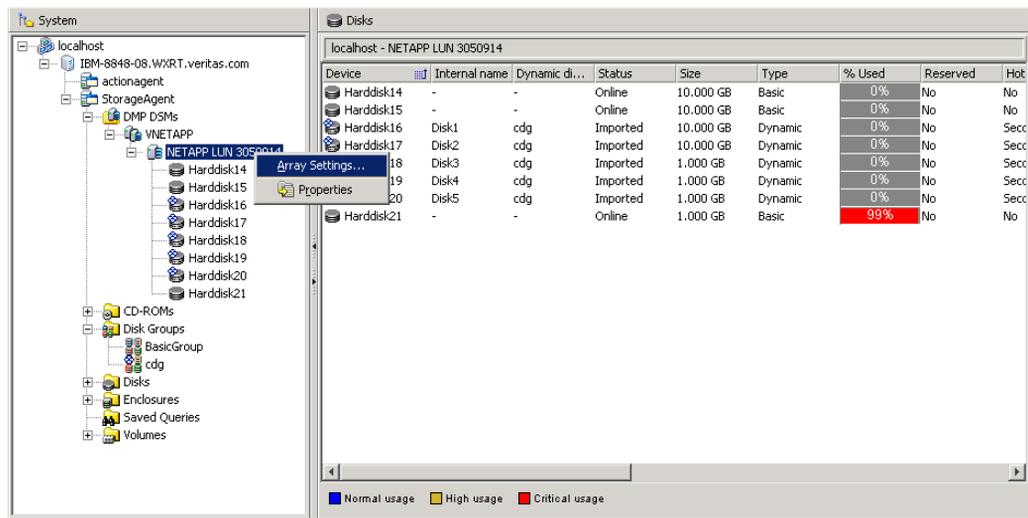
- [Displaying the menu for arrays](#)
- [Commands for arrays](#)
- [Displaying the menu for disks](#)
- [Commands for paths of a disk](#)

Displaying the menu for arrays

There is a context menu for arrays that are under the control of DMP DSMs that allow you to access the settings and properties of the array. It is available when you select an array in the tree view of the left pane of the VEA GUI.

To display the menu for arrays

- 1 Open the DMP DSMs folder in the tree view.
- 2 Right-click the array that you are interested in and the array context menu appears.



Commands for arrays

This section describes the DMP DSMs menu commands.

The menu commands are the following:

- [Array settings](#)
- [Properties](#)

Array settings

The **Array Settings** command launches the Array Settings wizard.

It allows you to select the setting for the operational modes for the array's paths in the Load Balance Policy section. The Control Timer Settings is a section of tunable parameters for testing the status or health of a path.

At the bottom of the screen there is an option for applying all the settings to all the arrays under control of DMP DSMs. This option applies all the settings to all arrays under control of a specific DMP DSMs driver. When you select this option, the current settings for this array are applied to all the arrays controlled by this specific DMP DSMs driver.

Note: There are specific DMP DSMs that work with specific families of hardware arrays. If your environment has more than one family of hardware arrays under control of DMP DSMs, then each family of hardware arrays would work with specific DMP DSMs. When you select the option for applying all the settings to all the arrays under control of the DSM, you are applying the settings to only those arrays that work with that specific DMP DSMs.

See <http://www.symantec.com/business/support/index.jsp> for more information about which hardware arrays are supported by a specific DMP DSMs.

For additional information about array settings, see "[Array status](#)" on page 747.

Note: If the Fail Over Only (Active/Passive) array load balancing setting is selected and a Primary Path has not been set, DMP DSMs set the Primary Path. Generally, DMP DSMs set the Primary Path to the first path that is able to transfer data. You can manually set the Primary Path with the **Set Primary Path** command.

Properties

The **Properties** command brings up the Properties screen, which displays information about the selected array, including array name, array type, load balance policy, and a list of the devices contained in the array.

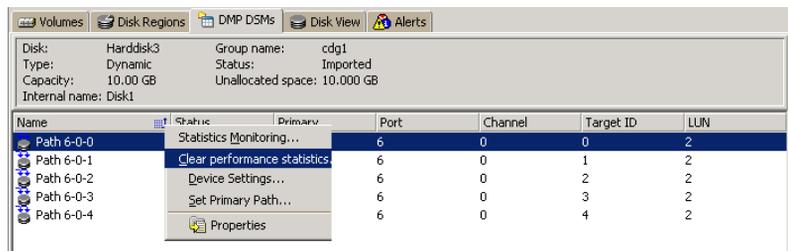
For additional information, see “[Path status](#)” on page 750.

Displaying the menu for disks

The context menu for a disk is available when you highlight a path that is connected to the disk. The menu requires the DMP DSMs tab to be active.

To display the disk context menu

- 1 Open the DMP DSMs folder in the tree view.
- 2 Select the disk that you are interested in.
Note that opening the Disks folder and clicking a disk that is under DMP DSMs control is an alternative way to select a disk.
- 3 Select the DMP DSMs tab in the right pane. This tab displays the paths to the selected disk.
Each path is displayed with its properties. Some of the attributes displayed are Port, Channel, Target ID, LUN, and Load Balance Policy.
The name of the path is derived from a combination of properties of the path. For example, if the path has properties of Port Number = 2, Channel = 1, and Target ID = 1, then the name of the path is 2-1-1.
- 4 Right-click on a path and the context menu appears.



Commands for paths of a disk

This section describes the DMP DSMs menu commands.

The menu commands are the following:

- [Statistics monitoring](#)

- [Clear performance statistics](#)
- [Device settings](#)
- [Set primary path](#)
- [Properties](#)

Statistics monitoring

The **Statistics Monitoring** command brings up the Path Statistics screen, which displays the I/O statistics of the selected path.

The I/O statistics for the selected path are the following:

- Number of read operations per second
- Number of write operations per second
- Number of bytes read per second
- Number of bytes written per second

The statistics are updated and displayed at a specified polling interval. The range of values for the polling interval is 2 to 900 seconds. You can set the polling interval by entering the number of seconds in the Polling Interval field and clicking **Set Polling Interval**.

Clear performance statistics

The **Clear Performance Statistics** command brings up the Clear Performance Statistics screen, which allows you to clear the performance statistics that are being monitored for a single device, an array, or for all the arrays under control of a DMP DSMs. After selecting which performance statistics to clear, click **OK** to complete the operation.

Device settings

The **Device Settings** command brings up the Device Settings screen, which displays the DMP DSMs characteristics of the disk whose path is selected on the DMP DSMs tab. It has a Load Balance Policy section to set the operational mode that applies to the selected disk.

See “[Device status](#)” on page 748.

Note: If the Fail Over Only (Active/Passive) device load balancing setting is selected and a Primary Path has not been set, DMP DSMs set the Primary Path. Generally, DMP DSMs set the Primary Path to the first path that is able to transfer data. You can manually set the Primary Path with the **Set Primary Path** command.

Set primary path

The **Set Primary Path** command on the DMP DSMs menu can be used to specify the currently selected path as the Primary Path to the disk, array, or all arrays under control of the DSM.

The following options are available:

- Set Primary Path for device

This menu option is available only when the operational mode for the path to the disk is specified as Fail Over Only (Active/Passive) and the currently selected path is not the Primary Path. The Primary Path is the only path that is used to transfer data to and from the disk. Clicking this menu selection makes the selected path the Primary Path to the disk.

See “[Specifying the primary path for an array or disk](#)” on page 742.

- Set Primary Path for array

This allows you to specify the currently selected path as the Primary Path to the array. The Primary Path is the only path that is used to transfer data to and from the array.

The array’s Primary Path can be set regardless of the array’s current load balance setting. This means that if a disk in the array is set to Fail Over Only (Active/Passive), the Primary Path for the array becomes the Primary Path for the disk. If the setting is set to any other load balance option, then the Primary Path setting for the array is not used. However, if a disk in the array is set to Fail Over Only (Active/Passive), the Primary Path for the array becomes the Primary Path for the disk.

For example, if an array has a load balance setting of Round Robin (Active/Active) and the Primary Path for the array is set to path 2-1-1, then any disk in the array that has the load balance setting of Fail Over Only (Active/Passive) will have its Primary Path set to path 2-1-1.

See “[Specifying the primary path for an array or disk](#)” on page 742.

- Set Primary Path for all arrays under control of the DSM

This applies the Primary Path setting to all the arrays under control of the DSM. Selecting this option means that the selected Primary Path is applied to all the arrays controlled by this specific DSM (DMP DSMs driver). Refer to your hardware array documentation for details on how your arrays may support this setting.

Note: There are specific DMP DSMs that work with specific families of hardware arrays. If your environment has more than one family of hardware arrays under control of DMP DSMs, then each family of hardware arrays would work with specific DMP DSMs. When you select the option for applying all the settings to all the arrays under control of the DSM, you are applying the settings to only those arrays that work with that specific DMP DSMs.

See <http://www.symantec.com/business/support/index.jsp> for more information about which hardware arrays are supported by a specific DMP DSMs.

Properties

The **Properties** command brings up the Properties screen, which displays information about the selected path, including path name, status, and SCSI address.

For additional information, see “[Path status](#)” on page 750.

Add and remove paths

This section describes how to add and remove paths.

After you have been using DMP DSMs for a while, you might want to add a path to an array if you are adding more disks to the array or if you want additional fault tolerance for the array by having another path. In addition, you may want to remove a path if you are reconfiguring your system.

This section covers the following topics:

- [Adding a path](#)
- [Removing a path](#)

Adding a path

You might want to add a path when you add more disks to an array or to increase fault tolerance for the array.

To add a path to an array

- 1 Add the path by physically connecting a new cable.
- 2 To view the screen changes caused by the additional path, open the Disks folder in the tree view and select a disk. Then select the DMP DSMs tab in the right-hand pane.
- 3 Select **Actions>Rescan** from the VEA menu.
DMP DSMs scans for paths and updates the screen, reflecting any changes you have made in the physical installation.

Removing a path

Remove a path by physically disconnecting the cable. The system monitors existing paths and detects that the disconnected path is no longer functioning properly. The SFW display is updated to indicate this, and data transfers fail over to the next path in the sequence.

Note: You may need to perform a rescan to update the screen after removing a path from an array that was under control of DMP DSMs. Select **Actions>Rescan** from the VEA menu to display the change you have made to the configuration.

Specify load balancing settings and the primary path

This section gives the step-by-step directions for specifying the load balancing settings for the paths in an array and for individual disks.

For a general discussion of these load balancing settings, see “[Active/Active and Active/Passive settings](#)” on page 721.

The Primary Path setting is only available when you select the Fail Over Only (Active/Passive) load balancing setting for an array or disk.

When you first set up an array under DMP DSMs, you must make sure you have the load balancing setting you want for the paths in the array. After that is done, all of the disks in the array by default have the same load balancing setting. Then, if desired, you can change this setting for individual disks. The load balancing settings are located in the Load Balance Policy section of the Array Settings wizard and the Device Settings screen.

All of the load balancing settings, except for Fail Over Only (Active/Passive), enable load balancing among the active paths. The Fail Over Only (Active/Passive) setting does not provide load balancing because data transfer only occurs on the one active path, the Primary Path.

Note: The type of array or disk determines which load balancing settings are available. Load balance settings that are not supported are grayed-out in the GUI. Refer to the documentation for your array or disk for more information about supported load balance settings.

This section covers the following topics:

- [Specifying load balancing settings for an array](#)
- [Specifying load balancing settings for a disk](#)
- [Specifying the primary path for an array or disk](#)

Specifying load balancing settings for an array

To specify load balancing settings for an array

- 1 To launch the Array Settings wizard, open the DMP DSMs folder in the tree view.
- 2 Right-click the array that you are interested in and the array context menu appears.
- 3 Select **Array Settings** from the context menu.
- 4 The Array Settings welcome screen appears. Click **Next** to continue.
- 5 The Select Array Settings parameters screen appears.

Select the load balancing option by clicking the appropriate radio button. SCSI-3 reservation support is required for all load balancing settings, except for Fail Over Only (Active/Passive). Refer to your array documentation to determine if your array supports SCSI-3 reservations before selecting any of these load balancing settings.

- **Round Robin (Active/Active)**

This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths in the array as active and I/O transfers occur on the paths each in turn, in a round-robin fashion.
- **Dynamic Least Queue Depth**

This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths to the array as active and selects the path with the least number of I/O requests in its queue for a data transfer.
- **Balanced Path**

This policy is designed to optimize the use of caching in disk drives and RAID controllers. The size of the cache depends on the characteristics of the particular hardware. Generally, disks and LUNs are logically divided into a number of regions or partitions. I/O to and from a given region is sent on only one of the active paths. Adjusting the region size to be compatible with the size of the cache is beneficial so that all the contiguous blocks of I/O to that region use the same active path. The value of the partition size can be changed by adjusting the value of the tunable parameter, Block Shift.

For more details about this option, see “[Active/Active and Active/Passive settings](#)” on page 721.
- **Weighted Paths**

This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths to the array as active and selects the path with the lowest weight for data transfer. Weights are assigned by the user to designate which path is favored. If two or more paths have the same weight and are the lowest weight of all paths, then these paths are used each in turn, in round-robin fashion, for the data transfer.
- **Round Robin with Subset**

This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths to the array as active and uses a subset of paths. These paths are used each in turn, in round-robin fashion, for data transfer. The subset of

paths are specified by the user. The remaining paths are in standby mode.

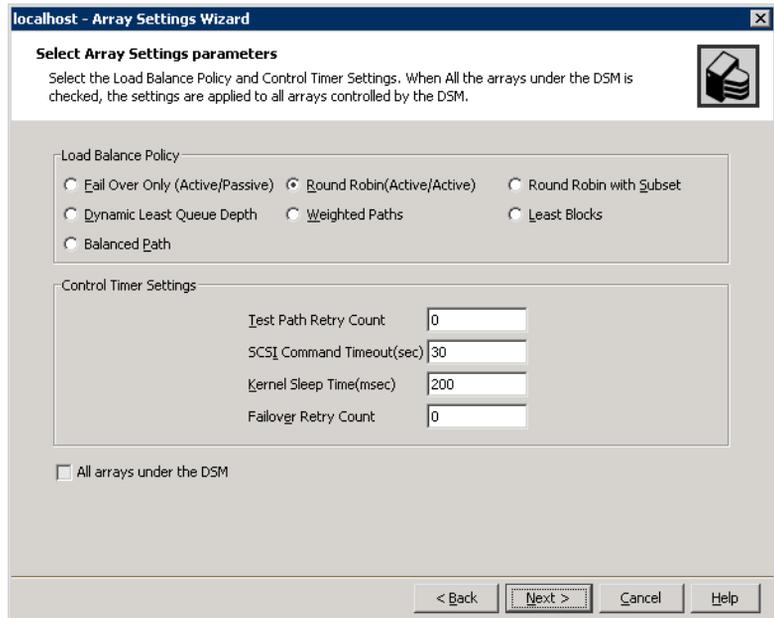
- **Least Blocks**
This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths to the array as active and selects the path with the least number of blocks of I/O in its queue for data transfer.
- **Fail Over Only (Active/Passive)**
This option has one Primary Path with the remaining path or paths on standby (backups) in case the primary path fails. The Primary Path is the only path that is used to transfer data. This option does not provide load balancing among paths. DMP DSMs sets a path to be the Primary Path. However, you may choose a specific path to be the Primary Path. See “[Specifying the primary path for an array or disk](#)” on page 742

If you want the selected load balancing setting to be the setting for all the arrays controlled by this specific DMP DSMs driver, check the checkbox for **All arrays under the DSM**. This option means that the current load balancing setting and the other settings for this array are applied to all the arrays controlled by this specific DMP DSMs driver.

There are specific DMP DSMs that work with specific families of hardware arrays. If your environment has more than one family of hardware arrays under control of DMP DSMs, then each family of hardware arrays would work with specific DMP DSMs. When you select the option for applying all the settings to all the arrays under control of the DSM, you are applying the settings to only those arrays that work with that specific DMP DSMs. See <http://www.symantec.com/business/support/index.jsp> for more information about which hardware arrays are supported by a specific DMP DSMs.

The default load balancing setting of an array is dependent on the particular array. Consult the documentation for your storage array to determine the default setting and any additional settings it supports.

In the sample screen shown below, the Round Robin (Active/Active) setting is selected.



Click **Next** to continue.

- 6 The Array Settings summary screen appears displaying the settings for the array. Review the settings and click **Finish** to apply the settings and exit the wizard.

For some load balance policies, such as Round Robin with Subset, additional specifications are required. The Array Settings wizard displays a screen before the summary screen to collect these specifications. Click **Next** after setting these specifications to continue to the summary screen.

Specifying load balancing settings for a disk

If a setting has not been specified for an individual disk, the disk assumes the same load balancing setting as the one used by the array. However, by using the Device Settings screen, you can change the load balancing option for an individual disk and make it different than the setting of the array.

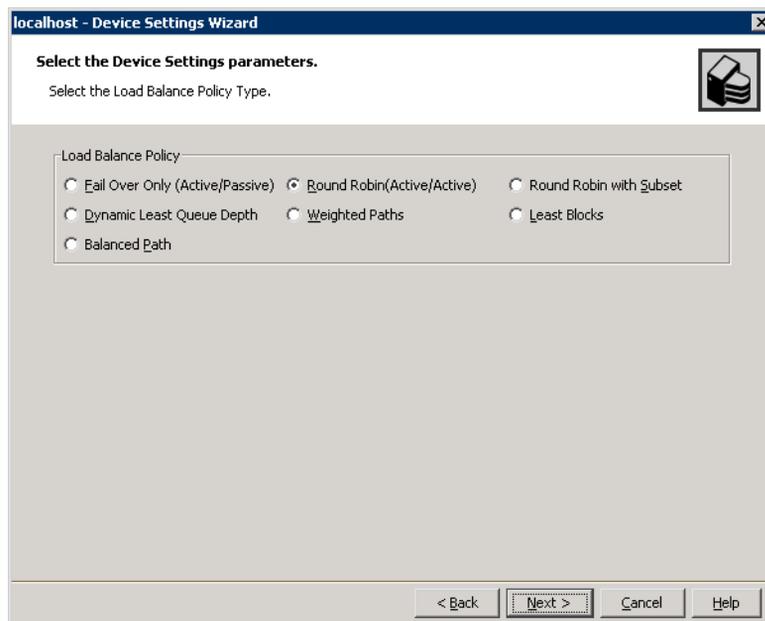
Note: DMP DSMs automatically set the load balancing to Fail Over Only (Active/Passive) for disks under SCSI-2 reservation. The Fail Over Only (Active/Passive) setting is always used on disks under SCSI-2 reservation and the system ignores other load balance settings that may be set.

