Veritas Storage Foundation™ and High Availability Solutions Installation and Upgrade Guide

Windows Server 2003, Windows Server 2008

5.1 SP1

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 Service Pack 1

Document version: 5.1.SP1.0

Legal Notice

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

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

Contacting Technical Support

Customers with a current maintenance 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 non-technical support Web page at the following URL:

customercare.symantec.com

Customer service

Customer Care information is available at the following URL:

www.symantec.com/customercare

Customer Service is available to assist with 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 maintenance 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

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

sfha_docs@symantec.com

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance 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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Section 1

Installation

Chapter 1

SFW and SFW HA preinstallation and planning

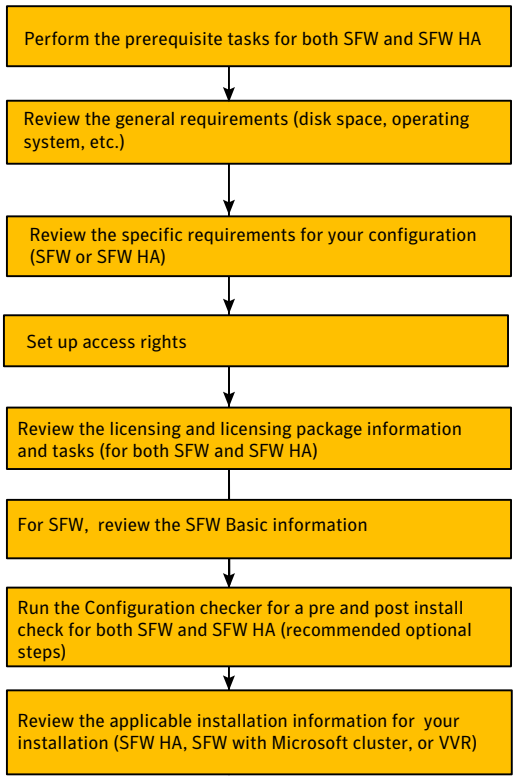
This chapter includes the following topics:

About SFW and SFW HA preinstallation planning and tasks

Before installing Veritas Storage Foundation 5.1 SP1 for Windows (SFW) or Veritas Storage Foundation High Availability 5.1 SP1 for Windows (SFW HA), you need to plan for the installation and perform some preinstallation tasks.

Figure 1-1 displays an overview of the SFW and SFW HA 5.1 SP1 preinstallation and planning tasks.

Figure 1-1 SFW and SFW HA 5.1 SP1 preinstallation and planning tasks



Prerequisites

Perform the following tasks before an installation:

- Review the release notes for your products
- Exit all running applications
- Review the product installation requirements

Requirements

Review the product installation requirements for your systems before installation. Minimum requirements and Symantec recommended requirements may vary. For the latest information on requirements for this release, see the following Symantec Technical Support TechNote:

http://entsupport.symantec.com/docs/303042

The following specific requirements should be reviewed before an installation:

- Disk space requirements
- Operating system requirements
- General requirements
- SFW requirements
- SFW HA requirements
- Access rights

Disk space requirements

For normal operation, all installations require a minimum of 50 MB of disk space in addition to the requirements listed in Table 1-1 below.

Table 1-1 summarizes approximate disk space requirements for SFW and SFW HA 5.1 SP1 on 32-bit and 64-bit systems.

Table 1-1 Disk space requirements

Installation options	Install directory or drive 32-bit	Install directory or drive 64-bit
SFW + all options + client components	1430 MB	1860 MB
SFW + all options	1140 MB	1400 MB
SFW Client components	590 MB	560 MB
SFW HA + all options + client components	1950 MB	2370 MB
SFW HA + all options	1520 MB	1880 MB
SFW HA Client components	780 MB	650 MB

Operating system requirements

SFW and SFW HA 5.1 SP1 have server and client components that run on specific Windows operating systems. For information about the supported Windows operating systems:

- SFW and SFW HA 5.1 SP1 software for servers:

See "SFW and SFW HA 5.1 SP1 software for servers" on page 20.

- SFW and SFW HA 5.1 SP1 software for clients:
  See "SFW and SFW HA 5.1 SP1 software for clients" on page 21.

For the latest information on supported software, see the Software Compatibility List at:

http://entsupport.symantec.com/docs/302145

SFW and SFW HA 5.1 SP1 software for servers

Your server must run one of the operating systems listed below to install the SFW or SFW HA 5.1 SP1 server software.

Note: SFW 5.1 SP1 software for servers supports Hyper-V and parent partitions. SFW HA 5.1 SP1 software for servers does not support Hyper-V and parent partitions.

- Windows Server 2003 x86: Web Edition (SP2 required)
- Windows Server 2003 x86, x64, IA64: Standard Edition, Enterprise Edition, Datacenter Edition (SP2 required for all editions)
- Windows Server 2003 R2 x86, x64: Standard Edition, Enterprise Edition, Datacenter Edition (SP2 required for all editions)
- Windows Server 2003 R2 x86, x64: Small Business Server (SP2 required)
- Windows Storage Server 2003 R2 x86, x64: Standard Edition, Enterprise Edition (SP2 required for these editions)
- Windows Unified Data Storage Server 2003 x86, x64: Standard Edition, Enterprise Edition (SP2 required for these editions)
- Windows 2008 Server Core
- Windows 2008 R2 Server Core
- Windows 2008 SP2 Server Core
- Windows Server 2008 x86, x64: Standard Edition, Enterprise Edition, Datacenter Edition, Web Edition, Small Business Sever (SP1 or SP2 required for all editions)

  Note: SFW HA 5.1 SP1 supports Windows Server 2008 without Hyper -V x86, x64: Standard Edition, Enterprise Edition, Datacenter Edition (SP1 or SP2 required for all editions).

- Windows Server 2008 for IA Systems (IA64) (SP1 or SP2)
- Windows Server 2008 R2 x64: Standard Edition, Enterprise Edition, Datacenter Edition, Web Edition

Note: SFW HA 5.1 SP1 supports Windows Server 2008 R2 without Hyper-V x64: Standard Edition, Enterprise Edition, Datacenter Edition.