Disks under SCSI-2 reservation are:

- Disks that may be in a clustering environment.
 - Disks with Private Disk Group Protection.
-

To specify load balancing settings for a disk

- 1 Open the DMP DSMs folder in the VEA console's tree view.
- 2 Select the disk that has the load balancing settings you want to change. Note that opening the Disks folder and clicking a disk that is under DMP DSMs control is an alternate way to select a disk.
- 3 Make sure the DMP DSMs tab is selected in the right pane, right-click one of the displayed paths, and then select **Device Settings** from the path context menu.
- 4 The Device Settings welcome screen appears. Click **Next** to continue.
- 5 The Select Device Settings parameters screen appears.



Select one of the load balancing options.

- **Round Robin (Active/Active)**

This option ensures that load balancing is used for data transfers to and from a disk. With this setting, DMP DSMs configures all paths to the disk as active and enables paths, each in turn, in a round-robin fashion for data transfer.
- **Dynamic Least Queue Depth**

This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths to the array as active and selects the path with the least number of I/O requests in its queue for a data transfer.
- **Balanced Path**

This policy is designed to optimize the use of caching in disk drives and RAID controllers. The size of the cache depends on the characteristics of the particular hardware. Generally, disks and LUNs are logically divided into a number of regions or partitions. I/O to and from a given region is sent on only one of the active paths. Adjusting the region size to be compatible with the size of the cache is beneficial so that all the contiguous blocks of I/O to that region use the same active path. The value of the partition size can be changed by adjusting the value of the tunable parameter, Block Shift.

For more details about this option, see [“Active/Active and Active/Passive settings”](#) on page 721.
- **Weighted Paths**

This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths to the array as active and selects the path with the lowest weight for data transfer. Weights are assigned by the user to designate which path is favored. If two or more paths have the same weight and are the lowest weight of all paths, then these paths are used each in turn, in round-robin fashion, for the data transfer.
- **Round Robin with Subset**

This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths to the array as active and uses a subset of paths each in turn, in round-robin fashion, for data transfer. The subset of paths are specified by the user. The remaining paths are in standby mode.
- **Least Blocks**

This option ensures that load balancing is used for data transfers to and from an array. With this setting, DMP DSMs configures all paths to

the array as active and selects the path with the least number of blocks of I/O in its queue for data transfer.

- **Fail Over Only (Active/Passive)**

This option has one Primary Path with the remaining path or paths on standby (backups) that are used when the current primary path fails. The Primary Path is the only path that is used to transfer data. This option does not provide load balancing among paths. DMP DSMs chooses a path to be the Primary Path. However, you may choose a specific path to be the Primary Path.

See “[Specifying the primary path for an array or disk](#)” on page 742.

Click **Next** to continue.

- 6 The Device Settings summary screen appears displaying the settings for the array. Review the settings and click **Finish** to apply the settings and exit the wizard.

For some load balance policies, such as Round Robin with Subset, additional specifications are required. The Array Settings wizard displays a screen before the summary screen to collect these specifications. Click **Next** after setting these specifications to continue to the summary screen.

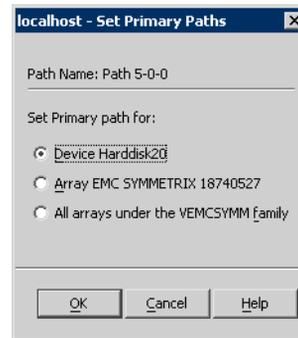
Specifying the primary path for an array or disk

When an array is configured for Fail Over Only (Active/Passive) operation, you can specify the path that is used for data transfer. The specified path, called the Primary Path, is the only path used for data transfer.

To specify the primary path for an array or disk

- 1 Display the Set Primary Path screen by doing the following:
 - Make sure the DMP DSMs tab is selected in the right pane.
To display the DMP DSMs tab, use the tree view in the left pane to select a disk under the DMP DSMs folder, or a disk under the Disks folder that has DMP DSMs enabled, and then click the DMP DSMs tab that appears in the right pane.
 - In the DMP DSMs tab, right-click on the path you want to be the Primary Path for the array, and select **Set Primary Path** from the path context menu.

The Set Primary Path screen appears.



- 2 Select the Primary Path for device, Primary Path for array, or Primary Path for all arrays under control of the DSM option, as follows.
 - Primary Path for device is available only when the operational mode for the path to the disk is specified as Fail Over Only (Active/Passive) and the currently selected path is not the Primary Path. The Primary Path is the only path that is used to transfer data to and from the disk. Clicking this menu selection makes the selected path the Primary Path to the disk. The other paths to the disk are placed on standby and available for failover.
 - Primary Path for array
This allows you to specify the currently selected path as the Primary Path to the array. The Primary Path is the only path that is used to transfer data to and from the array.
The array's Primary Path can be set regardless of the array's current load balance setting. This means that if the load balance setting for the array is set to Round Robin (Active/Active) or other active/active load balance setting, then the Primary Path setting for the array is not used. However, if a disk in the array is set to Fail Over Only (Active/Passive), the Primary Path for the array becomes the Primary Path for the disk. For example, if an array has a load balance setting of Round Robin (Active/Active) and the Primary Path for the array is set to path 2-1-1, then any disk in the array that has the load balance setting of Fail Over Only (Active/Passive) will have its Primary Path set to path 2-1-1.
 - Primary Path for all arrays under control of the DSM
This applies the Primary Path setting to all the arrays under control of the DSM. Selecting this option means that the selected Primary Path is applied to all the arrays controlled by this specific DSM (DMP DSMs driver). In the Set Array Primary Path screen above, this option displays the name of the DMP DSMs, VEMCSYMM.

Refer to your hardware array documentation for details on how your arrays may support this setting.

There are specific DMP DSMs that work with specific families of hardware arrays. If your environment has more than one family of hardware arrays under control of DMP DSMs, then each family of hardware arrays would work with specific DMP DSMs. When you select the option for applying all the settings to all the arrays under control of the DSM, you are applying the settings to only those arrays that work with that specific DMP DSMs.

See <http://www.symantec.com/business/support/index.jsp> for more information about which hardware arrays are supported by a specific DMP DSMs.

- 3 Click **OK** to save your setting and exit the screen.
The Primary Path is identified by a blue checkmark icon.

Specifying control timer settings for an array

Control Timer Settings for an array are a set of tunable parameters that affect the testing of a path's status or health.

To specify control timer settings for an array

- 1 To launch the Array Settings wizard, open the DMP DSMs folder in the tree view.
- 2 Right-click the array that you are interested in and the array context menu appears.
- 3 Select **Array Settings** from the path context menu.
- 4 The Array Settings welcome screen appears. Click **Next** to continue.
- 5 The Select Array Settings parameters screen appears.

localhost - Array Settings Wizard

Select Array Settings parameters

Select the Load Balance Policy and Control Timer Settings. When All the arrays under the DSM is checked, the settings are applied to all arrays controlled by the DSM.

Load Balance Policy

Fail Over Only (Active/Passive) Round Robin (Active/Active) Round Robin with Subset

Dynamic Least Queue Depth Weighted Paths Least Blocks

Balanced Path

Control Timer Settings

Test Path Retry Count

SCSI Command Timeout(sec)

Kernel Sleep Time(msec)

Failover Retry Count

All arrays under the DSM

Edit the values for the parameters and click **Next** to continue.

The Control Timer Settings parameters are as follows:

- **Test Path Retry Count** – The number of times DMP DSMs test a path to determine if it has recovered from an error condition. The default value is 0. The maximum value is 50.
- **SCSI Command Timeout** – The amount of time a SCSI command waits for a device to respond to it. The default value is 30 seconds. The maximum value is 120 seconds.

- **Kernel Sleep Time** – The interval of time the DMP DSMs kernel waits between attempts to recover a path from an error condition. The default value is 200 milliseconds. The maximum value is 10000 milliseconds.
 - **Failover Retry Count** – The number of times DMP DSMs attempt a failover to another path when the current path fails. The default value is 0. The maximum value is 50.
- 6 The Array Settings summary screen appears displaying the settings for the array. Review the settings and click Finish to apply the settings and exit the wizard.

For some load balance policies, such as Round Robin with Subset, additional specifications are required. The Array Settings wizard displays a screen before the summary screen to collect these specifications. Click **Next** after setting these specifications to continue to the summary screen.

View array, disk, and path status

DMP DSMs provide status information for arrays, disks, and paths to the disks. Status displays are accessed through the path context menu.

This section covers the following topics:

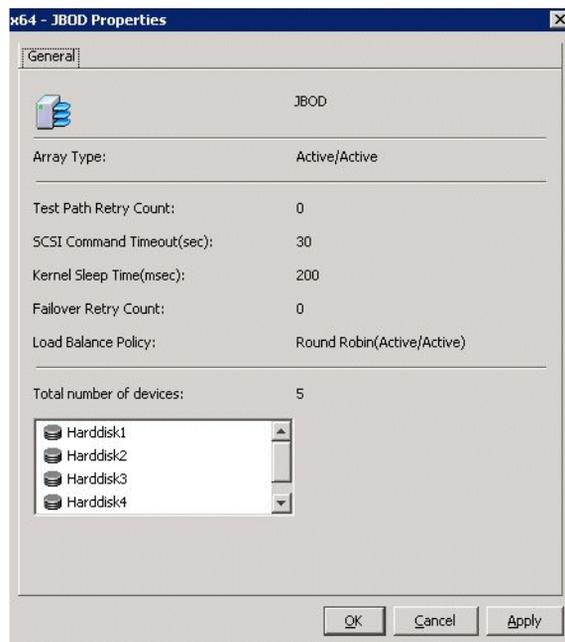
- [Array status](#)
- [Device status](#)
- [Path status](#)

Array status

To view array status

Display the Array Properties by doing the following:

- 1 Open the DMP DSMs folder in the tree view.
- 2 Right-click the array that you are interested in and the array context menu appears.
- 3 Select **Properties** from the context menu.
- 4 The Properties screen appears.



The Properties screen contains the following:

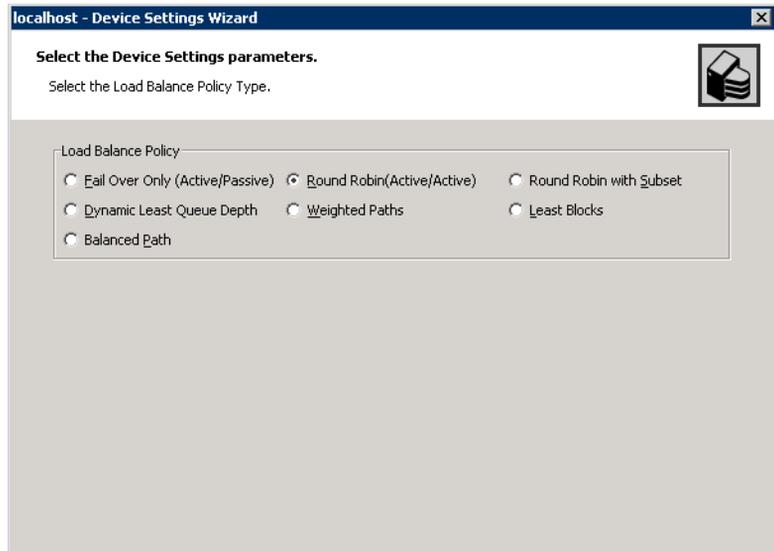
- **Array Name** – Displays the name of the array. The name is fixed by the array and is not user definable.
- **Array Type** – Displays the type of load balance policy in effect for the array.
- **Control Timer Settings** – A set of the following tunable parameters that affect the testing of a path’s status or health.
 - **Test Path Retry Count** – The number of times DMP DSMs test a path to determine if it has recovered from an error condition. The default value is 0. The maximum value is 50.
 - **SCSI Command Timeout** – The amount of time a SCSI command waits for a device to respond to it. The default value is 30 seconds. The maximum value is 120 seconds.
 - **Kernel Sleep Time** – The interval of time the DMP DSMs kernel waits between attempts to recover a path from an error condition. The default value is 200 milliseconds. The maximum value is 10 seconds.
 - **Failover Retry Count** – The number of times DMP DSMs attempt a failover to another path when the current path fails. The default value is 0. The maximum value is 50. Click **OK** to exit.
- **Load Balance Policy** – Displays the load balancing setting in effect. There is one option, Fail Over Only (Active/Passive), that does not provide load balancing. All other options provide load balancing. For option descriptions, see “[Active/Active and Active/Passive settings](#)” on page 721. For the procedure to specify settings, see “[Specifying load balancing settings for an array](#)” on page 736.
- **Devices in the Array** – Displays the number of disks in the array and lists them by name.

Device status

To view device status

- 1 In the tree view under the DMP DSMs folder, select a disk whose status you want to view.
- 2 In the right pane, click the DMP DSMs tab for the disk.
- 3 Right-click the path and select **Device Settings** from the path context menu that comes up.
- 4 The Device Settings welcome screen appears. Click **Next** to continue.

The Device Settings screen appears.



The Device Settings screen contains the setting for the **Load Balance Policy** for the disk.

Load Balance Policy – Indicates the setting in effect for the individual disk. The Fail Over Only (Active/Passive) option provides no load balancing. The other options provide load balancing.

For option descriptions, see “[Active/Active and Active/Passive settings](#)” on page 721.

For the procedure to specify settings, see “[Specifying load balancing settings for a disk](#)” on page 739

- 5 Click **Cancel** to exit.

Path status

To view path status

- 1 Make sure that the path you want to view the status for is displayed in the DMP DSMs tab in the right pane of the VEA console.
If the DMP DSMs tab is not showing, select a disk that uses that path in the tree view under the Disks folder. Then, in the right pane, click the DMP DSMs tab for the disk.
- 2 Right-click the path in the DMP DSMs tab, and select **Properties** from the path context menu that comes up.

The Path Properties screen appears.



The Properties screen displays the following information for the selected path:

- **Name** – The name of the selected path.
- **Status**
DMP DSMs have two path state indicators:
 - Healthy** – The path is operational.
 - Unhealthy** – The path is not operational.
- **Primary** – Whether the path is primary or not.
- **Port Number** – The number of the physical port on the storage array that the selected path is connected to.
- **Channel** – The channel that is associated with the path.
- **Target ID** – The number that, when combined with the LUN, uniquely identifies a disk on the port.
- **LUN** – Logical Unit Number, the number that, when combined with the Target ID, uniquely identifies a disk on the port.
- **Load Balance Policy** – Current load balance policy in effect.

- 3 Click **OK** to close the screen.

Microsoft Clustering support

- [Overview of support for Microsoft Clustering](#)
- [How SFW works with Microsoft Clustering](#)
- [Create a cluster dynamic disk group](#)
- [Make the cluster disk- group a cluster resource](#)
- [Display cluster disk group resource properties](#)
- [Create a dynamic mirrored quorum resource](#)
- [Microsoft Clustering quorum arbitration time settings](#)
- [Additional considerations for SFW Microsoft Clustering support](#)

Overview of support for Microsoft Clustering

You can use Veritas Storage Foundation for Windows to manage storage for a cluster set up for Microsoft Clustering. For Windows Server 2003, Microsoft Clustering is available with Microsoft Cluster Service (MSCS) software. For Windows Server 2008, it is available as the Failover Cluster feature.

Veritas Storage Foundation for Windows supports a cluster environment set up under the Microsoft Clustering for up to eight nodes. A cluster consists of two or more nodes, which are linked servers that support a set of common resources and provide an image of a single system to the client. Microsoft Clustering has failover functionality so that if one of the nodes fails or is taken offline, another node gains access to all resources held by the failed node, thus providing minimum downtime for applications using these resources.

With Veritas Storage Foundation for Windows, you can create mirrored, RAID-5, and other advanced dynamic volumes on clustered storage.

To use Veritas Storage Foundation for Windows with Microsoft Clustering, you need to do the following three main tasks:

- **Set up the cluster environment.**
The minimum requirement is two servers connected by a network. The servers must be on a shared SCSI or Fibre Channel bus. You install and configure Microsoft Clustering on each machine that is to be a member of the new cluster.
- **Install SFW and create one or more cluster disk groups.**
The process is almost identical to creating a regular dynamic disk group in SFW, except that when you create a cluster disk group, the program sets up the group so that it can be accessed by Microsoft Clustering and be used as a resource in the cluster. You create the desired dynamic volumes in the cluster disk group in exactly the same way as in a regular dynamic disk group.
See [“Create a cluster dynamic disk group”](#) on page 759.
- **Use the Windows Server 2003 Cluster Administrator or Windows Server 2008 Failover Cluster Management to add the cluster disk group as a resource to the cluster.**
After this step is done, the storage is part of the cluster and is associated with a specific node of the cluster. If the node fails or goes offline, the clustered storage on the node is transferred to another node in the cluster.
See [“Make the cluster disk- group a cluster resource”](#) on page 761.
If you are using an application, you may want to set up a separate resource group for the application.

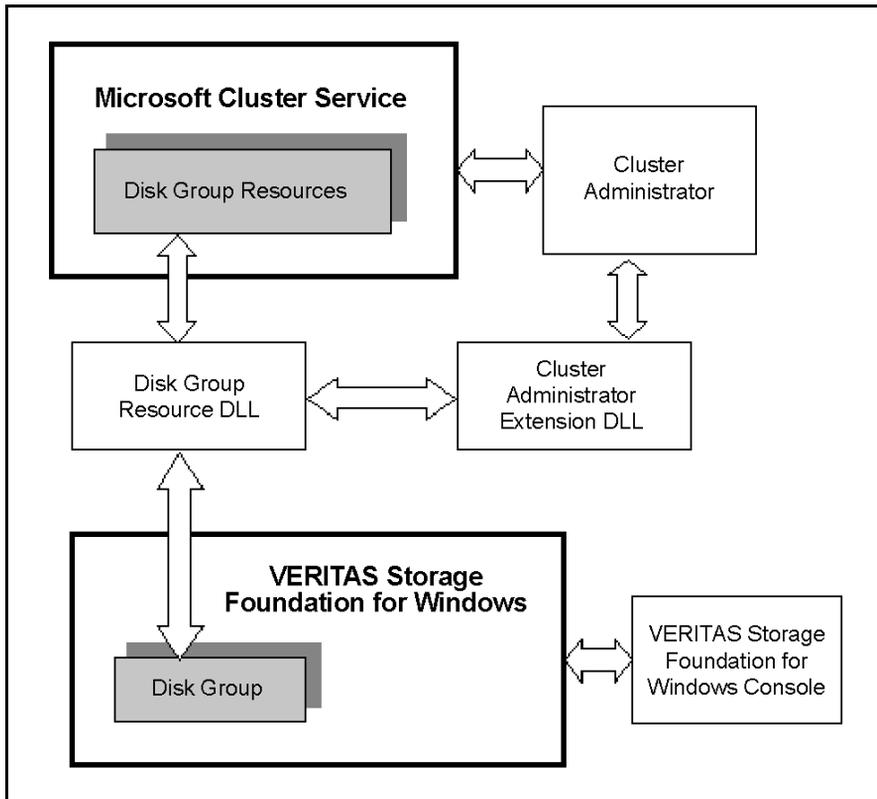
Note: For detailed instructions on setting up SFW and Microsoft Clustering with an application and also for integrating it with VVR, see the procedures in the *Veritas Storage Foundation and High Availability Solutions Solutions Guide*. The Solutions Guide also has instructions for setting up SFW and Microsoft Clustering with VVR.