- Windows Server 2008 R2 for IA Systems (IA64)
- Windows Storage Server 2008

SFW and SFW HA 5.1 SP1 software for clients

Your system must run one of the following operating systems to install the SFW or SFW HA 5.1 SP1 client software:

- Any one of the operating system versions, editions, and architectures that the Server Components are supported on except Server Core:
  See "SFW and SFW HA 5.1 SP1 software for servers" on page 20.
- Windows XP x86, x64 (SP3 required)
- Windows Vista x86, x64: Ultimate Edition, Business Edition, Premium Edition (SP1 or SP2 required)
- Windows 7 x86, x64: Ultimate Edition, Business Edition, Premium Edition

General requirements

Before you install the SFW or SFW HA 5.1 SP1 software, verify that your configuration meets the following criteria and that you have reviewed the SFW 5.1 Hardware Compatibility List to confirm supported hardware:

http://entsupport.symantec.com/docs/302144

Table 1-2 displays the hardware requirements for an SFW or SFW HA 5.1 SP1 software installation.

Table 1-2 Hardware requirements for SFW or SFW HA 5.1 SP1

Requirements	Specifications
Memory	1 GB of RAM required
32-bit processor requirements	800-megahertz (MHz) Pentium III-compatible or faster processor 1GHz or faster processor recommended

Table 1-2 Hardware requirements for SFW or SFW HA 5.1 SP1 *(continued)*

Requirements	Specifications
x64 processor requirements	1GHz AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support processor or faster
IA64 processor requirements	1GHz Itanium or faster processor 1GHz Dual-Core Intel Itanium 2 or faster processor
Display	Minimum resolution: 1024 X 768 pixels or higher VCS Cluster Manager (Java and Web Console) requires an 8-bit (256 colors) display and a graphics card that can render 2D images

Storage device compatibility

If you are not using Veritas Dynamic Multi-pathing or clustering (SFW HA or Microsoft clustering), SFW supports any device in the Microsoft Windows Server Catalog.

For Veritas Dynamic Multi-pathing and clustering configurations, refer to the Hardware Compatibility List to determine the approved hardware for SFW:

http://entsupport.symantec.com/docs/302144

Note: If your storage devices are SCSI-3 compliant, and you wish to use SCSI-3 Persistent Group Reservations (PGR), you must enable SCSI-3 support using the Veritas Enterprise Administrator (VEA).

For additional information about this procedure:

See the *Veritas Storage Foundation Administrator's Guide*.

Remote systems

You must have network access and appropriate administrative privileges to each remote computer. SFW HA 5.1 SP1 and SFW 5.1 SP1 with the VVR option do not support DHCP for access to the system. They only support static IP addresses.

Veritas Volume Replicator static IP address

VVR requires a static IP for replication. Make sure the system has at least one IP address configured that is not assigned by Dynamic Host Configuration Protocol (DHCP).

Single instance of SFW

Only one instance of Veritas Storage Foundation 5.1 for Windows (SFW 5.1 SP1) should be running on a system.

Driver signing options

When installing on systems running Windows Server 2003, you must either set the Windows driver signing option to ignore software authentication warning messages or select an installation option to install a Symantec Trusted certificate for unsigned drivers.

For Windows Server 2008, this is set by default. Windows Server 2008 does not allow you to change the driver signing option. The Symantec product installer provides an installation option to install a Symantec Trusted certificate to allow installation of Symantec drivers that are not certified by Microsoft:

See "Installing Symantec Trusted certificate for unsigned drivers" on page 50.

Veritas Cluster Server Management Console

Veritas Cluster Server Management Console is supported on the following browsers:

- Microsoft Internet Explorer 6.0 and 7.0
- Firefox 2.0 and 3.0.x

Veritas Cluster Server Management Console also requires Macromedia Flash Plug-in, Version 8.0 or greater.

Note: VCS Management Console does not support Firefox on Linux platforms.

Firewall and anti-spyware

Disable spyware monitoring and removal software before installing SFW or SFW HA 5.1 SP1. This is done only for your installation and should be re-enabled immediately after installation.

Ensure that your firewall settings allow access to ports used by SFW HA 5.1 SP1 wizards and services.

For a detailed list of services and ports used by SFW HA 5.1 SP1:

See "About SFW HA services and ports" on page 277.

SFW 5.1 SP1 requirements

This section describes the requirements for Veritas Storage Foundation for Windows (SFW 5.1 SP1).

Before you install SFW, verify that your configuration meets the following criteria and that you have reviewed the SFW 5.1 SP1 Hardware Compatibility List and Software Compatibility List to confirm supported hardware and software:

- For the Hardware Compatibility List:
  http://entsupport.symantec.com/docs/302144
- For the Software Compatibility List:
  http://entsupport.symantec.com/docs/302145

Permission requirements for SFW 5.1 SP1

You must be a member of the Local Administrators group or a domain administrator for all the nodes where you are installing SFW 5.1 SP1.

Additional SFW 5.1 SP1 installation requirements

The following are additional SFW 5.1 SP1 installation requirements:

- Installation media for all products and third-party applications
- Licenses for all products and third-party applications

Note: SFW supports SCSI, Fibre Channel, iSCSI host bus adapters (HBAs), or iSCSI Initiator supported NICs to access shared storage.

SFW HA 5.1 SP1 requirements

This section describes the requirements for Veritas Storage Foundation High Availability for Windows (SFW HA 5.1 SP1).

Before you install SFW HA 5.1 SP1, verify that your configuration meets the following criteria and that you have reviewed the Hardware Compatibility List and Software Compatibility List to confirm supported hardware and software:

- For the Hardware Compatibility List:
  http://entsupport.symantec.com/docs/302144
- For the Software Compatibility List:
  http://entsupport.symantec.com/docs/302145

System requirements for SFW HA 5.1 SP1

The following system requirements must be met:

- Minimum 1 GB of RAM per server for SFW HA 5.1 SP1.
- You must install the operating system in the same path on all systems.
  For example, if you install Windows Server 2003 on C:\WINDOWS of one node, installations on all other nodes must be on C:\WINDOWS. Make sure that the same drive letter is available on all nodes and that the system drive has adequate space for the installation.
- Shared disks to support applications that migrate between nodes in the cluster. Campus clusters require more than one array for mirroring. Disaster recovery configurations require one array for each site. Replicated data clusters with no shared storage are also supported.