How SFW works with Microsoft Clustering

Microsoft Clustering provides a set of standard resources, such as physical disks, file and print shares, and network addresses and names. Each resource is accessed using a resource DLL and an extension DLL. The resource DLL provides communication between Microsoft Clustering and the resource. The extension DLL allows the user to set the resource properties.

Microsoft also allows vendors to integrate product-specific resources into Microsoft Clustering through the use of custom resource and extension DLLs. SFW's product-specific resource is the Veritas Storage Foundation for Windows Disk Group resource with its two DLLs, Disk Group resource DLL and Cluster Administrator extension DLL. The block diagram below shows the relationship between Veritas Storage Foundation for Windows cluster components and the Microsoft Cluster Service.

Figure 14-1 Relationship between SFW and the Microsoft cluster Service



The initial install program for Veritas Storage Foundation for Windows will install both the Veritas Storage Foundation for Windows Disk Group resource DLL and the Cluster Administrator extension DLL, provided that you select the Microsoft Clustering (MSCS) support option and the install program detects that Microsoft Clustering is already installed and running on the server.

In the situation where you want to add Microsoft Clustering and Microsoft Clustering (MSCS) support after SFW has already been installed, SFW is enabled to install these resources and the extension DLLs.

See [“Installing Microsoft Clustering support after SFW is already installed”](#) on page 757

If you are installing the client version of Veritas Storage Foundation for Windows, you can choose the client install and the Microsoft Clustering (MSCS) support option. This combination installs remote cluster support on the client machine and does not require Microsoft Clustering to be installed on that machine. However, Microsoft Clustering, Veritas Storage Foundation for Windows, and SFW Microsoft Clustering (MSCS) support must be installed on any servers that the client manages.

Installing Microsoft Clustering support after SFW is already installed

This section describes the steps needed to install Microsoft Clustering support on a server if Veritas Storage Foundation for Windows is already installed. You will need to do a “rolling install,” in which you install the SFW Microsoft Clustering (MSCS) support option on the inactive node or nodes of the cluster first. Then you make the active cluster node inactive by moving the cluster resources to another node and install on that node.

To install SFW Microsoft Clustering (MSCS) support when SFW is installed

- 1 First, you must have an Microsoft Clustering set up and have Microsoft Clustering running on each server where you want to install the SFW Microsoft Clustering (MSCS) support. SFW also must be running on each server in the cluster.
- 2 On the inactive node of the cluster, select **Add or Remove Programs** in the Windows Control Panel.
- 3 From the menu located on the left side of the Add or Remove Programs window, select **Change or Remove Programs**.
- 4 Highlight the SFW Server Components entry and click **Change**.
- 5 The installer window appears. Select **Add or Remove** to add or remove features. Click **Next** to continue.

- 6 The Option Selection window appears. Check the **Cluster Option for Microsoft Cluster Service (MSCS)**.
If the option is grayed out, you need to add its license key:
 - Click the **Add License** link located at the far right of the window to add a license key for an option.
 - In the pop-up window that appears, enter the license key for the option and click **OK**. Click the checkbox to add the option.Click **Next** to continue.
- 7 The Validation window appears. The installer checks for prerequisites for the selected systems and displays the results. Review the information and click **Next** to continue.
- 8 The Summary window appears. Review the information and click **Update** to begin the product update.
The Update Status window appears. Status messages and the progress of the update are displayed. At the completion of the update, click **Next** to continue.
- 9 A report summarizing the update appears. Review the information and click **Next** to continue.
- 10 The Thank You window appears when the feature has been added or removed. Click **Finish** to complete the process.
- 11 A message box appears. Click **Yes** to reboot your system and complete the update.
- 12 Complete the installation by repeating the sequence on any remaining nodes.
For the active node, use the **Move Group** command in the Windows Server 2003 Cluster Administrator or with Windows Server 2008 Failover Cluster Management to move the cluster resources to another node before installing.

Create a cluster dynamic disk group

This section contains a summary of the steps necessary to create a cluster disk group.

To create a cluster disk group, follow the steps for creating a new dynamic disk group.

See “[Create dynamic disk groups](#)” on page 53.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support cluster disk groups.

In the step for defining the attributes, be sure to check the **Create cluster group** checkbox.

Please note the following considerations in this process:

- When creating a cluster disk group for use as a Volume Manager Disk Group resource, make sure that the disk group name is unique across the cluster. If the cluster software attempts to fail over a disk group to another node that has a disk group with the same name or if you move a disk group to another node that has a disk group with the same name, unpredictable results can occur.

Note: With release 4.0, the name of the Volume Manager for Windows program changed to Veritas Storage Foundation for Windows; however, the program’s disk group resource name in Microsoft Clustering is still the “Volume Manager Disk Group” resource.

- When assigning a drive letter to a new volume that is going to be part of a Veritas Storage Foundation for Windows disk group resource, make sure the drive letter assigned is available on all other nodes. Failure to do so may result in drive letter changes when the resource is moved or failed over to another node.
- SFW normally does not allow you to create a cluster dynamic disk group with disks that are on the same bus as the cluster node’s system or boot disk, but you can now remove this limitation by running a `vxclus` command from the SFW command line interface. Users have requested this change to facilitate booting from a SAN. If you plan to set up your system to boot from a SAN, proceed with caution to make sure that you are following the correct procedure.

See “[vxclus UseSystemBus ON](#)” on page 327.

- Setting up the cluster disk group on Windows Server 2008 creates physical disk resources for all the basic disks on the shared bus. Later you create resources for the SFW cluster disk groups. Before doing so, you must remove any physical disk group resources for disks used in the cluster disk groups. Otherwise, a reservation conflict occurs.

After creating the cluster disk group, create the necessary dynamic volumes on the cluster disks.

Make the cluster disk- group a cluster resource

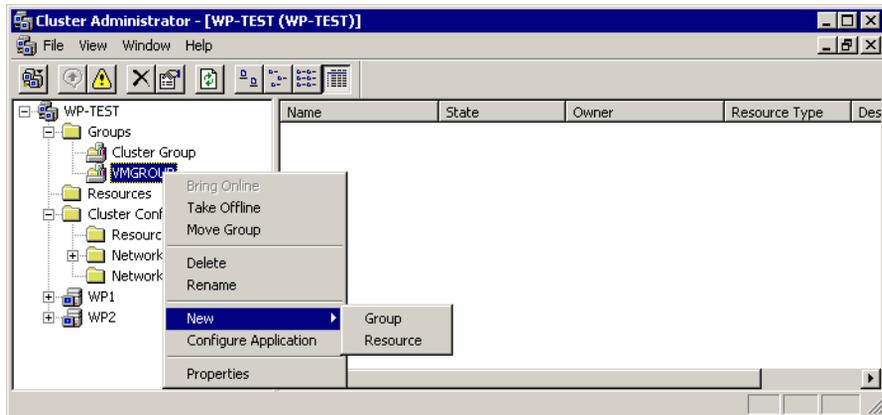
The following steps describe how to make a Veritas Storage Foundation for Windows cluster disk group a resource in a cluster.

Making the cluster disk group a cluster resource in Windows Server 2003

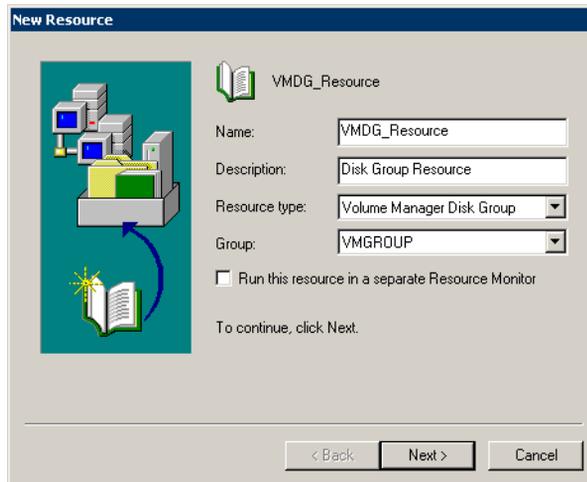
To make the cluster disk group a cluster resource

- 1 Start Cluster Administrator.
- 2 Right-click the label of the MSCS cluster group for which you want to create the resource.

The cluster group context menu appears.



- 3 Select **New** and then **Resource**, which brings up the New Resource screen.

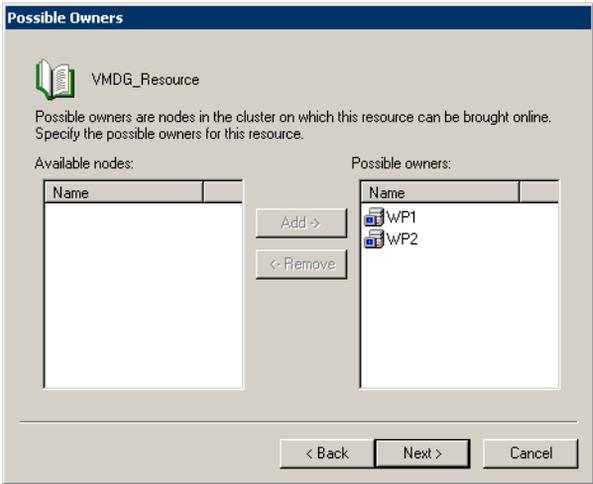


- 4 Fill in the fields for the New Resource screen:

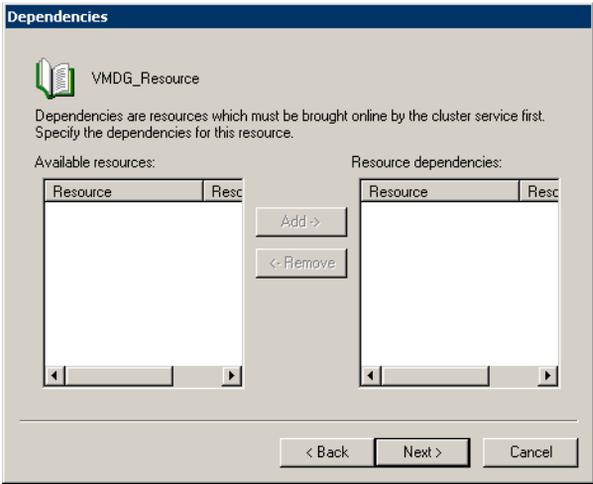
Name	Designate a useful name.
Description	“Disk Group Resource” is an appropriate description.
Resource type	Use the drop-down list to select Volume Manager Disk Group . Note that the disk group name has not been changed to Veritas Storage Foundation Disk Group.
Group	Use the drop-down list to select the appropriate MSCS cluster group. The MSCS group you chose in step 2 should already be selected.
Run this resource in a separate Resource Monitor	Generally, make sure that this is NOT checked. Check this box if you wish to run the resource in a separate resource monitor, which can be useful for troubleshooting, but is typically not necessary.

Click **Next** to go to the next screen.

The Possible Owners screen appears.

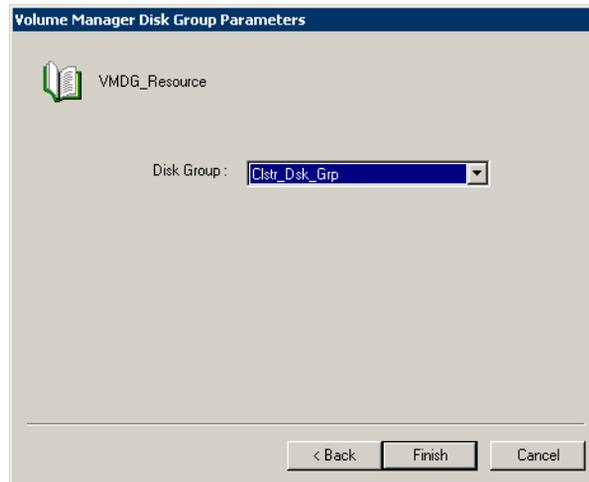


- 5 Use the **Add** button to add all possible owners of the new resource to the “Possible owners” list, and click **Next** to continue.
The Dependencies screen appears.

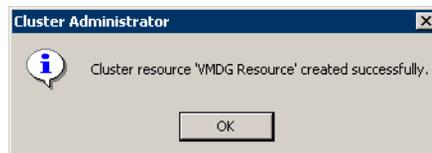


- 6 In the Dependencies screen, click **Next** to continue.
The disk group resource does not depend on any other resources.

The final screen for creating a resource in Cluster Administrator appears.

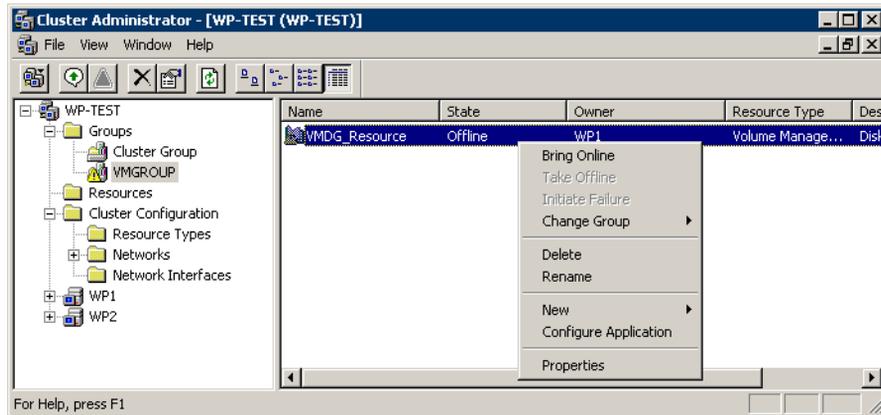


- 7 Make sure that the appropriate Veritas Storage Foundation for Windows cluster disk group is selected from the drop-down list for the resource, and then click **Finish** to complete the operation.
If the cluster disk group you want doesn't appear, exit the Cluster Administrator New Resource wizard and do the following:
 - Make sure the cluster disk group you want as an MSCS resource is imported and note which node it is imported on.
 - Move the MSCS group to the same node where the cluster disk group is imported.
 - Invoke the Cluster Administrator New Resource wizard and attempt to add the cluster disk group again (step 1 through step 7 of this procedure). This time, you should be able to add the desired cluster disk group as a resource.
- 8 In the final dialog box that appears, click **OK** to confirm.

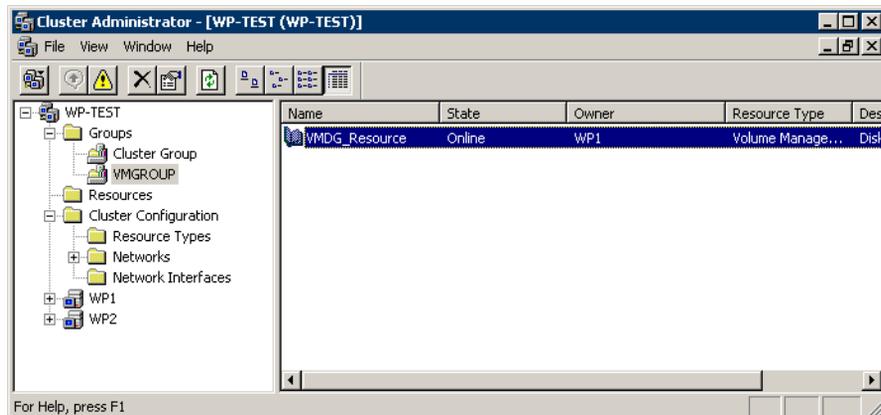


- 9 Bring the disk group resource online by doing the following:

- Right-click the name of the resource to bring up a context menu as shown:



- Select **Bring Online** on the context menu. The sample screen that follows shows the VMDG resource in an Online state.

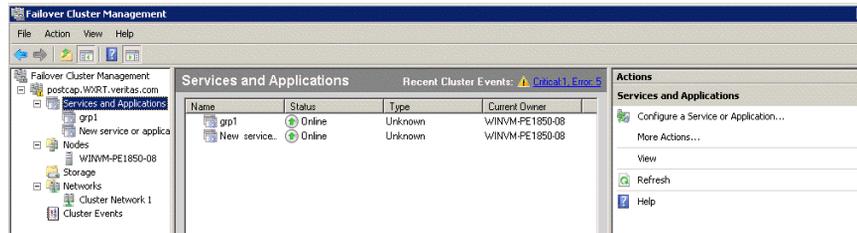


Making the cluster disk group a cluster resource in Windows Server 2008

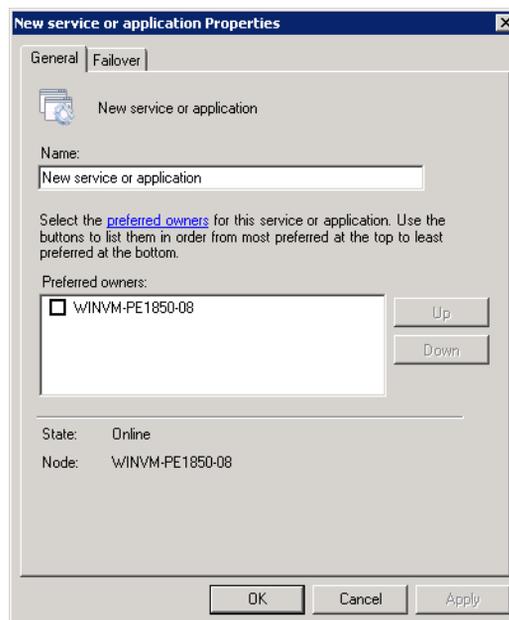
To make the cluster disk group a cluster resource

- 1 Start Failover Cluster Management by selecting All Programs>Administrative Tools>Failover Cluster Management.
- 2 Expand the tree view in the left pane to display Services and Applications.

- 3 Right-click Services and Applications and in the context menu select More Actions>Create Empty Service or Application.
The Services and Applications window appears displaying the generic New service or application entry in the table.



- 4 Right-click the New service or application entry and select Properties from the context menu.
The new service and application Properties window appears.



- 5 Enter a name for the New service and application in the Name field and click **OK** to continue.
- 6 In the tree-view of Failover Cluster Management, expand the Services and Applications node to display the service created in the above step.

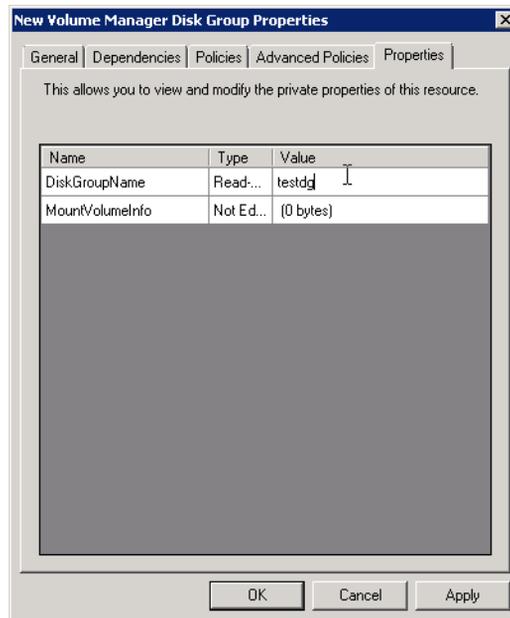
Right-click the service and select Add a resource>More resources>Add Volume Manager Disk Group.

The Summary of the service window appears displaying the generic New Volume Manager Disk Group entry in the table.

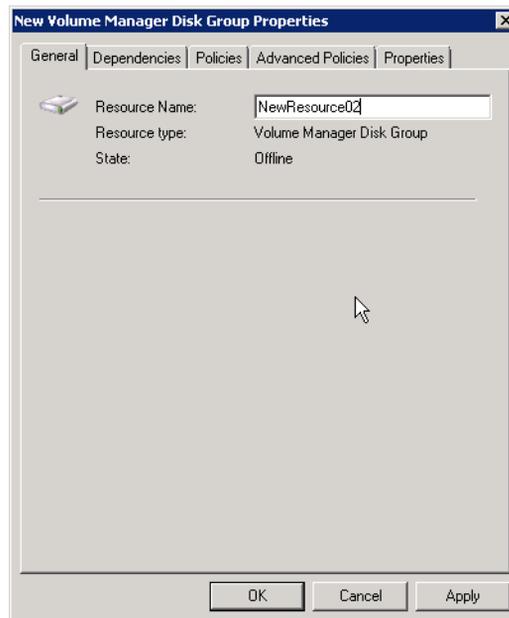
- 7 Right-click the NewVolume Manager Disk Group entry and select Properties on the context menu.

The New Volume Manager Disk Group Properties window appears.

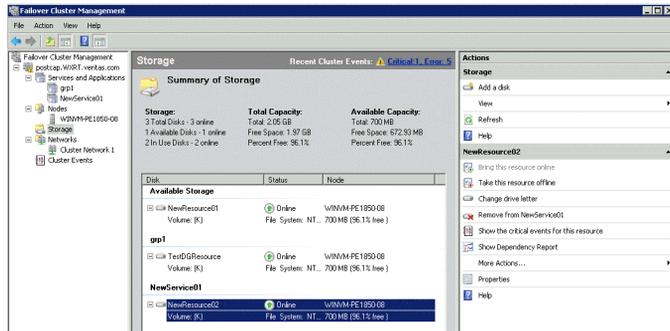
- 8 Under the Properties tab, enter the name of the SFW cluster disk group that will be the cluster resource in the Value column of the DiskGroupName entry.



- 9 Under the General tab, enter a name for this new resource in the Resource Name field and click **OK** to continue.



The Summary of the service window appears displaying the new cluster resource as a Disk Drive entry in the table. The cluster resource should have an online status. If the resource is not online, then right-click the new cluster resource and select **Bring this resource online** on the context menu. Expanding the entry in the table displays the name of the volume, the type of file system, and the amount of free space.



- 10 In the tree-view of Failover Cluster Management, expand the Storage node to review the attributes of the new cluster resource.

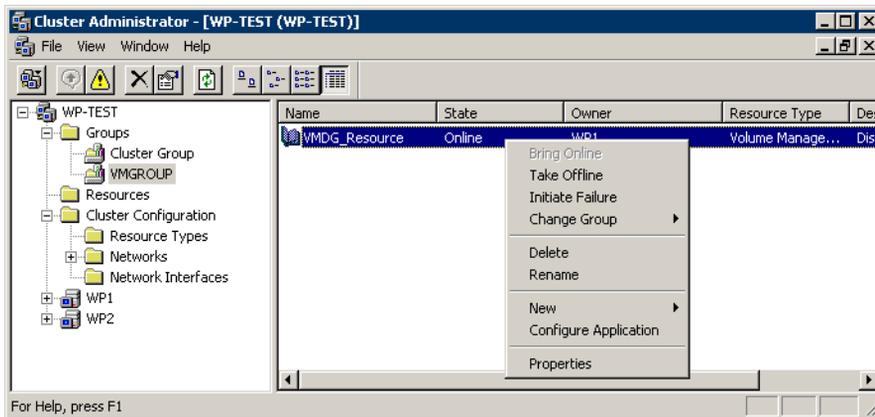
Display cluster disk group resource properties

The following describe how to display cluster disk group resource properties.

Displaying cluster disk group resource properties in Windows Server 2003

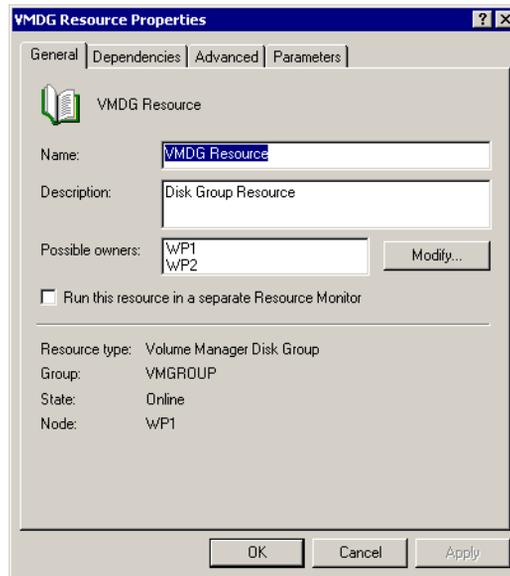
To display cluster disk group resource properties

- 1 Start Cluster Administrator.
- 2 Right-click the resource label to bring up the cluster resource context menu.

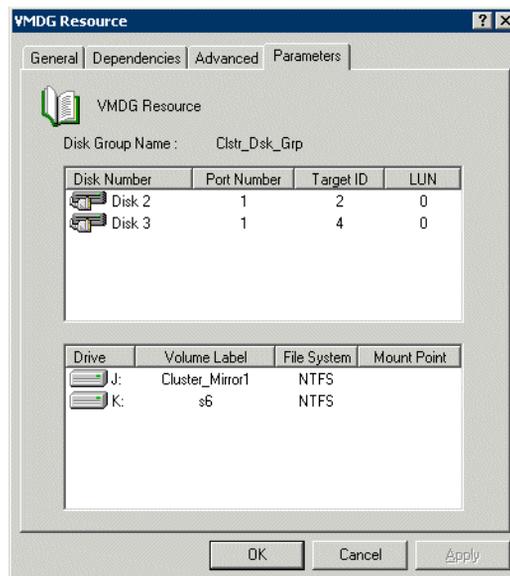


- 3 Select **Properties** from the context menu.

The Properties window for the disk group comes up.



- 4 Click the **Parameters** tab to display the disk and volume information for the disk group, as shown in the next sample screen. Clicking **OK** returns you to the Cluster Administrator main window.



Displaying cluster disk group resource properties in Windows Server 2008

To display cluster disk group resource properties

- 1 Start Failover Cluster Manager by selecting All Programs>Administrative Tools>Failover Cluster Manager.
- 2 Expand the tree view in the left pane to display Storage.
The Summary of Storage window appears displaying the cluster disk group resource.
- 3 Right-click the cluster disk group resource and select Properties from the context menu.
The Properties window appears.



Create a dynamic mirrored quorum resource

When you install the first node of a cluster, you specify a basic disk volume for a physical disk resource known as the quorum resource. This resource contains the cluster log and is also used for determining which node in a cluster has control over the cluster. If the physical disk quorum resource fails or becomes corrupted, the cluster becomes unusable.

A quorum resource failure can be avoided by using a dynamic mirrored quorum resource instead of a physical disk quorum resource. Unlike a physical disk quorum resource, which contains a single disk, a dynamic mirrored quorum resource will provide a high level of redundancy by allowing the mirroring of the quorum disk. It is strongly recommended that a dynamic mirrored quorum contain three disks because a cluster disk resource cannot be brought online unless a majority of disks are available. With the quorum volume in a two-disk group, loss of one disk will prevent the quorum volume from coming online and make the cluster unavailable.

If you are using a system running SQL Server, a problem can occur when migrating to a dynamic mirrored quorum volume.

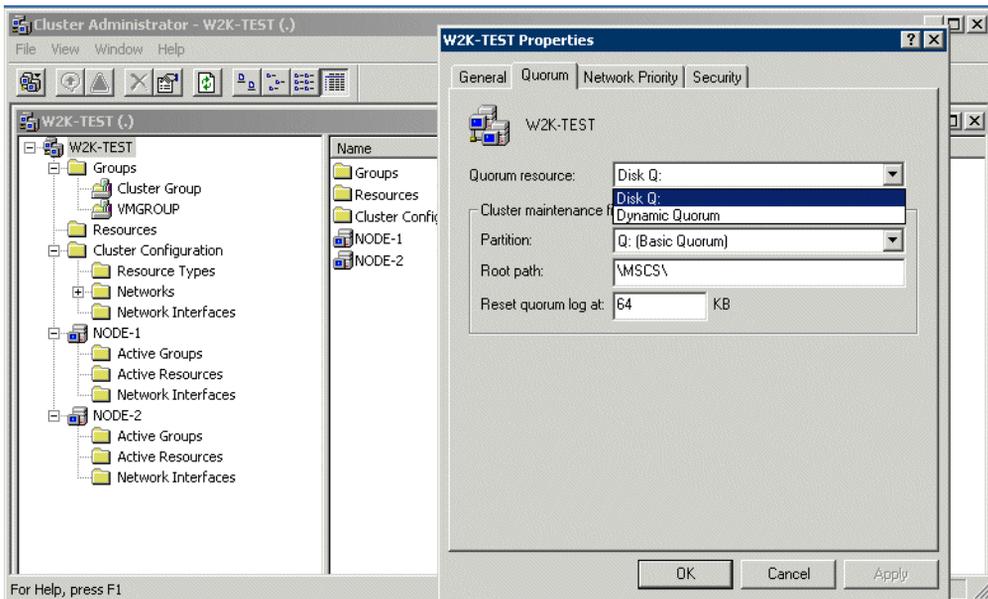
See [“Problem on a SQL server system with Microsoft Clustering when migrating to a dynamic mirrored quorum volume on a volume Manager disk group resource”](#) on page 507.

Creating dynamic mirrored quorum resource in Windows Server 2003

To create a dynamic mirrored quorum resource

- 1 Create a Veritas Storage Foundation for Windows cluster disk group that contains three disks.
If possible, use small disks, since the disk group will be used only for the quorum volume, which is recommended by Microsoft to be a size of 250 to 500 MB.
If other volumes are added to this disk group, any failures related to their operation can cause disruptive failovers of the quorum volume; or if another volume in the group experiences a high volume of read/write activity, failovers may result from delays in access to the quorum volume by MSCS.
See [“Create a cluster dynamic disk group”](#) on page 759.
- 2 Create a mirrored volume with all three disks in the cluster disk group.
It is strongly recommended that you maximize redundancy by using all three disks to create a three-way mirrored quorum.
See [“Mirroring”](#) on page 257.

- 3 Make the cluster disk group a cluster resource.
See “[Make the cluster disk- group a cluster resource](#)” on page 761.
- 4 Use Cluster Administrator to change the quorum resource from a physical disk resource to a dynamic disk resource by doing the following:
 - Right-click on the cluster name in the tree to bring up a context menu. For example, in the screen shown below, the cluster name is “**W2K-TEST**,” and the dynamic quorum disk group resource has been named “Dynamic Quorum.”
 - In the menu that comes up, click **Properties**, which displays the Cluster Properties window.
 - Select the **Quorum** tab of the Properties window.
 - Select **Dynamic Quorum** from the list of possible quorum resources, as shown in the screen below.

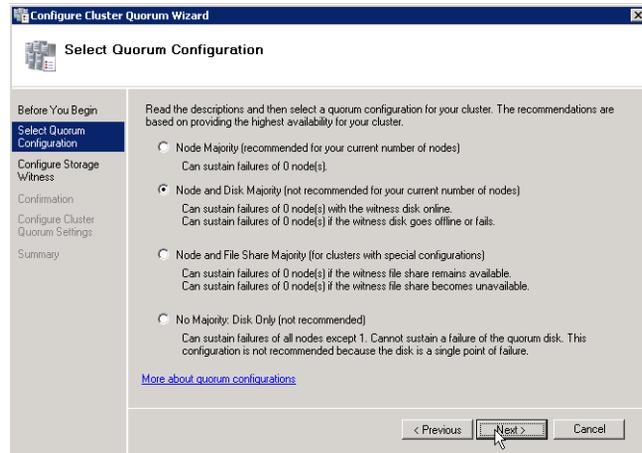


- Click **OK** to complete the operation.

Creating dynamic mirrored quorum resource in Windows Server 2008

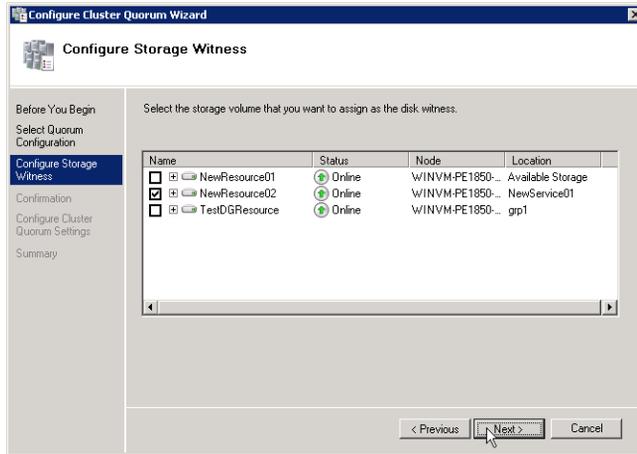
To create a dynamic mirrored quorum resource

- 1 Start Failover Cluster Manager by selecting All Programs>Administrative Tools>Failover Cluster Manager.
- 2 Right-click the cluster node and in the context menu select More Actions>Configure Cluster Quorum Settings. The Configure Cluster Quorum Wizard appears. Click **Next** to continue.
- 3 Select the appropriate quorum configuration.



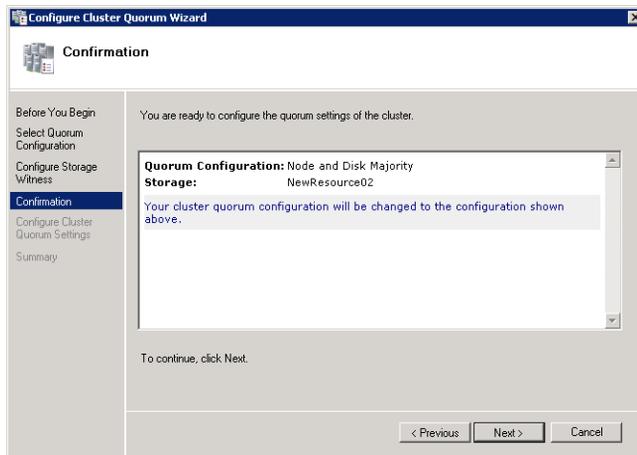
Click **Next** to continue.

- 4 Check the storage volume to assign as the quorum resource.



Click **Next** to continue.

- 5 Confirm the quorum settings of the cluster.



Click **Next** to continue.

- 6 Review the report generated by the wizard and click **Finish** to complete the operation.

Microsoft Clustering quorum arbitration time settings

When the SFW Microsoft Clustering (MSCS) support option is selected during installation, a message box appears to remind you that the minimum and maximum quorum arbitration times can be adjusted to ensure optimal functioning of Veritas Storage Foundation for Windows dynamic volumes with Microsoft Clustering .

The quorum arbitration minimum and maximum time settings are used to set the limits of the time period that is allowed for quorum arbitration. Quorum arbitration is the process that occurs when the controlling node of the cluster is no longer active and other nodes of the cluster attempt to gain control of the quorum resource and thus control of the cluster.

You may want to set up a dynamic quorum resource.

See “[Create a dynamic mirrored quorum resource](#)” on page 773.

The advantage of a dynamic quorum is that it can be mirrored to provide fault tolerance for the quorum resource.

The optimal quorum arbitration time settings for a dynamic quorum are:

Minimum time - 30 seconds

Maximum time - 120 seconds

To specify these settings, type the following commands in the command line:

```
cluster.exe /prop QuorumArbitrationTimeMin=30
```

```
cluster.exe /prop QuorumArbitrationTimeMax=120
```

If you do not plan to use a dynamic quorum and instead want to retain the quorum resource on a basic disk, then you may want to specify the default settings that Windows Server 2003 and Windows Server 2008 use for the basic quorum.

The Windows Server 2003 and Windows Server 2008 quorum arbitration time settings are:

Minimum time - 7 seconds

Maximum time - 60 seconds.

To reset the settings, type the following commands in the command line:

```
cluster.exe /prop QuorumArbitrationTimeMin=7
```

```
cluster.exe /prop QuorumArbitrationTimeMax=60
```

The advantage of changing the settings back is that it speeds up the quorum arbitration process.

Additional considerations for SFW Microsoft Clustering support

This section contains additional information that is important in working with Microsoft Clustering and Veritas Storage Foundation for Windows.

Note the following considerations:

- When a cluster disk group resource is offline or a cluster disk group that is not a Microsoft Clustering resource is in a Deported state, it is not protected from access by other machines. For maximum data protection, keep Volume Manager Disk Group resources online. Note that the SFW disk group resources still retain the “Volume Manager” name.
- When using the Windows Server 2003 Cluster Administrator or Windows Server 2008 Failover Cluster Management to create a disk group resource, the Volume Manager Disk Group Parameters screen might not list all the available Veritas Storage Foundation for Windows cluster disk groups in the drop-down list. If this happens, exit the New Resource wizard and use the Windows Server 2003 Cluster Administrator or Windows Server 2008 Failover Cluster Management to select the cluster group to which the resource is to be assigned. Next, move the cluster group to the cluster node where the Veritas Storage Foundation for Windows cluster disk group is currently online. Then create the Veritas Storage Foundation for Windows disk group resource.
- Under the following circumstances, the VEA Disk View may not reflect the latest state of the disk(s) until a refresh is performed:
 - When you change the state of a cluster disk resource on one node and try to view the disks under this resource from another node on the same cluster.
 - When you change the state of a cluster disk resource on one node and try to view the disks under this resource from a remote computer.
- SFW support of the Microsoft Clustering environment allows the selection of SCSI-2 reservation mode or SCSI-3 reservation mode. Selecting the type of SCSI support for the Microsoft Clustering environment is done by using the System Settings portion of the SFW Control Panel.

When selecting the type of SCSI support in a Microsoft Clustering environment, it is important to know if your storage arrays support SCSI-3. SFW SCSI-3 clustering support does not allow you to mix storage arrays that support SCSI-3 with storage arrays that cannot. In a situation of mixed storage arrays, you must use SFW SCSI-2 clustering support. Refer to the HCL for arrays that support SCSI-3.

Note: Veritas maintains a Hardware Compatibility List (HCL) for Veritas Storage Foundation & High Availability Solutions 5.1 for Windows Products on the Symantec Support web site. Check the HCL for details about your storage arrays before selecting the type of SCSI support in a Microsoft Clustering environment.