  Note: If your storage devices are SCSI-3 compliant, and you wish to use SCSI-3 Persistent Group Reservations (PGR), you must enable SCSI-3 support using the Veritas Enterprise Administrator (VEA). For additional information about this procedure, see the *Veritas Storage Foundation Administrator's Guide*.

- SCSI, Fibre Channel, iSCSI host bus adapters (HBAs), or iSCSI Initiator supported NICs to access shared storage.
- A minimum of two NICs is required. One NIC will be used exclusively for private network communication between the nodes of the cluster. The second NIC will be used for both private cluster communications and for public access to the cluster.
  Symantec recommends three NICs. For additional information:
  See " SFW HA 5.1 SP1 best practices" on page 27.
- NIC teaming is not supported for the private network.
- All servers must have the same system architecture, run the same operating system, and be at the same service pack (SP) level.

Network requirements for SFW HA 5.1 SP1

The following network requirements must be met:

- Install SFW HA 5.1 SP1 on servers in a Windows Server 2003 or Windows Server 2008 domain.
- Do not install SFW HA 5.1 SP1 on servers that are assigned the role of a Domain Controller. Configuring a cluster on a domain controller is not supported.

- Configure a minimum of one static IP address for each physical node in the cluster.
- Configure one static IP address available per site for each application virtual server.
- One static IP address per cluster is used when configuring the Notification, Cluster Management Console (web console), or Global Cluster option. The same IP address may be used for all options.
- Configure name resolution for each node.
- Verify the availability of DNS Services.
  AD-integrated DNS or BIND 8.2 or higher are supported.
  Make sure that a reverse lookup zone exists in the DNS. Refer to the application documentation for instructions on creating a reverse lookup zone.
- Set the DNSRefreshInterval attribute for the Lanman agent, if you use DNS scavenging.
  DNS scavenging affects virtual servers configured in VCS because the Lanman agent uses Dynamic DNS (DDNS) to map virtual names with IP addresses. If you use scavenging, then you must set the DNSRefreshInterval attribute for the Lanman agent. This enables the Lanman agent to refresh the resource records on the DNS servers.
  See the *Veritas Cluster Server Bundled Agents Reference Guide*.
- Ensure that your firewall settings allow access to ports used by SFW HA 5.1 SP1 wizards and services. For a detailed list of services and ports used by SFW HA 5.1 SP1:
  See "About SFW HA services and ports" on page 277.
- For VVR replication in a disaster recovery configuration, a minimum of one static IP address per site for each application instance running in the cluster.
- For VVR replication in a Replicated Data Cluster configuration, a minimum of one static IP address per zone for each application instance running in the cluster.

Permission requirements for SFW HA 5.1 SP1

The following permission requirements must be met:

- You must be a domain user.
- You must be a member of the Local Administrators group for all nodes where you are installing.
- You must have write permissions for the Active Directory objects corresponding to all the nodes.

- If you plan to create a new user account for the VCS Helper service, you must have Domain Administrator privileges or belong to the Account Operators group. If you plan to use an existing user account context for the VCS Helper service, you must know the password for the user account.

Additional installation requirements for SFW HA 5.1 SP1

Review the following additional installation requirements for SFW HA 5.1 SP1:

- Installation media for all products and third-party applications.
- Licenses for all products and third-party applications.
- For installing VCS, all the systems must belong to the same domain. For a disaster recovery (DR) environment, if the systems at the primary and the secondary site reside in different domains, you must ensure that there is a trust relationship set up between those domains. Refer to your Microsoft documentation for information about setting up trust relationships between domains.

SFW HA 5.1 SP1 best practices

Symantec recommends that you perform the following tasks:

- Verify that you have three network adapters (two NICs exclusively for the private network and one for the public network).
  When using only two NICs, lower the priority of one NIC and use the low-priority NIC for public and private communication.
- Route each private NIC through a separate hub or switch to avoid single points of failure.
- Verify that you have set the Dynamic Update option for the DNS server to Secure Only.
- For a Replicated Data Cluster configuration, although you can use a single node cluster as the primary and secondary zones, you must create the disk groups as clustered disk groups. If you cannot create a clustered disk group due to the unavailability of disks on a shared bus, use the `vxclus UseSystemBus ON` command.

Setting up access rights

SFW uses the standard Microsoft Windows administrator privileges, which you must have to install these products. These privileges govern the access rights of users to the SFW servers and services.

The following services are associated with the product:

- Veritas Enterprise Administrator service (vxob) - the main SFW service
- Veritas Installer Service (vxinstaller) - used during installation

By default, administrators have the right to load and unload device drivers and to install and uninstall Storage Foundation for Windows. For accessing and using the program you must have administrator rights.

As an administrator, you need to grant these same administrator privileges to other users. For example, you can grant these rights in the Local Users and Groups function under Windows Server 2003 or Windows Server 2008 Administrative Tools. For more information, refer to your Microsoft Windows Server documentation.

Before proceeding, exit all programs and log on with administrator rights.

Licensing

Licensing for SFW and SFW HA is based on the Microsoft Windows Server 2003 or Windows Server 2008 operating systems in use on a specific server. A license is required for each system that runs any of the Symantec products.

Note: License keys for SFW and SFW HA release versions can only be used with their respective SFW and SFW HA software releases. For example, license keys for 4.x release versions of SFW and SFW HA can only be used with SFW and SFW HA 4.x software releases. License keys for 5.x release versions of SFW and SFW HA can only be used with SFW and SFW HA 5.x software releases.

Evaluation license key

An evaluation license key is embedded in the product. To use this key, click **Next** at the license key entry screen of the product installer. This license key is only valid for a limited evaluation period.

Virtual Server license policy

Each copy of the Storage Foundation for Windows High Availability including all options and agents, whether used on a physical server or within a virtual machine must be separately licensed. Each Licensed Software license specifies the number of instances of the Licensed Software you may run on a particular server at one time.