After selecting the type of SCSI support, you must issue the following CLI commands to complete the setting on your system.

- `net stop vxvm`
- `net start vxvm`

Note: If a cluster disk group is imported on the system, you must deport or move the cluster disk group to another system before issuing these CLI commands.

Note: If SFW SCSI-2 clustering support is selected and Active/Active load balancing is desired, the SCSI-3 Persistent Group Reservations (SCSI-3 PGR) support mode must be enabled for the DMP DSM. For more information about enabling SCSI-3 PGR (Windows Server 2003 only), see [“Active/Active and Active/Passive settings in a cluster environment”](#) on page 723 and [“vxdmadm”](#) on page 388.

- A cluster dynamic disk group that is part of the cluster resources cannot be a source disk group for a join command. However, it can be a target disk group for the command.
- **Change in Bringing a Two-Disk Cluster Group Online**
 In earlier versions of Volume Manager for Windows, it was possible to bring a two-disk cluster disk group online when only one disk was available. If a cluster were to lose all network communication, this allowed the disk group to be brought online on two cluster nodes simultaneously, with each node owning a single disk, possibly resulting in data loss or a partitioned cluster. Though the likelihood of this situation occurring is slim for most customers, the consequences if it does happen may be severe. Accordingly, in Volume Manager 3.0 and 3.1 and Veritas Storage Foundation for Windows 4.0 and 5.1, it is no longer possible to bring a two-disk cluster disk group online unless it complies with the normal majority algorithm ($n/2 + 1$), which means both disks must be available.
- You are not allowed to deport a cluster disk group that is also a Volume Manager disk group resource for Microsoft Clustering.
- Connecting to a Cluster Node

If you connect to a machine from the VEA GUI using the virtual name or the virtual IP address, the VEA GUI will display the machine name of the cluster node that currently owns the virtual name and IP resources. Therefore, it is not recommended to use the virtual name or virtual IP address when connecting and administering a cluster node through SFW HA.

Instead, use the actual machine name or the IP address of the cluster node.

- Veritas Dynamic Multi-pathing does not support using a basic disk as a cluster resource under Microsoft Clustering.
Failover may not function properly when using Veritas Dynamic Multi-pathing with a Microsoft Clustering basic disk cluster resource. Refer to Tech Note 251662 on the Veritas Support site for details.
If you want to use Veritas Dynamic Multi-pathing with SFW and a Microsoft Clustering cluster, you must convert any Microsoft Clustering basic disk cluster resources to dynamic disk cluster resources before activating Veritas Dynamic Multi-pathing. The initial setup of Microsoft Clustering requires that you use a basic disk as the quorum disk. Once SFW is installed, you should upgrade the basic disk to dynamic by including it in a dynamic cluster disk group and then convert the quorum resource from a basic disk resource to a dynamic disk resource.

Note: DMP DSMs do not support an Active/Active setting in an Microsoft Clustering environment when a quorum disk is a basic disk.

- Cluster dynamic disk groups that contain iSCSI disks are not set up for persistent login on all nodes in the cluster.
SFW ensures that the iSCSI targets of cluster dynamic disk groups that contain iSCSI disks are configured for persistent login. If the persistent login is not configured for the target, SFW automatically configures it. Cluster dynamic disk groups that contain iSCSI disks are only automatically configured for persistent login on the node where they were created. The other nodes in the cluster are not enabled for persistent login. You need to manually set up the persistent login for each of the other nodes in the cluster.
- Copying the Policy File, VxVolPolicies.xml, to Another Node
If the second node is configured the same as the first and if the first node's policy settings for Automatic Volume Growth and VxCache are to be maintained on the second node, you need to copy the VxVolPolicies.xml file of the first node to the second node. Copy the VxVolPolicies.xml file to the same path location on the second node as its location on the first node. The default path of the VxVolPolicies.xml file is **Documents and Settings\All Users\Application Data\Veritas**.

For more information about the Policy File, see the following topics:

- [“Automatic volume growth”](#) on page 246
- [“More on the policy file”](#) on page 560
- For information about using SFW and Microsoft Clustering in a shared cluster environment with the FlashSnap off-host backup procedure, see the following topic:
 - [“Using dynamic disk group split and join with a cluster on shared storage”](#) on page 609.

VCS support in SFW HA

- Overview
- How SFW HA works with VCS
- Integration steps
 - Setting up the cluster hardware
 - Installing and configuring Windows
 - Installing SFW HA
 - Setting up a VCS cluster
 - Creating cluster dynamic disk groups and volumes
 - Installing the application on cluster nodes
 - Configuring cluster disk groups and volumes as VCS resources
 - Bringing resources online
 - Testing the cluster
- Additional considerations for SFW VCS support

Overview

SFW HA provides built-in Veritas Cluster Server (VCS) support to allow you to set up cluster disk groups for a VCS cluster on a Windows Server 2003 or Windows Server 2008 system.

Veritas Cluster Server (VCS) is a high-availability solution for clustered environments. It monitors systems and services on a cluster and fails over services to a different system in case of a system crash or a service failure. VCS provides policy-based, application-focused failover management, which enables applications to be failed over to any server in the cluster or SAN environment and to consecutive servers as necessary. VCS supports up to 32-node clusters in SAN and traditional client-server environments.

With SFW HA, you can create mirrored, RAID-5, and other advanced dynamic volumes on VCS clustered storage.

This chapter gives a high-level overview of how you can set up Veritas Storage Foundation HA to manage storage for a cluster with the VCS software. Please refer to the VCS documentation and the SFW Solutions Guides for detailed step-by-step information on setting up various SFW HA configurations.

For full details on clustering steps with SFW HA, see the *Veritas Storage Foundation and High Availability Solutions, Solutions Guide*. If you are using Microsoft Exchange Server 2003 or Microsoft SQL Server 2000, refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange* or the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL*.

How SFW HA works with VCS

VCS uses application-specific programs called agents to manage hardware and software entities within a highly available cluster environment. The entities being managed are called resources. Resources with similar characteristics are collectively known as a resource type. Resources can be grouped together to be part of a service group, which is an organizational grouping for related resources.

VCS provides the Volume Manager Disk Group (VMDg) and MountV agents to manage cluster disk groups and mounts created on cluster disk groups.

Note: Even though the name of the Volume Manager program has changed to Storage Foundation for Windows, the Volume Manager Disk Group (VMDg) name remains in effect.

About the volume Manager disk group agent

The VMDg agent imports, monitors, and departs a cluster disk group configured with SFW HA. The agent makes the disk group highly available. The VMDg agent supports Dynamic Multi-pathing (DMP) and works in a SAN environment. The agent is represented by the VMDg resource type.

About the MountV agent

The MountV agent mounts, monitors, and unmounts volumes on cluster disk groups imported using SFW HA. The agent supports NTFS, FAT, and FAT32 formatted volumes. When a cluster disk group fails over to another system, the MountV agent ensures that the new system accesses the disk group from the same path it was accessed from before failover. The MountV agent ensures a consistent device path by mounting the disk group with the same mount point (drive letter) on the new system. It also dismounts the disk group from a failed system when a resource or group is taken offline. The agent supports mounting disk groups as NTFS folders.

The agent is represented by the MountV resource type.

Refer to the VCS documentation for more information about the agents, their resource types, and attributes.

Integration steps

To use SFW HA with VCS, you must perform the following tasks. Each task is described more fully in the following sections.

- [Setting up the cluster hardware](#)
- [Installing and configuring Windows](#)
- [Installing SFW HA](#)
- [Setting up a VCS cluster](#)
- [Creating cluster dynamic disk groups and volumes](#)
- [Installing the application on cluster nodes](#)
- [Configuring cluster disk groups and volumes as VCS resources](#)
- [Bringing resources online](#)
- [Testing the cluster](#)

For detailed step-by-step procedures for installing and configuring a cluster with SFW HA, see the *Veritas Storage Foundation and High Availability Solutions, Solutions Guide*, which is included on the product CD.

Setting up the cluster hardware

Set up the hardware for VCS according to the recommendations in the VCS documentation. Refer to instructions from the hardware manufacturers for specific hardware installation details.

Installing and configuring Windows

Install the Windows operating system on all cluster nodes and configure the necessary network settings. See *Veritas Storage Foundation and High Availability Solutions, Solutions Guide* for specific recommendations.

Installing SFW HA

The SFW HA installer allows you to install the software for Veritas products for Storage Foundation HA for Windows on multiple nodes simultaneously. The HA installer automatically installs SFW, VCS, and the Veritas Cluster Server Enterprise Agent.

For instructions, see *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Setting up a VCS cluster

Use the VCS configuration wizard (VCW) to set up the VCS cluster. To start the wizard, select **Start>All Programs>Symantec>VERITAS Cluster Server>Configuration Wizards>Cluster Configuration Wizard**. Full steps for this wizard are given in the *Veritas Storage Foundation and High Availability Solutions, Solutions Guide*.

Creating cluster dynamic disk groups and volumes

At this point, you will use Veritas Storage Foundation for Windows to create disk groups and dynamic volumes for the application on the shared storage.

To create cluster dynamic disk groups and volumes

- 1 Create one or more cluster disk groups in SFW as follows:
 - See “[Create dynamic disk groups](#)” on page 53.
 - Create a separate cluster disk group with a unique name for each application to be clustered.
 - Make sure the device path to each disk group is recognized by all systems sharing the disk.
 - In the step for defining the attributes, be sure to select the checkbox **Create cluster group**.

When creating a cluster disk group for use as a Volume Manager disk group resource, make sure that the disk group name is unique across the cluster. If the cluster software attempts to fail over a disk group to another node that has a disk group with the same name or if you move a disk group to another node that has a disk group with the same name, unpredictable results can occur.

- 2 In SFW, create one or more dynamic volumes for each cluster disk group. See “[Create dynamic volumes](#)” on page 60.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support cluster disk groups.

Installing the application on cluster nodes

If you are installing an application on the cluster nodes, this is the point in the process where that task will be done. VCS requires that the application program files be installed on the same local drive of all the cluster nodes and that the application data and log files or other files related to the application data be

installed on the shared storage, using the cluster disk groups and dynamic volumes that were set up in the previous task.

Applications may have built-in procedures for running on a cluster. Consult the application documentation to determine whether these procedures are available. Make sure that the disk groups and volumes are imported and thus mounted on the server before you install the application.

Configuring cluster disk groups and volumes as VCS resources

This section describes the procedures for configuring cluster disk groups and volumes as VCS resources through a VCS service group. You can create a new service group for these resources or add these resources to an existing service group. The disk groups must be configured as resources of type VMDg and volumes as resources of type MountV. You must create a resource dependency such that the MountV resources depend on the VMDg resources.

Once the cluster disk groups are configured as VCS resources, VCS will take over the tasks of importing and deporting disk groups and mounting and unmounting volumes.

Please note that VCS provides multiple ways to create service groups. For example, if you are using Microsoft Exchange or Microsoft SQL Server with VCS, you need to use the VCS service group wizard for Exchange or SQL. There are also separate wizards for setting up file shares and for setting up print shares, as well as a generic application wizard, a Web GUI wizard, and the Cluster Manager Java Console. You can also use the command line to configure the VCS service group. Please refer to the VCS documentation to determine which wizard is most appropriate to configure the service group for your situation. This section describes how to create and configure a service group with the Cluster Manager Java Console. All the different methods for creating a service group cover similar steps.

This section covers the following topics:

- [Creating a service group](#)
- [Adding resources to a service group](#)
- [Editing resource attributes](#)
- [Creating the resource dependency](#)
- [Bringing resources online](#)

Creating a service group

A service group is a collection of resources working together to provide application services to clients. It typically includes multiple hardware and software resources working together to produce a single service. For example, a

database service group may include a logical network (IP) address, the database management system software (DBMS), underlying file systems, logical volumes, and a set of physical disks managed by SFW HA. If this service group migrates to another node for recovery purposes, all of its resources must migrate together to recreate the group on another node without affecting other service groups.

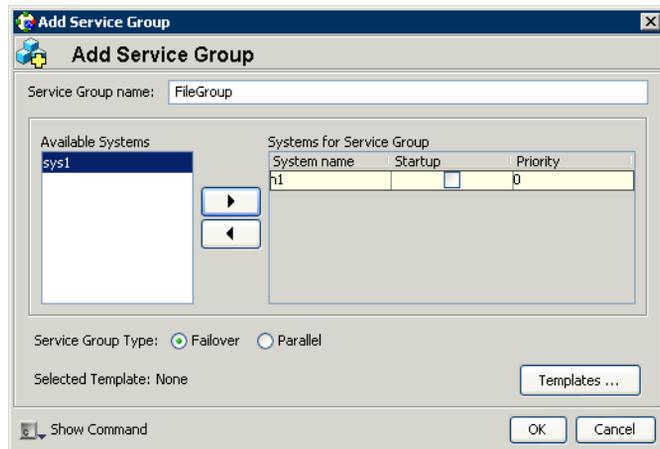
This section describes the procedure for creating a new service group.

You can also add resources to an existing service group.

See “[Adding resources to a service group](#)” on page 790.

To create a new service group

- 1 Start Cluster Manager (Java Console) and log on to the cluster.
- 2 On the Edit menu, click **Add**, and then click **Service Group**. The Add Service Group window appears.



- 3 Enter the name of the service group.
- 4 In the **Available Systems** box, click the systems to which the service group will be added.
- 5 Click the right arrow to move the selected systems to the **Systems for Service Group** box.
- 6 To add a new service group based on a template, click **Templates**.
- 7 Click the appropriate template name in the Templates dialog box that comes up.
- 8 Click the appropriate service group type. A failover service group runs on only one system at a time; a parallel service group runs concurrently on multiple systems.

9 Click **OK**.

You can see the newly created service group in the Cluster Explorer configuration tree.

Adding resources to a service group

To add resources of the **MountV** and **VMDg** resource type to the service group

- 1 If you have not already done so, start Cluster Manager (Java Console) and log on to the cluster.
- 2 From the Cluster Explorer configuration tree, select the service group to which the resources will be added.
- 3 From the Cluster Explorer Edit menu, choose **Add>Resource**.
- 4 In the Add Resource dialog box, enter a unique name for the resource.

Attribute name	Type	Dimension	Value	Edit
ForceUnmount	String	Scalar	NONE	
ListApplications	Boolean	Scalar	false	
AutoFSClean	Boolean	Scalar	false	
MountPath	String	Scalar		
VolumeName	String	Scalar		
MMNRCacheName	String	Scalar		

Critical Enabled

Show Command OK Cancel

- 5 From the **Resource Type** list, select the **MountV** resource type.
- 6 Select the **Critical** and **Enabled** checkboxes and click **OK**.
- 7 Repeat steps 3 to 6 to add a resource of the **VMDg** resource type.
After adding the resources, you must define attribute values for the resources according to your configuration.
See “[Editing resource attributes](#)” on page 790.

Editing resource attributes

This section describes the attributes that need to be defined to configure the **MountV** and **VMDg** resources and the procedure for defining these attributes.

Attributes for resources of type MountV

MountV includes the following resources:

- *MountPath* – The drive letter or path to an empty NTFS folder that will be assigned to the volume being mounted. VCS will mount the volume at this path. The attribute can be specified as X, X:, X:\, X:\Directory, or X:\Directory\.
- *VolumeName* – The name of the volume to be mounted. For example, the name could be Raid1, Stripe2, Volume01, and so on.
- *VMDgResName* – The name of the Volume Manager disk group (VMDg) resource on which the MountV resource depends.

Attributes for resources of type VMDg

DiskGroupName – The name of the cluster disk group. The disk group name can be retrieved from the VEA console by running the command `vxdg list`, or by using the VCS **VMGetDrive** utility.

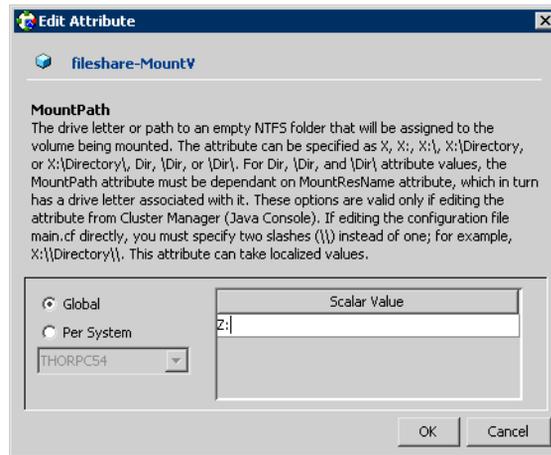
Before defining resources of type MountV and VMDg, take the following precautions:

- Do not configure a system drive as a resource of type Mount or MountV.
- When using the Mount or MountV agents to configure a resource as a folder mount, you must also configure the root folder as a VCS resource.
- If you remove the EVERYONE=READ permission from the volume to be configured as a Mount/MountV resource, make sure that the system account has READ permissions (SYSTEM=READ) to the volume.

To edit resource attributes

- 1 In the Cluster Explorer configuration tree, click the object whose attributes you want to edit.
- 2 In the View panel, click the **Properties** tab. If the attribute does not appear in the Properties View, click **Show All Attributes**. This opens the Properties View.
- 3 In the Properties View, click the icon in the Edit column of the Key Attributes or Type Specific Attributes table. In the Attributes View, click the **Edit** icon in the Edit column of the attribute table.

- 4 In the Edit Attribute dialog box, enter changes to the attribute values and click **OK**.



Repeat these instructions for all MountV and VMDg attributes.

See “[Editing resource attributes](#)” on page 790.

Creating the resource dependency

VCS requires that you create a dependency between resources of type MountV and those of type VMDg.

To create the resource dependency

- 1 In the Cluster Explorer configuration tree, click the **Service Groups** tab.
- 2 Click the service group to which the MountV and VMDg resources belong.
- 3 In the view panel, click the **Resources** tab. This opens the resource dependency graph.
- 4 Click the **MountV** resource.
- 5 Drag the yellow line to the **VMDg** resource and click the resource.
- 6 In the Confirmation dialog box, click **Yes**.
You can now bring the resources online.
See “[Bringing resources online](#)” on page 793.

Bringing resources online

When you bring resources of type MountV and VMDg online, VCS imports the disk group on the active system in the cluster and mounts the volumes at the specified mount paths.

To bring resources online

- 1 In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the resource of type MountV.
- 2 From the pop-up menu, click **Online**, and click the system on which to bring the resource online.

Once the command is completed, the resources should come online on the selected system. You can view the status of the resources in the Cluster Explorer's View panel.

Testing the cluster

You can verify your installation by switching nodes in the VCS Cluster Manager (Java Console). For the most complete test of the cluster's failover capability, shut down the computer that is currently online. Bring it back up again after the cluster fails over.

Additional considerations for SFW VCS support

The following additional information is important in working with VCS and Veritas Storage Foundation for Windows:

- A cluster dynamic disk group that is part of the cluster resources cannot be a source disk group for a join command. However, it can be a target disk group for the command.
- Connecting to a Cluster Node through the VEA GUI
If you connect to a machine from the VEA GUI using the virtual name or the virtual IP address, the VEA GUI will display the machine name of the cluster node that currently owns the virtual name and IP resources. Therefore, it is not recommended to use the virtual name or virtual IP address when connecting and administering a cluster node through SFW HA. Instead, use the actual machine name or the IP address of the cluster node.
- Cluster dynamic disk groups that contain iSCSI disks are not set up for persistent login on all nodes in the cluster.
SFW ensures that the iSCSI targets of cluster dynamic disk groups that contain iSCSI disks are configured for persistent login. If the persistent login is not configured for the target, SFW automatically configures it. Cluster dynamic disk groups that contain iSCSI disks are only automatically configured for persistent login on the node where they were created. The other nodes in the cluster are not enabled for persistent login. You need to manually set up the persistent login for each of the other nodes in the cluster.
- Copying the Policy File, VxVolPolicies.xml, to Another Node
If the second node is configured the same as the first and if the first node's policy settings for Automatic Volume Growth and VxCache are to be maintained on the second node, then you need to copy the VxVolPolicies.xml file of the first node to the second node. Copy the VxVolPolicies.xml file to the same path location on the second node as its location on the first node. The default path of the VxVolPolicies.xml file is **Documents and Settings\All Users\Application Data\Veritas**.
For additional information about the policy file, see the following topics:
 - [“Automatic volume growth”](#) on page 246
 - [“More on the policy file”](#) on page 560
- SFW support of the VCS environment allows the selection of SCSI-2 reservation mode or SCSI-3 reservation mode. Selecting the type of SCSI support for the VCS environment is done by using the System Settings portion of the SFW Control Panel.

When selecting the type of SCSI support in a VCS environment, it is important to know if your storage arrays support SCSI-3. SFW SCSI-3 clustering support does not allow you to mix storage arrays that support SCSI-3 with storage arrays that cannot. In a situation of mixed storage arrays, you must use SFW SCSI-2 clustering support. Refer to the HCL for arrays that support SCSI-3.

Note: Veritas maintains a Hardware Compatibility List (HCL) for Veritas Storage Foundation & High Availability Solutions 5.1 for Windows Products on the Symantec Support web site. Check the HCL for details about your storage arrays before selecting the type of SCSI support in a VCS environment.

After selecting the type of SCSI support, you must issue the following CLI commands to complete the setting on your system.

- `net stop vxvm`
- `net start vxvm`

Note: If a cluster disk group is imported on the system, you must deport or move the cluster disk group to another system before issuing these CLI commands.

Note: If SFW SCSI-2 clustering support is selected and Active/Active load balancing is desired, the SCSI-3 Persistent Group Reservations (SCSI-3 PGR) support mode must be enabled for the DMP DSM. For more information about enabling SCSI-3 PGR (Windows Server 2003 only), see “[Active/Active and Active/Passive settings in a cluster environment](#)” on page 723 and “[vxdlmpadm](#)” on page 388.

Implementing disaster recovery with VVR

- [Overview of VVR](#)
- [Summary of the steps for setting up a disaster recovery solution with VVR](#)
- [VVR terms](#)

Overview of VVR

Veritas Volume Replicator Option (VVR) is a data replication tool designed to maintain a consistent copy of application data at a remote site as part of an effective disaster recovery plan. In the event that the data center is down, the application data is immediately available at the remote site, and the application can be restarted at the remote site.

VVR works as a fully integrated component of SFW or SFW HA. VVR benefits from the robustness, ease of use, and high performance of SFW or SFW HA and, at the same time, adds replication capability. VVR can use existing SFW or SFW HA configurations, with some restrictions. Any application, even with existing data, can be configured to use SFW transparently.

For detailed information about VVR, refer to the *Veritas Storage Foundation Volume Replicator Option, Administrator's Guide*.

Note: Dynamic disks belonging to a Microsoft Disk Management Disk Group do not support VVR.

VVR feature highlights

The following are some of the feature highlights of VVR:

- Supports replication of data over any IP network, LAN or WAN.
- Runs on all storage hardware supported by Veritas Storage Foundation for Windows.
- Supports replication over a firewall.
- Provides volume-level replication of application or file system data, including support of commercial database management systems.
- Replicates the data in asynchronous or synchronous mode, ensuring complete data integrity and consistency in either mode.

How VVR works

VVR's purpose is to replicate data from a primary site to one or more secondary sites. It does this by using a replicated volume group (RVG) within a SFW disk group as the unit of replication.

Following is a summary of how VVR works:

- Through the VVR software, the volumes to be replicated on the primary site are identified as part of an RVG, which consists of one or more volumes in a SFW disk group. If you have multiple disk groups with volumes to be

replicated, each disk group must have a separate RVG. It is possible to have more than one RVG per disk group.

- With each RVG, a Replicator Log volume is also set up. The Replicator Log volume at the primary site holds the writes that are to be sent to the secondary site.
- A corresponding RVG and Replicator Log volume at the secondary site are also set up.

An identical disk group and volume setup is created on the secondary site. The disk groups and volumes must be of the same size and have the same names as those on the primary site. The volumes do not have to be the same volume type.

The Replicator Log volume on the secondary site must have the same name as on the primary site, but its size can differ. However, Symantec recommends that the two log volumes be the same size.

The secondary site Replicator Log is held in reserve so that it can be used if the primary site goes down or has to be migrated and the secondary site needs to become the new primary site.
- The RVG at the primary site and the corresponding RVG at the secondary site are called a Replicated Data Set (RDS). Most VVR commands operate on an RDS. Normally, you can perform VVR operations from any host in an RDS.
- Once the VVR components are properly installed and configured, replication starts.

VVR uses the Replicator Log volume on the primary site to track all the writes to the application or file system in the order that they were received and then transmits the writes to the secondary site. Each write to a data volume under an RVG on the primary site generates two writes: the first one is sent to the Replicator Log, and when that is complete, the other is sent to the application data volumes and to the secondary site at the same time.

When the secondary system receives a write, it sends an initial acknowledgment of the receipt back to the primary site, even before the write is committed to disk. This is called the “Network Acknowledgment.” Once the secondary commits the write to disk, a second acknowledgment, called the “Data Acknowledgment,” is sent to the primary system. The Replicator Log volume on the primary system discards the write when it receives the Data Acknowledgment.

Replication is a unidirectional process. The updates on the primary host are sent to the secondary host, but access to the data at the secondary host or hosts is read-only on the replication volumes.

- The three modes of replication – synchronous, asynchronous, and synchronous override – work as follows:
 - The synchronous mode waits until the Network Acknowledgment has been received from the secondary host before it completes the write to the application. Thus, the primary and the secondary have the same data.
 - The asynchronous mode completes the application write after it has been written to the primary Replicator Log volume.
If the primary site goes down, there may still be some writes that were not yet received at the secondary site. This mode has better performance but with a risk of some data loss.
 - The synchronous override is a mode of replication that is synchronous as long as the network is available, but when the network becomes unavailable, the replication is continued in the asynchronous mode.
- If a disaster occurs on the primary site and its data is destroyed, a secondary host can take over the role of the primary host to make the data accessible. You can then restart the application on that host.
- You can also manually migrate the role of a healthy primary host to a secondary host when the application involved in replication is inactive. You may want to do this for maintenance purposes.

Summary of the steps for setting up a disaster recovery solution with VVR

This section provides a high-level summary of the steps for setting up a VVR disaster recovery solution with SFW. For more detailed information, refer to the *Veritas Storage Foundation Volume Replicator Option, Administrator's Guide*.

These instructions do not give all the steps for setting up a cluster with VVR. For full details on clustering steps, see the *Veritas Storage Foundation and High Availability Solutions, Solutions Guide*. If you are using Microsoft Exchange Server 2003 or Microsoft SQL Server 2000, refer to the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft Exchange* or the *Veritas Storage Foundation and High Availability Solutions High Availability and Disaster Recovery Solutions Guide for Microsoft SQL*.

All the guides are included on the product CD.

- 1 Set up and configure the hardware at each site.
For VVR, installation requires at least two servers running SFW with a network connection between them: one as the primary at the main site and the other as the secondary at a second site. Optionally, you can have additional secondary sites.
If you plan to use clustering with SFW HA or with SFW and Microsoft Clustering, you have several configuration choices. Probably the most common one is to have four servers, two each clustered together at each site. You can also have a cluster with two servers, one node at the primary site and the other at the secondary. Another variation is for the primary site to have a two-node cluster while the secondary site has a standalone server for replication.
- 2 Install the operating system and configure the network.
- 3 Install SFW or SFW HA.
Be sure to select the VVR option.
With SFW HA, it is recommended that you purchase and install the Global Cluster Option (GCO) as well. GCO facilitates replication support after a site failure.
- 4 After the installation completes, the VVR Security Service Configuration wizard (VxSAS) will be launched.
Follow the instructions in the VVR documentation to configure this service, which is required for VVR commands to work properly.
- 5 Create one or more disk groups in SFW or SFW HA on your primary system. Then create the volumes within each disk group.

See “[Create dynamic disk groups](#)” on page 53.

See “[Create dynamic volumes](#)” on page 60.

You are creating the volumes to be replicated. You can create the volume for the VVR Replicator Log now or wait until you run the VVR wizard for setting up the Replicated Data Sets on the system.

The wizard allows you to either identify an existing volume for the log volume or to have the wizard bring up the screen for creating the volume so you can create the volume at that time.

- 6 If you plan to use an application on your system, you need to install and configure the application at this point.
- 7 On your secondary system, create a duplicate of the disk groups and volumes that are on the primary system. You can do this step in two ways:
 - Repeat the same manual procedures to set up the disk groups and volumes that you used previously on the primary system.
 - Wait until you run the VVR RDS wizard and allow VVR to make a duplicate of the disk groups and volumes for you.

The secondary disk groups and volumes should have the same names as the primary disk groups and volumes. The data volumes on the secondary site should be the same size as the corresponding data volumes on the primary site. The log volume on the secondary can be a different size, but Symantec recommends that the sizes be the same.

If you have installed an application on the primary site, it also needs to be installed on the secondary site.

- 8 If you have VCS or Microsoft Clustering clusters, create virtual IP resources for replication.

You will need to create a virtual IP resource that will be used for replication for each replicated disk group. In addition, if you are using VCS, you need to specify a NIC resource. This NIC resource is not needed for a Microsoft Clustering cluster. Create the IP resource on both the primary and secondary sites. Each site needs its own IP address. This virtual IP should be linked to the NIC that is used for the server at each site.

- 9 Set up the Replicated Data Sets for VVR.

Refer to the *Veritas Storage Foundation 5.1 Veritas Volume Replicator, Administrator's Guide* or the Veritas Storage Foundation Solutions Guides for detailed instructions. At the end of the procedure, you can have the replication start immediately.

At this point, if you do not have a clustered system, replication is set up. You will want to familiarize yourself with VVR's monitoring and disaster recovery procedures by reading the *Veritas Storage Foundation 5.1 Veritas Volume Replicator, Administrator's Guide*.

VVR terms

This section provides the definitions of the most commonly used VVR terms for reference purposes.

Replicated Volume Group (RVG)

An RVG is made up of one or more volumes in a SFW disk group. The updates made on the RVG on the primary host are sent to a configured secondary host. Thus, there is a corresponding RVG with a disk group of the same name and volumes with the same names. The data volumes should be the same size, but Replicator Log volume sizes can differ. Optionally, to add more redundancy, you can have multiple secondary hosts, all with the same corresponding copy of the RVG on the primary host.

An RVG within a disk group is the container for replication, so if you have multiple disk groups, you will need to create a separate RVG for each disk group. It is possible to have more than one RVG in a disk group; however, the RVG cannot span across disk groups.

Replicated Data Set (RDS)

An RVG on the primary host and the corresponding duplicate RVG on the secondary host or hosts make up a Replicated Data Set (RDS).

Replicator Log

Each RVG must have a Replicator Log associated with it. The Replicator Log volume at the primary site holds a copy of any data writes that are sent to the secondary site. The Replicator Log on the secondary site is held in reserve so that it can be used if the primary site becomes nonfunctional and the secondary site takes over the role of primary site. The logs at the two sites must have the same name; however, the sizes of the logs can differ. Symantec recommends having Replicator Log volumes of the same size at the primary site and the secondary site.

Replication Modes

The three modes of replication –synchronous, asynchronous, and synchronous override – work as follows:

- The synchronous mode waits until the Network Acknowledgment has been received from the secondary host before it completes the write to the application. Thus, the primary and the secondary have the same data.
- The asynchronous mode completes the application write after it has been written to the primary Replicator Log volume.
If the primary site goes down, there may still be some writes that were not yet received at the secondary site. This mode has better performance but with a risk of some data loss.
- The synchronous override is a mode of replication that is synchronous as long as the network is available, but when the network becomes unavailable, the replication is continued in the asynchronous mode.

Glossary

Use this glossary to find explanations of terms that relate to the Veritas Storage Foundation for Windows software.

Active/Active

The mode in which DMP allocates the data transfer across the possible paths to and from an array, thus enabling the desirable feature of load balancing. With this mode, DMP implements a round-robin algorithm, selecting each path in sequence for each successive data transfer to or from a disk. For example, if you have two paths active, A and B, the first disk transfer occurs on path A, the next on path B, and the next on path A again.

See also the Active/Passive and Load Balancing glossary entries.

Active Partition or Volume

The partition or volume from which the computer starts up. On a basic disk, the active partition must be a primary partition. For a dynamic disk, a dynamic volume cannot be marked active directly. However, you can upgrade a basic disk with a system partition to dynamic. After the disk is upgraded and the computer is rebooted, the system partition becomes a system volume, which retains its active status.

Upgrading a basic disk with a system partition to a dynamic disk preserves the partition table information, which is required when reinstalling the Windows operating system.

See also the Boot Partition or Volume and the System Partition or Volume glossary entries and the section [“Mark a partition as active”](#) on page 190.

Active/Passive

The mode in which DMP allocates data transfer to and from an array across a path designated as the “Preferred Path.” The Preferred Path is always active, and the other path or paths act as backups that are called into service if the current operating path fails. This option does not provide load balancing.

See also the Active/Passive and Load Balancing glossary entries.

Automatic Volume Growth Based on Capacity

This command allows a selected volume to automatically grow in size when it reaches a certain percentage of capacity. With Automatic Volume Growth, you can conserve disk space on your servers because space is distributed to users on an as-needed basis, and you do not have to be available to allocate the new disk space.

For full details on the procedure, see Automatic volume growth.

Basic Disk

A basic disk adheres to the partition-oriented scheme of Windows NT, Windows 95/98, and MS-DOS. Basic disks can also contain RAID volumes that were created in NT Disk Administrator, including spanned volumes (volume sets), mirrored volumes (mirror sets), striped volumes (stripe sets), and RAID-5 volumes (stripe sets with parity). In addition, CD-ROMs and other removable-media disks are considered basic disks.

See also the section [“What can you do with a basic disk?”](#) on page 183.

Basic Group

A disk group that contains all the basic disks on a server.

See also the Disk Group and Dynamic Disk Group glossary entries.

Basic Volume

In SFW, basic volumes refer to all the volumes that are on basic disks. Basic volumes can be primary or extended partitions, simple logical drives that reside on extended partitions, or RAID volumes that were originally created in Windows NT Disk Administrator.

Boot Partition or Volume

The volume, formatted with an NTFS, FAT, or FAT32 file system, that contains the Windows operating system and its support files. The boot volume can be in the same location as the system volume. In Windows, the system partition or volume is the one the computer starts from, while the boot volume is the one that has the operating system and support files.

See also the System Partition or Volume glossary entry.

Capacity Monitoring

Refers to SFW’s capability of monitoring dynamic volume capacities, so that when any volume reaches preset size thresholds, the user is notified with an alert message.

See the section [“Capacity monitoring”](#) on page 244.

Column

A column refers to an area on the disk where all or a portion of the volume resides. Striped volumes, RAID-5, and mirrored striped (RAID 0+1) volumes contain multiple columns. Other volume types contain one column.

Concatenation

Storing data either on one disk (simple) or on disk space that spans more than one disk (spanned).

Critical Threshold

The percentage of volume capacity at which SFW reports an error. The default is 90%.

See the section [“Capacity monitoring”](#) on page 244.

Dirty Region Logging (DRL)

Dirty region logging (DRL) uses a log-based recovery method to quickly resynchronize all the copies of a mirrored volume when a system is restarted following a system crash. A log can be created when a volume is created, or it can be added later.

See also [“Dirty region logging for mirrored volumes”](#) on page 274.

Discovery Domain

A Discovery Domain (DD) is a security and management mechanism used by iSNS Servers to administer access and connectivity to iSCSI initiators or iSCSI targets (storage nodes) in an iSCSI SAN.

Discovery Domain Set

A Discovery Domain Set (DDS) is a mechanism in an iSCSI SAN to store sets of discovery domain mappings in an iSNS database. A discovery domain set may contain one or more

discovery domains and a discovery domain can be a member of one or more discovery domain sets.

Disk

A physical data storage device attached to a computer.

See also the [Basic Disk](#) and [Dynamic Disk](#) glossary entries.

Disk Evacuation

The Evacuate Disk command moves the entire contents of a healthy disk to the free space on one or more dynamic disks. If there is a failed volume on the original disk, the volume cannot be moved and an error message will appear.

See also “[Evacuate disk](#)” on page 148.

Disk Group

SFW organizes disks into disk groups. Disk groups provide a way of organizing disks in a system and simplifying storage management for systems with large numbers of disks. They also allow you to move disks between computers so that you can easily transfer the storage between computers.

All basic and dynamic volumes are required to be in a disk group. There is only one disk group for basic disks, known as the Basic Group. There can be one or more dynamic disk groups, which are known as dynamic groups. Disks within a dynamic group share a common configuration. Dynamic volumes are created within a dynamic group and are restricted to using disks within that group.

See also “[About disk groups](#)” on page 194.

Disk Replacement

The Replace Disk command allows you to replace a failed disk with an empty basic disk. The volume configuration will be recreated on the new disk. The contents of nonredundant volumes are not guaranteed. Redundant volumes will be automatically resynchronized.

See also “[Replace disk](#)” on page 148.

Disk Signature

The disk signature identifies the disk to the operating system. Windows requires that a disk have a signature before it can be used. Once a signature is written on a disk, the disk will display as a basic disk.

See also “[Disk type shows no signature](#)” on page 496 and “[Add a disk signature to a disk](#)” on page 139.

Disk Striping

Disk striping writes data across multiple disk drives instead of just one disk. Disk striping involves partitioning each drive storage space into stripes that can vary in size. These stripes are interleaved in a repeated sequential manner. The combined storage space is composed of stripes from each drive.

See also “[RAID level 0 \(Striping\)](#)” on page 32.

DMP

See the glossary term [Dynamic Multi-pathing](#).