Table 1-3 lists Storage Foundation for Windows (SFW) editions and the additional licensing terms that apply.

Table 1-3 SFW licensing terms

Microsoft Operating System Edition	SFW licensing terms
■ Server Edition ■ Standard Edition ■ Web Edition	A separate license for the licensed software is required for each virtual or physical server, where the software is installed.
■ Advanced Edition ■ Enterprise Edition	For each license, you may run one instance of the licensed software on one physical server and up to four simultaneous instances of the licensed software on virtual servers located on the physical server.
Datacenter Edition	For each license, you may run one instance of the licensed software on one physical server and an unlimited number of virtual servers located on the physical server.

Client license

A license is not required, if you install the SFW or SFW HA client components.

License management

The product installer lets you add and remove specific licenses. Adding a license for an option does not install the option. Use the Add/Remove function to install an option. License keys support installation on multiple systems.

Note: License keys for releases earlier than 4.3 of SFW and SFW HA are not supported in release 5.1 of SFW and SFW HA. A default evaluation license key is supplied for your use. This license key is valid for a limited evaluation period only. You must purchase the product to obtain a permanent license key.

vxlicrep command

The `vxlicrep` command generates a report of the licenses in use on your system.

To use the vxlicrep command to display a license report

1. Access a command prompt.
2. Enter the `vxlicrep` command without any options to generate a default report.
3. Enter the `vxlicrep` command with any of the following options to produce the type of report required:

   -g default report

   -s short report

   -e enhanced/detailed report

   -i print report for valid keys only

   -k <key1, key2, ---- > print report for input keys key1, key2, ----

   -v print version

   -h display this help

vxlicrep license example

The following is an example of the display output from the `vxlicrep` command with the -e options for a detailed report.

```
C:\Documents and Settings\admin>vxlicrep help -e

Symantec License Manager vxlicrep utility version 3.02.34.0
Copyright (C) 1996-2008 Symantec Corporation. All rights reserved.

Creating a report on all VERITAS products installed on this system

 ------------------**********************------------------

   License Key                        = NGCE-C3UG-XXXX-G94L-3JM7-CPA9-NNP
   Product Name                       = Storage Foundation for Windows
   License Type                       = DEMO
   OEM ID                             = 4095
   Demo End Date                      = Tuesday, August 18, 2009
                                          1:00:00 AM
                                         (53.4 days from now).
   Editions Product                   = YES

 Features :=
   Platform                           = Windows
```

```
  License OS Platform                 = Windows Datacenter
  Version                             = 5.1
  Edition Type                        = Windows

  Storage Foundation                  = Storage Foundation Standard
  VxCache Option                      = Enabled
  DMP Option                          = Enabled
  FlashSnap Option                    = Enabled
  VVR Option                          = Enabled
  VCS Option                          = Enabled
  Mode#VERITAS Cluster Server         = VCS
  VCS App Agents#VERITAS Cluster Server = Enabled
  VCS HWREP Agents#VERITAS Cluster Server = Enabled
  Global Cluster Option#VERITAS Cluster Server = Enabled


----------------**********************----------------

  License Key                         = P4EE-72VI-XXXX-HM3G-O4OZ-DYUP-P
  Product Name                        = VERITAS Cluster Server
  License Type                        = DEMO
  OEM ID                              = 4095
  Demo End Date                       = Tuesday, August 18, 2009
                                        1:00:00 AM
                                        (53.4 days from now).
  Point Product                       = YES

Features :=
  Platform                            = Windows
  Version                             = Unused
  Tier                                = Unused
  Reserved                            = 0

  Mode                                = VCS
  Global Cluster Option               = Enabled
```

SFW and SFW HA license packages

License packages are available with SFW or SFW HA. Licenses for some options that are listed must be purchased separately.

Table 1-4 lists the agents and options available with SFW and SFW HA.

Table 1-4 SFW and SFW HA option and agent packages

Product license	Included options and agents	Separately available options and agents
SFW 5.1		Options: ■ FlashSnap Option ■ Dynamic Multi-pathing Option ■ Cluster Option for MSCS ■ Volume Replicator Option
SFW Enterprise (or Datacenter) 5.1	■ FlashSnap Option. ■ Dynamic Multi-pathing Option. ■ Cluster Option for MSCS.	■ Volume Replicator Option
SFW HA 5.1	■ Application Agent: Veritas Cluster Server Application Agent for Microsoft Exchange Database Agents: ■ Veritas Cluster Server Database Agent for Microsoft SQL ■ Veritas Cluster Server Database Agent for Oracle	■ FlashSnap Option ■ Dynamic Multi-pathing Option ■ Volume Replicator Option
SFW Enterprise (or Datacenter) HA 5.1	Options: ■ FlashSnap Option ■ Dynamic Multi-pathing Option Agents (See SFW HA 5.1 for the agent's full name): ■ Application Agent ■ Database Agents	■ Volume Replicator Option

Table 1-4 SFW and SFW HA option and agent packages *(continued)*

Product license	Included options and agents	Separately available options and agents
SFW HA/DR 5.1	Option: ■ Global Clustering Option Agents (See SFW HA 5.1 for the agent's full name): ■ Application Agent ■ Database Agents Hardware Replication Agents: ■ Veritas Cluster Server Hardware Replication Agent for EMC Symmetrix Remote Data Facility (SRDF). ■ Veritas Cluster Server Hardware Replication Agent for EMC SRDF Star. ■ Veritas Cluster Server Hardware Replication Agent for Hitachi TrueCopy. ■ Veritas Cluster Server Hardware Replication Agent for EMC Mirrorview. ■ Veritas Cluster Server Hardware Replication Agent for IBM Metro Mirror	■ FlashSnap Option ■ Dynamic Multi-pathing Option ■ Volume Replicator Option
SFW Enterprise (or Datacenter) HA/DR 5.1	Option: ■ Global Clustering Option ■ FlashSnap Option ■ Dynamic Multi-pathing Option Agents (See SFW HA 5.1 for the agent's full name): ■ Application Agent ■ Database Agents ■ Hardware Replication Agents (See SFW HA/DR 5.1 for the agent's list)	■ Volume Replicator Option

SFW Basic

This software release is also available as Storage Foundation Basic for Windows (SFW Basic). SFW Basic is a free technology specifically designed for edge-tier workloads.

SFW Basic has the same features of SFW and includes the Veritas Dynamic Multi-pathing (DMP) option. However, SFW Basic is limited to a maximum of four dynamic volumes and/or four file systems which must be located on the same physical server. The aggregate total of volumes and file systems for all virtual servers that are located on one physical server may not exceed four volumes and/or four file systems.

Note: SFW Basic has an embedded license key. You do not have to enter a license key to run SFW Basic.

SFW Basic Installation

The SFW Basic install and uninstall process is similar to the process for an SFW 5.1 install and uninstall:

- For information about installing SFW Basic:
  See "Installing using the Symantec product installer" on page 53.
- For information about uninstalling SFW Basic:
  See "Uninstalling using the product installer" on page 87.

Refer to the following section when installing SFW Basic and also upgrading to Microsoft Windows Server 2008 R2 or SP2:

See "Upgrading to Microsoft Windows Server 2008 R2 or SP2" on page 52.

SFW Basic Upgrade

SFW Basic can also be upgraded from SFW Basic to SFW 5.1 SP1 or SFW HA 5.1 SP1.

To upgrade from SFW Basic to SFW 5.1 SP1, enter a new SFW 5.1 SP1 license to get a fully functional SFW 5.1 SP1 application. For information about entering the new license:

See "License management" on page 85.

To upgrade from SFW Basic to SFW HA 5.1 SP1, follow the procedure for an upgrade from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 :

See "Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer" on page 166.

Refer to the following section when upgrading SFW Basic and also upgrading to Microsoft Windows Server 2008 R2 or SP2:

See "Upgrading Microsoft Windows Server 2008 after upgrading to SFW or SFW HA 5.1 SP1" on page 99.

Using the Configuration Checker

The Configuration Checker enables you to verify your configuration before you install SFW or SFW HA, or before you perform disaster recovery in a Microsoft Exchange or SQL Server environment.

The Configuration Checker operates in either GUI mode as a wizard, or by using the command line interface (CLI).

The Configuration Checker can be accessed in the following ways:

- Symantec Product Installer DVD (wizard)
- Solutions Configuration Center (wizard)
- Command line interface (CLI)

Run the Configuration Checker to perform the following tasks:

- Confirm your configuration before installing Veritas Storage Foundations and High Availability Solutions software (SFW or SFW HA) to ensure that the existing configuration(s) meet all pertinent software and hardware requirements.
- Confirm your configuration when you have a high availability (HA) environment, after the SFW HA software has been installed, but before you configure disaster recovery.

Once the Configuration Checker has completed the check, you can save a summary report as an HTML file to a directory of your choosing. To save a report, click the **Save** button on the summary page from the wizard.

The report contains the number of Passed or Failed checks out of the total number of checks done on the selected systems, and provides a consolidated report of every check performed on the systems.

Note: You can select multiple systems when running a preinstallation check, but can select only one system when configuring for disaster recovery.

For information about running the Configuration Checker as a wizard (GUI mode):

See "Using the Configuration Checker wizard" on page 38.

For information about running the Configuration Checker using the CLI:

See "Using the Configuration Checker CLI" on page 41.

VIAS and Configuration Checker

Symantec's Veritas Installation Assessment Service (VIAS) lets you verify whether the systems in your environment meet the requirements to install or upgrade the Veritas Storage Foundation and High Availability software. The Configuration Checker application and features have been incorporated into the VIAS framework.

The VIAS web site is located at:

https://vias.symantec.com/vias/vias

At the VIAS web site, you are presented with the following options:

- Generate a detailed report that shows you whether your system is ready to install or upgrade the specified product.
- Display a hardware and software checklist that you can use to ensure that your system is ready to install or upgrade the specified product.

The VIAS Data Collector is used to generate a report that shows whether your system is ready to install or upgrade to SFW or SFW HA 5.1 SP1. The VIAS Data Collector is downloaded from the VIAS web site. The VIAS Data Collector then gathers information about your system and environment and saves it to a file. You can subsequently upload this file to the VIAS web site for analysis and report creation.

The Configuration Checker, which is part of the Symantec product installer for SFW or SFW HA 5.1 SP1 also produces a VIAS formatted result file (vos_results.xml). After running the Configuration Checker and creating the vos_results.xml file, you save this file to the directory where you previously saved the HTML file summary report. You can upload this results file to the VIAS web site for analysis and report creation.

Alternatively, you can also use the VIAS hardware and software checklist to ensure that your system is ready to install or upgrade the specified product. You do not have to download the VIAS Data Collector. This option provides a quick alternative to the detailed report. To generate a checklist, you must select responses at the VIAS web site to questions about your system and environment. After submitting your responses, a checklist is generated for you to review.

Running the Configuration Checker before installation

When running the Configuration Checker before installing SFW HA, the following checks are performed:

- Presence of SFW or SFW HA
- Software and hardware compatibility
- Operating system versions, service packs, and hotfixes
- Virtualized environment check - whether the host for SFW or SFW HA is a virtual machine, and of what type.
- Notification of host file modified on system and user prompt to check host file entries.
- Available disk space
- Total physical memory
- Availability of the network ports that are used by Symantec products
- VCS NIC
- Driver signing check
- Active Directory
- Network configuration

Running the Configuration Checker after installation

When running the Configuration Checker after installing SFW or SFW HA, the following checks are performed:

- Generic check:
  Provides a system check for compatible software and hardware, total physical memory; available memory; OS version; if the host for SFW or SFW HA is a virtual machine, and of what type; notification of host file modified on system and user prompt to check host file entries; driver signing policy settings; presence of Active Directory; availability of DNS, Domain Controller, and Global Category; status of VM volumes; and port availability.
- SFW HA check:
  Checks for drive letter in use; available NIC cards; presence of Active Directory; consistency of Windows Services across clusters; consistency of system environment variables across clusters; consistency of license files; consistency between VCS service groups across clusters; and consistency between VCS resource types across clusters.