Drive Path

A drive path refers to the path to a local drive that is mounted at an empty folder on an NTFS volume. For more about drive paths, see “[Mount a volume at an empty folder \(Drive path\)](#)” on page 170.

Dynamic Disk

A dynamic disk is a physical disk that can contain dynamic volumes created with SFW. A dynamic volume organizes space on one or more physical disks by using a specific type of volume layout. The six types of dynamic volume layouts are simple, spanned, mirrored, striped, RAID-5, and mirrored striped (RAID 0+1). In SFW’s New Volume command, the simple and spanned layouts are grouped together under the concatenated category.

On a dynamic disk, space is organized through volumes rather than partitions. Because a dynamic disk does not have the partitioning scheme used by Windows NT, Windows 95/98, and MS-DOS, you cannot access dynamic disks through those operating systems.

See also the Basic Disk glossary entry.

Dynamic Disk Group

A dynamic disk group contains dynamic disks and dynamic volumes. In SFW and earlier versions of Volume Manager for Windows, you can have multiple dynamic disk groups.

See also “[About disk groups](#)” on page 194.

Dynamic Multi-pathing

Veritas Dynamic Multi-pathing is a software option that is available with SFW. Dynamic Multi-pathing adds fault tolerance to disk storage by making use of multiple paths between a computer and individual disks in an attached disk storage system. Disk transfers that would have failed because of a path failure are automatically rerouted to an alternate path. With Dynamic Multi-pathing, the Veritas Enterprise Administrator console allows you to configure, manage, and obtain status information about these multiple paths. Dynamic Multi-pathing also improves performance by allowing load balancing between the multiple paths.

SFW offers Dynamic Multi-pathing as DMP DSMs.

DMP DSMs are designed to support a multipath disk storage environment set up with the Microsoft multipath input/output (Microsoft MPIO) solution. DMP DSMs work effectively with Windows to provide a fault tolerant multipath disk storage environment. DMP DSMs provide Windows Storport driver support.

For more about Veritas Dynamic Multi-pathing, see “[Dynamic multi-pathing software](#)” on page 717.

Dynamic Volume

Dynamic volumes are volumes created on dynamic disks by using SFW. On a dynamic disk, storage is divided into dynamic volumes instead of partitions. A dynamic volume consists of a portion or portions of one or more physical disks and is organized in one of five volume layout types. SFW’s five types of dynamic volumes—concatenated, mirrored, striped, RAID-5, and mirrored striped (RAID 0+1)—are described in the section “[Dynamic volume types](#)” on page 67. The size of a dynamic volume can be increased if the volume is formatted with NTFS and there is unallocated space on a dynamic disk within the dynamic disk group onto which the volume can be extended. See “[Expand a dynamic volume](#)” on page 177 for further information.

You can create any number of dynamic volumes in the unallocated space on a disk or create volumes that span two or more disks. Each volume on a disk can have a different file system, such as the file allocation table (FAT or FAT32) file system or the Microsoft Windows NT file system (NTFS).

Dynamic Relayout

SFW feature that allows you to reconfigure the layout of a volume without taking it off-line. You can change a volume's layout from concatenated to striped, striped to concatenated, and striped to another striped volume with a different number of columns and stripe unit size. The command is implemented through the **Add Mirror** window.

Extended Partition

A portion of a basic disk that can contain logical drives. Use an extended partition if you want to have more than four volumes on your basic disk. A basic disk can contain up to four primary partitions or three primary partitions plus an extended partition. The extended partition can be further divided into up to 32 logical drives.

See also the Basic DiskLogical DrivePartitionand Primary Partition glossary entries.

FastResync (FR)

FastResync is a part of the Veritas FlashSnap feature. FR supports resynchronization of mirrors by copying only changes to the temporarily split mirror by using FR logging. This reduces the time it takes to rejoin a split mirror to the mirror set and also reduces the server CPU cycles needed to complete the resynchronization. This feature's added functionality makes the process of splitting a mirror off for tasks such as third mirror backup, data mining, and snapshots much easier to implement. FastResync can also be used on ordinary mirrored volumes to speed up resynchronization.

See also "[FastResync](#)" on page 570.

FAT and FAT32

FAT and FAT32 are file systems that are defined as follows:

FAT (File Allocation Table) – A file system used by MS-DOS, Windows 3.x, and Windows 95/98. All later Windows operating systems also can use the FAT file system. The operating system maintains a table to keep track of the status of various segments of disk space used for file storage.

FAT32 (File Allocation Table) – A derivative of the file allocation table (FAT) file system. FAT32 supports smaller cluster sizes than FAT, thus providing more efficient space allocation on FAT32 drives. FAT32 is designed for larger disks than FAT.

See also the NTFS glossary entry.

Failover

With the Dynamic Multi-pathing (DMP) software, failover refers to the automatic process where an alternative path to data on a storage array is activated when the current data path fails.

Fault Tolerance

The characteristic of ensuring data integrity and system functionality when hardware failures occur.

FlashSnap

Veritas FlashSnap is a multi-step process that allows you to create independently addressable snapshot volumes that are copies or mirrors of the volumes on your server. These snapshot volumes can be easily moved to another server for backup or other purposes, such as loading or updating data warehouses or performing application testing with real production data while business continues.

FlashSnap makes use of FastResync, several Snapshot commands, and the Dynamic Disk Group Split and Join commands. See the chapter “[FlashSnap](#)” on page 563.

Foreign Disk

The status of a dynamic disk that was created on another computer and moved to the current computer, or the status of a disk that was moved or deleted from a computer and then returned to it.

See “[Merge foreign disk command](#)” on page 487 and “[Bring a foreign disk back to an online state](#)” on page 479.

Free Space

Available space that can be used to create a primary or extended partition or a logical drive on a basic disk or to create a dynamic volume on a dynamic disk.

FT Disk

Refers to a disk that contains FT (fault tolerant) volumes that are created in Windows NT Disk Administrator. See the next entry for definition of FT volumes.

FT Volume

Refers to a RAID volume that was originally created in Windows NT Disk Administrator. These volumes include spanned volumes (volume sets), mirrored volumes (mirror sets), striped volumes (stripe sets), and RAID-5 volumes (stripe sets with parity). The FT refers to fault tolerant, even though some of the volume sets are not fault tolerant.

Windows Server 2003 and later versions of Windows does not support FT volumes; however, if you are running Windows 2000, SFW can maintain and repair these volumes, but it cannot recreate them. You can, however, upgrade a disk that contains these volumes to dynamic, and the volumes will be converted to dynamic volumes of the corresponding type. Versions of SFW that are earlier than SFW 5.0 provide support for this operation.

Hot Relocation

When a disk fails, hot relocation automatically moves all subdisks from redundant volumes on the failed disk to hot spare disks, or to free space on other disks if enough space is not available on hot spare disks.

See also “[Hot relocation](#)” on page 268.

Hot Spare

If there are I/O errors anywhere on a disk, all healthy subdisks and subdisks of redundant volumes on that disk will automatically be moved to a designated spare disk.

See also “[Hot relocation](#)” on page 268.

Hot Spot

A hot spot is an area of high I/O activity that may cause bottlenecks in I/O throughput. The Online Monitoring window displays a hot spot indicator. For more information, see “[Online monitoring window features](#)” on page 522.

iSCSI initiator

An iSCSI initiator is a server that initiates requests to and receives responses (I/O) from an iSCSI target.

iSCSI SAN

An iSCSI SAN is a storage array network that uses the iSCSI protocol that is built on top of TCP/IP for block level I/O.

iSCSI target

The data stored in an iSCSI SAN is stored on iSCSI targets. An iSCSI target can be a hardware array or a software iSCSI target node such as Microsoft's iSCSI Software Target.

iSNS server

A server in an iSCSI SAN that processes iSNS registrations and queries from iSNS clients. It maintains a database to manage the registrations.

Load Balancing

Refers to the process of balancing the data load between disks so that I/O demands are spread as evenly as possible across an I/O subsystem's resources. With SFW, load balancing is achieved either by moving subdisks between disks or by using the Active/Active path configuration with DMP to distribute the data load across multiple disks.

Logical Drive

A logical drive is a simple volume that resides on an extended partition on a basic disk. Logical drives are limited to the space on the extended partition. They cannot span multiple disks. A logical drive can be formatted and assigned a drive letter.

An extended partition can be subdivided into as many as 32 logical drives. You can use all or part of the free space in an extended partition when creating logical drives.

See also the Basic DiskBoot Partition or Volume and Extended Partition glossary entries.

LUN

Logical Unit Number – The number that, when combined with the Target ID, uniquely identifies a disk on the port.

Mirrored Striped Volume

RAID 0+1 volumes are mirrors of striped volumes. For example, a two-disk stripe can be mirrored to two additional disks. This RAID type provides the advantages of both speed (from striping) and fault tolerance (from mirroring). You can add more mirrors to a mirrored striped volume, and you can extend this type of volume onto additional dynamic disks within the dynamic disk group.

See also "[RAID level 0+1 \(Mirrored striped volumes\)](#)" on page 34.

Mirrored Volume (RAID-1)

A mirrored dynamic volume is a fault-tolerant volume that duplicates your data on two or more physical disks. A mirror provides redundancy by simultaneously writing the same data onto two or more separate mirrors (or plexes) that reside on different disks. If one of the disks fails, data continues to be written to and read from the unaffected disk or disks. SFW supports up to 32 mirrors.

In contrast, the mirrored volumes originally created in Disk Administrator and supported for use on basic disks have only two mirrors.

A mirrored volume is slower than a RAID-5 volume in read operations but faster in write operations. You can create mirrored volumes only on dynamic disks. In SFW, you can extend mirrored volumes.

See also “[RAID level 1 \(Mirroring\)](#)” on page 33.

Monitor Interval

DMP (Dynamic Multi-pathing) monitors the paths to an array to determine whether they are functioning properly. The monitor interval specifies the time interval for the monitoring of that array.

MPIO

See the glossary term Dynamic Multi-pathing.

NTFS

An advanced file system designed for use specifically within Windows operating systems. It supports file system recovery, extremely large storage media, long file and folder names, and file and folder compression. NTFS is also called the Windows NT file system.

If you want to extend a dynamic volume in SFW, you must format it with NTFS.

See also the FAT and FAT32 glossary entry.

Off-Host Backup

Refers to a situation in which the processing of the backup of a server is moved to another server. This allows the applications on the working server to be maintained at a consistently higher performance level because the backup is performed on another machine. In SFW, off-host backup is done by using the FlashSnap process.

Parity

Redundant information that is associated with a block of information. Parity is a calculated value used to reconstruct data after a failure.

RAID-5 volumes stripe data and parity intermittently across a set of disks. Within each stripe, the data on one disk is parity data and the data on the other disks is normal data. RAID-5 volumes, therefore, require at least three disks to allow for this extra parity information. When a disk fails, Symantec software uses the parity information on the good disks to recreate the data on the failed disk.

See the RAID-5 Volume glossary entry, as well as “[RAID level 5 \(Striping with distributed parity\)](#)” on page 33.

Partition

A portion of a physical disk that functions as though it were a physically separate disk. Partitions can be created only on basic disks. Partitions cannot span disks; they must be contiguous regions. When a basic disk that contains partitions is upgraded to a dynamic disk, the partitions become simple volumes on the dynamic disk.

See also the Extended Partition Primary Partition and System Partition or Volume glossary entries.

Plex

A plex refers to an instance of the volume. Mirrored volumes have two or more plexes. All other volumes have one plex.

Plexes, columns, and subdisks are the constituent parts of the volume.

Polling Interval

The polling interval is the interval at which SFW checks volume capacities. The minimum and default value is 20 seconds. See the section “[Capacity monitoring](#)” on page 244.

Preferred Path

The Preferred Path command on the DMP menu is used to specify the currently selected path as the Preferred Path to the disk. This menu option is available only when the operational mode for the array’s paths to the disks is specified as Active/Passive. The Preferred Path is the path that is used to transfer data to and from the disks.

See also the glossary entries [Active/Active](#) and [Active/Passive](#)

Primary Disk Group

The disk group that contains the computer’s boot or system disk. All other dynamic disk groups are called secondary disk groups. If none of the dynamic disk groups on a system contain the boot or system disk, then there is not a primary disk group. For more on primary and secondary disk groups, see “[Primary and secondary dynamic disk groups](#)” on page 195.

Primary Partition

A volume you create by using unallocated space on a basic disk. Microsoft Windows NT and other operating systems can start from a primary partition. You can create up to four primary partitions on a basic disk, or three primary partitions and an extended partition. Primary partitions can be created only on basic disks and cannot be subpartitioned. However, the extended partition can be further divided into as many as 32 logical drives. See also the [Partition](#) and [Extended Partition](#) glossary entries.

Projection

In the Disk View, the Projection command highlights all the subdisks associated with a selected volume and shows the volume configuration across disks.

See also “[Projection](#)” on page 109.

Providers

In SFW, providers are similar to drivers. Each provider manages a specific hardware or software storage component. For example, there is a disk provider that manages all disks that the Windows operating system sees as disks. The providers discover the existing physical and logical entities and store that information in SFW’s distributed database. Normally, providers operate in the background. The only time you might encounter a provider situation is when there is a provider error on startup. See “[Deal with a provider error on startup](#)” on page 483 for more information.

RAID

RAID (Redundant Array of Independent Disks) is a collection of specifications that describe a system for ensuring the reliability and stability of data stored on large disk subsystems. For full details on the RAID terminology and the RAID levels that Symantec software supports, see “[SFW’s software RAID](#)” on page 30.

RAID-5 Logging

RAID-5 logging ensures prompt recovery of a RAID-5 volume after a system crash. With RAID-5 logging, updates need to be made only to the data and parity portions of the volume that were in transit during the system crash. Thus, the entire volume does not have

to be resynchronized. A log can be created when a volume is created, or it can be added later.

See also [“RAID-5 logging”](#) on page 274.

RAID-5 Volume

A RAID-5 volume is a fault-tolerant volume with data and parity striped intermittently across three or more physical disks. Parity is a calculated value that is used to reconstruct data after a failure. If a portion of a physical disk fails, the data on the failed portion can be recreated from the remaining data and parity. You can create RAID-5 volumes only on dynamic disks. You cannot mirror RAID-5 volumes.

See also the section [“RAID-5 volumes”](#) on page 69.

RAID 0+1 Volume

See the glossary entry [Mirrored Striped Volume](#)

Region

Contiguous area of storage on a disk. These regions can also be referred to as subdisks.

See the glossary entry [Subdisk](#)

Same-Host Backup

Refers to a situation in which the backup process of a server is done on the server itself. This is the most common method of backup. Same-host backup can be done by using the FlashSnap procedure.

Secondary Disk Group

Any dynamic disk group that is not primary. A primary disk group is a dynamic disk group that contains the computer's boot or system disk. All other dynamic disk groups are called secondary disk groups. For more on primary and secondary disk groups, see [“Primary and secondary dynamic disk groups”](#) on page 195.

Simple Dynamic Volume

A simple dynamic volume consists of a single contiguous region (or subdisk) on a single physical disk.

Simple dynamic volumes can be extended or mirrored. You can extend a simple volume within the same disk or onto additional disks.

When a basic disk with a partition is upgraded, the partition becomes a simple volume. An extended partition on a basic disk also becomes a simple volume when the disk is upgraded to dynamic.

See also [“Simple volumes”](#) on page 67.

Spanned Volume

A volume made up of disk space on more than one physical disk. You can add more space to a spanned volume by extending it at any time. You can create spanned volumes only on dynamic disks. Spanned volumes by themselves are not fault tolerant. However, they can be mirrored to be made fault tolerant.

See also [“Spanned volumes”](#) on page 67.

Statistics Threshold

The statistics threshold is the minimum amount of I/O per second that a disk or subdisk has to have to display a color other than blue on its status icon. Blue designates the lowest

state, Low I/O activity. The default threshold is 15. You set this threshold in the Online Data Display Options window. For details, see the section “[Selecting online display options](#)” on page 525.

Striped Volume (RAID-0)

A volume that stores data in stripes on two or more physical disks. Data in a striped volume is allocated alternately and evenly (in stripes) to the disks of the striped volume. You can create striped volumes only on dynamic disks. Striped volumes by themselves are not fault tolerant; however, they can be mirrored to be made fault tolerant. They also can be extended.

See also “[Striped volumes](#)” on page 68.

Subdisk

Refers to a region of contiguous space on a disk. Subdisks are the basic units in which Veritas Storage Foundation for Windows allocates disk space in a volume. A SFW disk can be divided into one or more subdisks. Each subdisk represents a specific portion of the volumes on a dynamic disk.

A SFW disk may contain multiple subdisks, but subdisks cannot overlap or share the same portions of a SFW disk. Any SFW disk space that is not part of a subdisk is considered to be unallocated space, which can be used to create new volumes.

You can move subdisks to improve disk performance. For information about moving subdisks, see “[Moving subdisks](#)” on page 544.

System Partition or Volume

The partition or volume that has the files needed to load the operating system. It is the same as the active partition or volume. In Windows, the system partition or volume is the one the computer starts from, while the boot volume is the one that has the operating system and support files. The system partition or volume and the boot partition or volume can be the same partition or volume.

See also the Active Partition or Volume and the Boot Partition or Volume glossary entries.

Target ID

The number that, when combined with the LUN, uniquely identifies a disk on the port.

Track alignment

In SFW, track alignment refers to the feature that allows you to set dynamic volumes to store blocks of data in alignment with the boundaries of the physical track of the disk. Storing data so that it is aligned with track boundaries helps optimize I/O performance.

Unallocated Space

Available disk space that is not allocated to any partition, logical drive, or volume. The type of object you can create on unallocated space depends on the disk type (basic or dynamic). For basic disks, you can use unallocated space outside partitions to create primary or extended partitions. You can use free space inside an extended partition to create a logical drive. For dynamic disks, you can use unallocated space to create dynamic volumes.

See also the Free Space glossary entry.

Volume

A volume is a logical entity that is made up of a portion or portions of one or more physical disks. A volume can be formatted with a file system and can be accessed by a drive letter or a mount path. Like disks, volumes can be basic or dynamic.

See also the Basic Volume and Dynamic Volume glossary entries.

Volume Read Policy

The volume read policy on a dynamic volume allows you to specify either that a particular mirror be used for reads or that all mirrors be read in turn in “round-robin” fashion for each nonsequential I/O detected.

See also “[Set the mirrored volume read policy](#)” on page 262.

Warning Threshold

The percentage of volume capacity at which SFW sends out a warning message. The default is 80%.

See the section “[Capacity monitoring](#)” on page 244.