- Exchange Disaster Recovery check:
  When SFW HA is configured in a Microsoft Exchange environment, the Configuration Checker checks for compatible version of Exchange and service pack, and for consistency of Exchange Service group across clusters.
- SQL Server Disaster Recovery check:
  When SFW HA is configured in a Microsoft SQL Server environment, the Configuration Checker checks for compatible version of SQL Server and service pack, and for consistency of SQL Server Service group across clusters.

Using the Configuration Checker wizard

You access the Configuration Checker wizard (GUI) in the following ways:

- Symantec Product Installer DVD
- Solutions Configuration Center

The executable for the Configuration Checker is called ConfigChecker.exe, and is available on the DVD at the root\Installer directory.

Running the Configuration Checker wizard before installation

The following procedure describes how to run the Configuration Checker wizard before installation.

To run the Configuration Checker wizard before installation

1. Launch the Configuration Checker wizard in one of the following ways:
   - In the Product Selection screen of the Symantec Product Installer, click **Run Configuration Checker**.
   - Type the complete path to the ConfigChecker.exe in the command prompt and press Enter, or locate and double-click the ConfigChecker.exe.
2. Read the information on the Welcome screen and click **Next**.
3. In the Computer Selection screen, either type in the name or names (separated by commas) of the nodes that you want to check, or click **Browse**.

   When you click **Browse**, a list of available nodes appears in a pop-up window. Select one or more nodes and click **OK**.
4. Once you select a node, click **Add**. A description of the node appears on the right side of the screen.

   This description includes the computer name, operating system, and a list of Symantec installed products.
5. Click **Next** when you are done.

6 In the Option Selection screen, you are presented with the following preinstallation options:

- **SFW Pre-Install Check**
- **SFW HA Pre-Install Check**
- **VCS Pre-Install Check**

Select the appropriate preinstallationcheck option for your installation.

By default, all of the sub-options under each option are selected. Review the selected sub-options. Click the check box to unselect a sub-option.

When you are done selecting your options and sub-options, click **Next**.

7 The Validation screen appears, and the Configuration Checker proceeds with the check.

When status is complete, the Summary screen appears.

8 The Summary screen lists the completed checks.

An option with a blue check indicates that the check completed successfully. An option with a red X means that the check failed. Click on a failed option (if any) and review the description.

For example, if the option **Available Disk Space Check** failed, click the option to select it and the Description pane specifies the reason for the failure.

9 If the Configuration Checker identifies a supported virtualized environment (SFW or SFW HA being installed on a host that is a virtual machine) , then you are directed to the Symantec support site for technical notes on the best-practices for running SFW or SFW HA in a virtualized environment.

10 Click **Save** to save the summary as an HTML file, or click **Print** to print it.

11 Click **Finish** to close the wizard.

If some or all of the option checks failed, you can modify your configuration (increase memory or disk space, update drivers, etc.) and run the wizard again.

Running the Configuration Checker wizard after installation

The following procedure describes how to run the Configuration Checker wizard after installation.

To run the Configuration Checker wizard after installation

1 Launch the Configuration Checker wizard in one of the following ways:

- In the Product Selection screen of the Symantec Product Installer, click **Run Configuration Checker**.

- Launch the Solutions Configuration Center by clicking **Start > All Programs > Symantec > Veritas Cluster Server | Veritas Storage Foundation > Solutions Configuration Center**.
  Under **Tools**, select the **Configuration Checker** option on the right side of the screen view.
- Type the complete path to the ConfigChecker.exe in the command prompt and press Enter, or locate and double-click the ConfigChecker.exe.

2. Read the information on the Welcome screen and click **Next**.
3. In the Computer Selection screen, either type in the name or names (separated by commas) of the nodes that you want to check, or click **Browse**.

   When you click **Browse**, a list of available nodes appears in a pop-up window. Select one or more nodes and click **OK**.
4. Once you select a node, click **Add**. A description of the node appears on the right side of the screen.

   This description includes the computer name, operating system, and a list of Symantec installed products.
5. Click **Next** when you are done.
6. In the **Account Information** dialog box, type the Username and Password for the selected computer and click **OK**.

   If you select a node in a secure cluster, log on with your Windows domain account information. Make sure that you type "<domain name>\" before your username.
7. The Option Selection screen then appears.

   The post-installation options that are listed depend upon what solution or application is installed. Only those relevant to the users environment are listed.

   Possible options that may be listed include the following:

   - **SFW Post Install Checks**
   - **SFW HA Post Install Checks**
   - **SQL DR Checks**
   - **Exchange DR Checks**

   Select the option or options for the check that you want to run.

   Review the selected sub-options for your selected option or options. Click the check box to unselect a sub-option.

   When you are done selecting your option or options, click **Next**.

8 The Validation screen appears, and the Configuration Checker proceeds with the check.

When status is complete, the Summary screen appears.

9 The Summary screen lists the completed checks.

An option with a blue check means that the check completed successfully. An option with a red X means that the check failed. Click on a failed option (if any) and review the description.

For example, if the option **Total Physical Memory Check** failed, click the option to select it and the Description pane specifies the reason for the failure.

10 If the Configuration Checker identifies a supported virtualized environment (SFW or SFW HA being installed on a host that is a virtual machine) , then you are directed to the Symantec support site for technical notes on the best-practices for running SFW or SFW HA in a virtualized environment.

11 Click **Save** to save the summary as an HTML file, or click **Print** to print it.

12 Click **Finish** to close the wizard. If some or all of the option checks failed, you can modify your configuration (increase memory or disk space, update drivers, etc.) and run the wizard again.

Using the Configuration Checker CLI

To run the Configuration Checker using the CLI, type the following command to access and run the Configuration Checker from the DVD:

```
configchecker.exe /s id=id node= node name resultsdir=save_dir
vcsusername= vcs user name vcspassword= vcs password
```

Table 1-5 describes the Configuration Checker command parameters.

Table 1-5 Configuration Checker command parameters

Command parameter	Definition
/s	The /s indicates a setting for silent mode.
id	Identification parameter value. For information about possible identification parameter values: See Table 1-6
node	Node name The node name is optional. The default value is local host.