Index

A

- accessing SFW 43
- active partition or volume 805
- Active/Active (Dynamic Multi-pathing) 721
- Active/Passive (Dynamic Multi-pathing) 722
- Add Disk to Dynamic Disk Group command 141
- Add Private Dynamic Disk Group Protection command 211
- add, change, or remove a drive letter or path 167
- adding
 - disks to a dynamic disk group 141
 - disks to your system 138
 - mirrors 258
 - paths (MPIO) 735
 - private dynamic disk group protection 211
- adding or changing a partition or volume label 172
- Alert Log 234
- Array Primary Path (MPIO) 733, 742
- Array Settings (MPIO) 730, 732, 747
- Automated System Recovery (ASR) 513
- Automatic Volume Growth based on capacity 805

B

- basic disk
 - bringing back online 478
 - configuring 51
 - definition 39
 - functions 183
 - troubleshooting 191
 - upgrade to dynamic disk 191, 497
- basic volumes
 - bringing a basic volume back to a Healthy state 481
 - definition 40
 - expanding 180
 - repairing 481
 - troubleshooting 191
- boot partition or volume 806
 - see also dynamic boot or system volume
- booting from a SAN 327
- breaking a mirror 260

- bugcheck 7B error message 504

C

- Cancel Format 173
- capacity monitoring
 - introduction 244
- Change Drive Letter and Path command 167
- check partition or volume properties 174
- Chkdsk command 478, 479
- clear hot relocation information 272
- cluster, using with DGSJ 609
- columns, definition 41
- command line interface
 - main topic 281
 - typographical conventions 285
- concatenated volume type 32, 67
- conditions for remote connection 46
- configuration information, disk 29
- connecting to a remote computer, troubleshooting issues 502
- Control Panel 122
- creating
 - dynamic disk group 55
 - dynamic volumes 60
 - logical drives 189
 - mirrors 258
 - partitions 184
- critical threshold for capacity monitoring 806
- Customize Table Header command 100

D

- DCO volume
 - adding a mirror 573
 - does not display in Disk View 512
 - main topic 572
 - moving a subdisk 576
 - removing a mirror 575
 - Snap Prepare command 584
- degraded volume status 473
- deleting

- dynamic disk group 197
- logical drives 165
- mirror 261
- partitions 165
- volume 164, 165
- Deport Dynamic Disk Group command 205
- Destroy Dynamic Disk Group command 197
- Device Settings (MPIO) 731, 732, 748
- DGSJ, see Dynamic Disk Group Split and Join (DGSJ) 597
- Dirty Region Logging
 - adding logs 275
 - description 274
 - removing logs 276
- disconnected disk status 470
- disconnecting from a server 46
- disk evacuation 807
- disk groups
 - adding disks 141
 - basic disk group 194
 - cluster 196
 - creating 55
 - definition 41, 194
 - deleting, two methods 197
 - deporting 205
 - dynamic disk group 194
 - importing 207
 - Microsoft Disk Management Disk Group 41
 - partitioned shared storage 209
 - primary 195
 - private protection 196, 209, 210, 212
 - properties 213
 - renaming 201
 - repairing a volume with degraded data after
 - moving disks between computers 482
 - secondary 195
 - types 56
 - upgrading from earlier Volume Manager
 - version 199
- Disk Management
 - Disk Management compatible disk group 57, 215
 - problem after uninstalling SFW 500
 - use with VDS 30
 - Windows Disk Management Disk Group 57
- disk offset on a subdisk 543
- disk phaseout 540
- Disk View
 - context menu 110
 - expand disk 105
 - expanded view 106
 - Full Volume Display 108
 - main topic 103
 - nonexpanded view 106
 - options for graphical views 105
 - overview 103
 - print 105
 - Print command 104
 - projection 105, 109
 - Refresh View command 104
 - Show Legend command 104
 - Vol Details 105, 107
- Disk View tab 98
- disks
 - add a disk 138
 - add a signature 139
 - configuration information 29
 - Evacuate Disk command 148
 - names 287
 - no signature 496
 - properties 161
 - removing 145
 - Replace Disk command 148
 - Rescan command 147
 - S.M.A.R.T. Monitoring 242
 - Set Disk Usage 147
 - status descriptions 468
 - viewing 85
 - see also Dynamic disk and Basic disk
- DMP, see Dynamic Multi-pathing
- drive path 170, 172, 808
- dynamic boot or system volume
 - mirroring 264
 - problem with extending 498
 - problem with mirroring 499
 - setting up 70
- dynamic disk
 - attaching 203
 - bringing an Offline dynamic disk back
 - online 477
 - configuration information 29
 - definition 39
 - detaching 202
 - disk phaseout 540
 - foreign 333, 487
 - reactivating 491
 - rescan 485
 - revert to a basic disk 144

- see also Disks
- Dynamic Disk Group Split and Join (DGSJ)
 - Join Dynamic Disk Group 606
 - limitations with VVR 612
 - main topic 597
 - recovery 604
 - split Dynamic Disk Group 600
 - troubleshooting tips 612
 - using on a cluster 609
 - see also vxdg split, vxdg recover, vxdg join
- dynamic Disk Group Split and Join (DGSJ)
 - about Partial Disk Group Join 608
- dynamic disk groups
 - see disk groups
- dynamic mirrored striped volumes (RAID 0+1) 69
- dynamic mirrored volumes 68
- Dynamic Multi-pathing
 - Active/Active 721
 - Active/Passive 722
 - fault tolerance 720
 - main topic 717
 - overview 718
- Dynamic Multi-pathing (DMP)
 - troubleshooting issues 508
- dynamic RAID-5 volumes 69
- Dynamic Relayout 277
- dynamic simple volumes 67
- dynamic spanned volumes 67
- dynamic striped volumes 68
- dynamic volumes
 - advantages of 29
 - definition 40
 - types 67
 - see also volumes

E

- enable file and folder compression 189
- error symbols 476
- Evacuate Disk 148
- event log 236
- event monitoring
 - Alert Log 234
 - event log configuration 236
 - event log severity levels 235
- event notification
 - main topic 236
 - Rule Manager 237
 - SNMP MIB files for SFW 241
- expand a dynamic volume 177

- expand disk (Disk View) 105
- Expand Partition command 180
- Expand Volume command 177
- expanded view (Disk View) 106
- extended partition 809

F

- failed volume status 474
- failing disk status 471
- Fast File Resync (FFR) 614
- FastResync
 - enabling and disabling 572
 - limitations 570
 - main topic 570
 - reconnection 571
 - resynchronization 571
- FAT file system 188
- FAT32 file system 188
- fault tolerance 256, 720
- features, SFW general 23
- FFR, see Fast File Resync
- File System command 172, 173
- FlashSnap
 - main topic 563
 - off-host backup 567
 - overview 563
- foreign disk
 - bringing a foreign disk back online 479
 - definition 810
 - Merge Foreign Disk command 333, 487
 - status 468
- format a partition or volume 172
- formatting volume status 475
- free space 810
- FT volumes
 - definition 810
- Full Volume Display (Disk View) 108

G

- general disk functions
- Global Cluster Option (GCO) 27
- graphing window 531, 537
- GUID recycle 128
- guidelines for running SFW 79

H

- HBA caching with SFW 45

- healthy volume status 472
- Historical Statistics 531
- Historical Statistics Settings window 533
- hot relocation
 - clear hot relocation information 272
 - hot relocation mode 269
 - main topic 268
 - Set Disk Usage 270
 - undo hot relocation 271
- hot spot 523, 810

I

- Import Dynamic Disk Group command 207
- Import Failed disk status 471
- imported disk status 468
- iSCSI
 - about iSCSI SANs 218
 - about iSNS servers 218
 - configuring with SFW 220
 - discovery Domain (DD) definition 218
 - discovery Domain Set (DDS) definition 218
 - iSCSI target and iSCSI initiator overview 218
 - VEA iSCSI arrays node 227
 - VEA iSCSI initiators node 223
 - VEA iSNS server node 228
 - vxvg latestart command 322

J

- Join Subdisk command 547

L

- left pane, VEA GUI 91
- legends 99
- load balancing
 - Dynamic Multi-pathing 721
 - subdisk move 539
- logging
 - adding logs 275
 - dirty region logging for mirrored volumes 274
 - RAID-5 logging 274
 - removing logs 276
- logical drives
 - creating 189
 - definition 811
 - deleting 165
- logs 89
- lower pane, VEA GUI 102

M

- Mark Partition Active command 190
- Max Size button 60, 64
- Merge Foreign Disk command 333, 487
- MIB files 241
- Microsoft Cluster Service (MSCS) support
 - additional considerations 778
 - creating a cluster disk group 759
 - creating a dynamic mirrored quorum resource 773
 - installation after SFW is installed 757
 - making the disk group a cluster resource 761
 - overview 754
 - quorum arbitration time settings 777
 - resource properties in Cluster Administrator 770
- Microsoft Clustering Quorum arbitration time settings 777
- Microsoft Clustering support
 - how SFW works with Microsoft Clustering 756
- mirroring
 - adding a mirror 258
 - boot and system volume 264, 499
 - breaking a mirror 260
 - creating a mirror 258
 - difference between breaking and removing 259
 - dynamic Relayout 277
 - performance 68
 - problem creating 498
 - problem in mirroring a boot or system volume 499
 - reactivating a mirrored volume 264
 - removing a mirror 261
 - repairing a mirror 493
 - setting read policy 262
- missing volume status 475
- mount an NTFS volume at an empty folder 170
- Move Subdisk command 544
- moving disk groups between computers 205
- MPIO
 - adding and removing paths 735
 - Array Primary Path 742
 - Array Settings 730, 732, 747
 - Device Settings 731, 732, 748
 - load balancing settings for a disk 739
 - load balancing settings for an array 736, 745
 - menus 729
 - path status 750

- Primary Path 742
- properties 731, 734, 750
- Set Array Primary Path 733
- Set Primary Path 733
- MPIO, see Dynamic Multi-pathing
- MSCS. See Microsoft Cluster Service (MSCS)
- Support

N

- New Dynamic Disk Group command 55
- New Logical Drive command 189
- New Volume command 60
- No Disk Signature disk status 470
- No Media disk status 468
- nonexpanded view (Disk View) 106
- NTFS file system 188

O

- off-host backup 567
- offline disk status 470
- offline disk, bringing online 477
- Online Data Display Options window 526
- online disk status 468
- Online Monitoring window 522
- options
 - configuring 73
 - general description 25

P

- PAE, physical address extension 550
- parity 812
- Partial Disk Group Join 608
- partitioned shared storage 209
- partitions
 - check properties 174
 - creating 184
 - definition 184, 812
 - deleting 165
 - expanding 180
 - format 172
 - Mark Active command 190
 - refresh partition information 166
- path (MPIO)
 - adding 735
 - configuration 736
 - removing 735
 - status 750

- physical address extension, PAE 550
- ping disk command 145
- plex offset on a subdisk 543
- plex, definition 41, 812
- policy file 246, 560
- polling interval 813
- preferences, setting 76
- primary and secondary dynamic disk groups 195
- primary partition 813
- Primary Path (MPIO) 733, 742
- Print command (Disk View) 104, 105
- private dynamic disk group protection
 - adding 211
 - creating 210
 - deleted after an uninstall 501
 - main topic 209
 - removing 212
- projection (Disk View) 105, 109
- properties
 - disks 161
 - dynamic disk groups 213
 - partitions or volumes 174
 - paths related to MPIO 731, 734, 750
 - subdisks 542
- providers 28, 483, 813

Q

- queue depth 527
- quick format 189
- quorum arbitration time settings 777

R

- RAID level 0 (striped) 32
- RAID level 0+1 (mirrored striped) 34
- RAID level 1 (mirrored) 33
- RAID level 5 (striped with parity) 33
- RAID, definition 30
- RAID, hardware and software 35
- RAID-5 Logging
 - adding logs 275
 - description 274
 - removing logs 276
- RAID-5 volume
 - problem creating volume 498
 - repairing 493
- Reactivate Disk command 491
- Reactivate Volume command 264, 492
- real-time statistics 522

- rebuilding (regenerating) 472
- recovery for Dynamic Disk Group Split and Join 604
- recovery storage group (RSG) 640
- Refresh command 166, 485
- Refresh View command (Disk View) 104
- regenerating volume status 472
- region 814
- remote connection, conditions 46
- Remove Disk from Dynamic Disk Group 144
- Remove Private Dynamic Disk Group Protection command 212
- removing
 - disks 145
 - mirrors 261
 - paths (MPIO) 735
- repairing
 - basic volumes 481
 - dynamic mirrored volumes 493
 - dynamic RAID-5 volume 493
- Replace Disk 148
- Replication in Microsoft Exchange 641
- Rescan command 147, 485
 - 486
- resolving common problems 477
- resynching volume status 472
- right pane, VEA GUI 95
- Rule Manager 237

S

- S.M.A.R.T. Monitoring 242
- SAN, booting from 327
- SCSI protocol setting 129
- Search command 111
- search reports, creating 116
 - dynamic volumes
- Select Objects for Online Monitoring window 528
- Set Disk Usage 147, 270
- Set Volume Usage 262
- severity levels (events) 235
- Show Legend command (Disk View) 104
- SI 129
- SmartMove 130, 561
- snapshot commands
 - main topic 577
 - Prepare 580
 - Snap Abort 591
 - Snap Back 588
 - Snap Clear 590

- Snap Shot 585
 - see also vxassist prepare, vxassist snapshot, vxassist snapback, vxassist snapabort
- SNMP MIB files for Volume Manager 241
- software components, SFW 28
- software RAID, SFW 30
- Split Subdisk command 546
- Start Historical Data Collection window 536
- statistics
 - graphing window 531, 537
 - historical 531
 - Historical Statistics Settings window 533
 - hot spot 523
 - Online Data Display Options window 526
 - Online Monitoring window 522
 - queue depth 527
 - real-time 522
 - Select Objects for Online Monitoring window 528
 - setup steps for historical statistics 533
 - setup steps for real-time statistics 524
 - Start Historical Data Collection window 536
 - statistics parameters 519
 - Stop Historical Data Collection window 538
 - submenu 524
 - threshold 814
- status information, using 467
- Stop Historical Data Collection window 538
- stopped volume status 475
- striping 807
- Subdisk Move, Split, and Join
 - context menu 541
 - main topic 539
- subdisk Move, Split, and Join
 - Join Subdisk command 547
 - Move Subdisk command 544
 - Split Subdisk command 546
- subdisks
 - definition 41, 815
 - disk offset 543
 - plex offset 543
 - problem with customizing on a spanned volume 499
 - properties 542
- synchronized snapshots 681
- system partition or volume 815

T

- table headers, customizing 100

- Task Throttling command 133
- terms, SFW 39
- toolbar 88
- track alignment
 - Control Panel settings 134
 - vxdisk command 336
- tree view, VEA GUI 91
- troubleshooting
 - additional issues 496
 - cluster issues 505
 - commands used 485
 - common problems 477
 - connection issues 502
 - disk group issues 500
 - disk issues 496
 - disk status descriptions 468
 - DMP issues 508
 - issues related to boot or reboot 504
 - volume issues 498
 - volume status descriptions 472

U

- unallocated space 815
- undo hot relocation 271
- unknown group 500
- unmount a volume 171
- unsigned disk type 139
- upgrade a basic disk to dynamic disk 191
 - considerations 53
 - troubleshooting 497
- Upgrade Dynamic Disk Group Version
 - command 199

V

- VCS, see Veritas Cluster Server support
- Veritas Cluster Server (VCS) support
 - additional considerations 794
 - how SFW/HA works with VCS 784
 - integration steps 786
 - overview 784
- Veritas Enterprise Administrator GUI
 - Control Panel 122
 - features 84
 - left pane 91
 - lower pane 102
 - right pane 95
 - tree view 91
- Veritas Volume Replicator (VVR) support 797

- how VVR Works 798
- overview 798
- summary of steps for a DR solution 801
- VVR Terms 803
- View All Drive Paths command 172
- viewing
 - all disks associated with a volume 85
 - all drive paths (mounted volumes) 172
 - all volumes associated with a disk 85
 - array, disk, and path status (MPIO) 747
- Virtual Disk Service (VDS) 30
- Vol Details (Disk View) 105, 107
- volume label, adding or changing 172
- Volume Manager Disk Group resource type in
 - Microsoft Clustering 762
- volume read policy 262
- Volume Shadow Copy Service (VSS) 617
- volume size in the New Volume wizard 60
- volumes
 - advantages of dynamic 29
 - bringing a dynamic volume back to a Healthy
 - state 481
 - capacity monitoring 244
 - check properties 174
 - creating a dynamic volume 60
 - definition 816
 - deleting 164
 - expanding 177
 - formatting 172
 - names 285
 - reactivating a dynamic volume 492
 - refresh 166
 - repairing a basic volume 481
 - repairing a dynamic volume 481, 493
 - shredding 165, 359
 - shrinking 180
 - status descriptions 472
 - unmounting 171
 - viewing 85
- VSS snapshot
 - Microsoft Exchange 624
 - Microsoft SQL 673
 - VSS scheduler wizard 627, 677
- VVR, see Veritas Volume Replicator (VVR) support
- vxassist command
 - addlog 360
 - assign 373
 - break 354
 - create_drive 375

- create_ext 375
 - create_part 374
 - delete 358
 - delete_ext 375
 - growby 346
 - main topic 341
 - make 342
 - mirror 350
 - prepare 363
 - refresh 372
 - remove 355
 - rescan 372
 - resetbus 372
 - shred 359
 - shrinkby 349
 - snapabort 371
 - snapback 368
 - snapclear 369
 - snapshot 367
 - unassign 374
 - VxCache 549
 - vxcache command 461
 - vxubr command
 - backup 404
 - configuration backup GUI 124
 - restore 405
 - write_signature 406
 - vxclus command
 - cleanup 327
 - disable 327
 - enable 326
 - main topic 325
 - useSystemBus OFF 328
 - useSystemBus ON 327
 - vxdbg command
 - adddisk 307
 - deport 311
 - dginfo 304
 - import 309
 - init 304
 - join 320
 - latestart 322
 - list 304
 - main topic 302
 - protect 311
 - recover 319
 - release 312
 - repldisk 315
 - rmdisk 307
 - split 316
 - upgrade 312
 - vxdisk command
 - diskinfo 330
 - list 331
 - main topic 329
 - merge 333
 - reactivate 334
 - sig 335
 - vxdmadm command 388
 - allperf 392
 - arrayinfo 389, 390
 - deviceinfo 390, 391
 - pathinfo 390, 391
 - setattr array 398
 - setattr device 400
 - setattr path 402
 - vxevac command 377
 - vxfsync command 455
 - vxprint command 464
 - vxscrub command 456
 - vxsd command
 - join 380
 - main topic 379
 - mv 379
 - split 380
 - vxsnapsql command
 - main topic 447
 - vxstat command 381
 - vxunreloc command 378
 - vxverify command 459
 - vxvol command
 - growfs 296
 - main topic 288
 - rdpol prefer 294
 - rdpol round 295
 - reactivate 291
 - repair 289
 - set fastresync 290
 - volinfo 289
- ## W
- warning threshold for capacity monitoring 816
 - Windows Server 2003 features
 - Automated System Recovery (ASR) 513
 - Virtual Disk Service (VDS) 30
 - Volume Shadow Copy Service (VSS) 617
 - write caching with SFW 45