Table 1-5 Configuration Checker command parameters *(continued)*

Command parameter	Definition
resultsdir	This parameter is used to save the report to a specified directory via CLI.
vcsusername	VCS user name The username that is required to access the node.
vcspassword	VCS password The password that is used to access the node.

Table 1-6 describes the possible values for the ID or identification parameter in the Configuration Checker command. The identification parameter is used to set what is reviewed and checked by the Configuration Checker.

Table 1-6 Identification parameter value

Identification parameter value	Description
`sfw_pre`	The identification parameter value that is used to run an SFW preinstallation check
`sfwha_pre`	The identification parameter value that is used to run an SFW HA preinstallation check.
`vcs_pre`	The identification parameter value that is used to run a VCS preinstallation check.
`sfw_post`	The identification parameter value that is used to run an SFW post-installation check.
`sfwha_post`	The identification parameter value that is used to run an SFW HA post-installation check.
`vcs_post`	The identification parameter value that is used to run a VCS post-installation check.
`vcs_dr_post`	The identification parameter value that is used to run a VCS or SFW HA with DR post-installation check.
`sql_dr_post`	The identification parameter value that is used to run a SQL service group check and SQL version check in the DR environment.

Table 1-6 Identification parameter value *(continued)*

Identification parameter value	Description
`exch_dr_post`	The identification parameter value that is used to run an Exchange service group check and Exchange version check in the DR environment .

Planning tasks

Planning tasks are required for the following installations:

- SFW HA 5.1 SP1 installation:
  See "Planning an SFW HA installation" on page 43.
- SFW 5.1 SP1 installation with Microsoft cluster:
  See "Planning an SFW installation with a Microsoft cluster" on page 46.
- VVR installation:
  See "Planning a VVR installation" on page 47.

Planning an SFW HA installation

During an SFW HA 5.1 SP1 installation, the product installer automatically installs Veritas Storage Foundation for Windows and Veritas Cluster Server. You may select other applicable options during the installation. You may also choose to install simultaneously on more than one system during the installation process.

After the installation is complete, run the VCS Configuration Wizard to complete the VCS cluster configuration. The VCS Configuration Wizard presents the opportunity to configure optional VCS features including security options, Cluster Management Console, notification, and the global cluster wide-area connection resource.

Depending on your environment you may choose configure the SPAS root broker and CMC management server for multiple clusters outside the cluster.

Review the following sections and decide how you want to configure your environment:

- About Symantec Product Authentication Service
- SFW HA upgrade and Veritas NetBackup
- About Veritas Cluster Server Management Console
- About notification

About Symantec Product Authentication Service

Symantec Product Authentication Service allows the security administrator to configure authentication to provide a single sign-on service for Symantec applications. In this case, users need log-on only once to a single Symantec application, and other applications can then use the credentials acquired through the first logon.

Symantec Product Authentication Service provides the ability to configure a cluster in secure mode. Symantec Product Authentication Service secures communication between cluster nodes and clients, including the Java console, by using digital certificates for authentication and SSL to encrypt communication over the public network.

To configure the cluster in secure mode, SFW HA requires you to specify and configure a system in your environment as a root broker and all nodes in the cluster as authentication brokers.

Table 1-7 defines the root broker and authentication broker.

Table 1-7 Root and authentication broker definitions

Broker type	Description
Root broker	A root broker serves as the main registration and certification authority. It is the single authority which validates requests from authentication brokers that are installed on the (cluster) systems.
Authentication broker	Authentication brokers serve as intermediate registration and certification authorities. Authentication brokers have certificates that are signed by the root. Each node in the cluster serves as an authentication broker.

For best practices and options for configuring the root broker in your environment, refer to the *Veritas Storage Foundation™ and High Availability Solutions Quick Start Guide for Symantec Product Authentication Service.*

SFW HA upgrade and Veritas NetBackup

If you are running Veritas NetBackup™ version 6.0 or 6.5 on systems where you are upgrading to SFW HA 5.1 SP1, then you must shut down the OpsCenterServer service before an upgrade.

Both NetBackup and SFW HA 5.1 SP1 share the same AT broker and client, and for this reason the OpsCenterServer service must by shut down before an upgrade.

About Veritas Cluster Server Management Console

Veritas Cluster Server Management Console is a high availability management solution that enables monitoring and administering clusters from a single web console.

You can configure Cluster Management Console to manage a single cluster, multiple clusters, or both:

- If you want to use the Cluster Management Console to manage multiple clusters, you must set up a standalone management server.
- If you want to use the Cluster Management Console to manage a single cluster, choose the option to configure the Cluster Management Console, also known as the Web console from the VCS Configuration Wizard. Configuring the Cluster Management Console may be done during initial cluster configuration or at a later time.

For additional information about the Veritas Cluster Server Management Console, refer to the *Veritas™ Cluster Server Management Console Implementation Guide*.

Contact customer service at the following URL to request the latest version of the guide:

www.symantec.com/customercare

About notification

You can configure SFW HA to send event notification either through SMTP email notification or SNMP traps.

Configuring the notifier process may be done during initial cluster configuration or at a later time using the VCS Configuration Wizard.

For additional information about the VCS Configuration Wizard, refer to the *Veritas Cluster Server Administrator's Guide*.

About global clusters

A global cluster consists of two or more clusters linked together. Global clusters provide the ability to fail over applications between geographically distributed clusters when disaster occurs.

Global clusters may be configured either through the Disaster Recovery Configuration Wizard available from the Solutions Configuration Center or through the Global Group Configuration Wizard. Both processes require a wide-area

connector resource for inter-cluster communication. This resource is configured automatically as part of the Disaster Recovery Configuration Wizard or may optionally be configured using the VCS Configuration Wizard.

The Disaster Recovery Configuration Wizard is described in the following Solutions Guides.

- *Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange*
- *Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007*
- *Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2000 and 2005*
- *Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008*
- *Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Enterprise Vault*
- *Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Office SharePoint® Server*

For information about the Global Group Configuration Wizard and VCS Configuration Wizard, refer to *Veritas Cluster Server Administrator's Guide*.

Planning an SFW installation with a Microsoft cluster

If you plan to set up a Microsoft cluster (MSCS or Microsoft failover cluster) with SFW, review the following recommendations:

- Microsoft clustering should already be configured. This enables SFW to install Microsoft cluster resources such as Volume Manager disk groups and various other shared resources.
- Symantec does not recommend a push installation on systems in a Microsoft cluster, because the Microsoft cluster must be active and running when installing SFW.
- Because SFW installation requires a reboot, and the reboot causes the active node of the cluster to fail over, use a rolling installation.
  Install SFW on the inactive node or nodes of the cluster first, then use the **Move Group** command in Microsoft clustering to move the active node. Install SFW on the cluster's remaining node.
  For additional information about planning an SFW installation with a Microsoft cluster, refer to the *Veritas Storage Foundation Administrator's Guide*.

Planning a VVR installation

For a planned VVR installation, replication between servers running Windows Server 2003 and Windows Server 2008 is supported in the following environments:

- Storage Foundation for Windows with the Volume Replicator (VVR) option on standalone servers (no clustering) selected.
- Storage Foundation for Windows HA with the Volume Replicator (VVR) and Global Cluster (GCO) options selected.
- Storage Foundation for Windows with the Volume Replicator (VVR) and Microsoft Clustering options selected.

Chapter 2

Installing SFW or SFW HA

This chapter includes the following topics:

About installing SFW or SFW HA

This chapter describes the process for a new installation of Veritas Storage Foundation 5.1 SP1 for Windows (SFW) or Veritas Storage Foundation High Availability 5.1 SP1 for Windows (SFW HA).

For information about upgrading from previous versions of SFW or SFW HA:

See "About preparing for upgrade" on page 95.

You can install SFW or SFW HA using either the product installer or the command line interface (CLI).

Preinstallation procedures

Review the following preinstallation procedures.

- Installing Symantec Trusted certificate for unsigned drivers:
  See "Installing Symantec Trusted certificate for unsigned drivers" on page 50.
- Enabling the Computer Browser service on Windows Server 2008 systems:

See "Enabling the Computer Browser service for Windows Server 2008" on page 52.

- Activating Microsoft Windows on your Windows 2008 server:
  See "Activating Microsoft Windows on your server" on page 52.
- Upgrading to Microsoft Windows 2008:
  See "Upgrading to Microsoft Windows Server 2008 R2 or SP2" on page 52.

Perform the appropriate preinstallation procedures for your installation.

Installing Symantec Trusted certificate for unsigned drivers

The Symantec product installer provides an installation option for Symantec Trusted Software Publisher Certificate for Veritas Storage Foundation for Windows drivers that are not certified by Microsoft.

If you select this installation option, a Symantec Trusted certificate is installed on the systems you select for installation.

Warning: On Windows Server 2008, if this option is not selected, a remote install will not install any SFW drivers that are not certified by Microsoft. No notification is given and it will appear that installation was successful, but issues can arise later because the drivers were not installed. If installing locally on Windows Server 2008, if this option is not selected, a driver signing popup will be displayed requiring user interaction.

If you select this option when installing on Windows Server 2003, you do not need to set the driver signing options to Warn or Ignore as described in the following section:

See "Setting Windows driver signing options" on page 50.

Setting Windows driver signing options

Some drivers provided by Symantec may not be signed by Microsoft. Depending upon your installation options, these unsigned drivers may stop your installation.

When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

Table 2-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers on Windows Server 2003.

Table 2-1 Installation behavior with unsigned drivers

Driver Signing Setting	Installation behavior on the local system	Installation behavior on remote systems
Ignore	Always allowed	Always allowed
Warn	Warning message, user interaction required	Installation proceeds. The user must log on locally to the remote system to respond to the dialog box to complete the installation.
Block	Never allowed	Never allowed

On local systems set the driver signing option to either Ignore or Warn. On remote systems set the option to Ignore to allow the installation to proceed without user interaction.

Windows Server 2008 does not let you change the driver signing option. The Symantec product installer provides an installation option to install a Symantec Trusted certificate to allow installation of Symantec drivers that are not certified by Microsoft:

See "Installing Symantec Trusted certificate for unsigned drivers" on page 50.

If you select this installation option when installing on Windows Server 2003, you do not need to set the driver signing options to Warn or Ignore as described in the following procedure.

To change the driver signing options on each system

1. Log on locally to the system.
2. Open the Control Panel and click **System**.
3. Click the **Hardware** tab and click **Driver Signing**.
4. In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.
5. Click **OK**.
6. Repeat for each computer.

   If you do not change the driver signing option, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing option to its previous state.

Enabling the Computer Browser service for Windows Server 2008

The Microsoft Computer Browser service helps maintain an updated list of domains, workgroups, and server computers on the network and supplies this list to client computers upon request. This service must be enabled for the Symantec product installer to discover and display all domain members during an SFW HA 5.1 SP1 installation.

By default, systems running Windows Server 2008 (x86/x64/IA64) disable the Computer Browser service. With this service disabled, remote domain members on the computer lists do not display during an SFW HA 5.1 SP1 installation.

Enable the Computer Browser Service on your Windows Server 2008 (x86/x64/IA64) systems before installing SFW HA 5.1 SP1.

Refer to your Microsoft documentation for information about enabling the Computer Browser service.

Activating Microsoft Windows on your server

Symantec recommends that you activate Microsoft Windows, before proceeding with an SFW or SFW HA 5.1 SP1 installation on a Windows Server 2008 server.

If you do not activate Microsoft Windows before an install, an "Optional update delivery is not working message" may appear. You can ignore this message, click **Close**, and continue with the installation.

Upgrading to Microsoft Windows Server 2008 R2 or SP2

This section describes additional procedures required when performing the followings tasks:

- Installing SFW 5.1 SP1 and then upgrading your Windows Server 2008 operating system to Windows Server 2008 R2 or SP2
- Installing SFW HA 5.1 SP1 and then upgrading your Windows Server 2008 operating system to Windows Server 2008 R2 or SP2

Installing SFW 5.1 SP1 and upgrading to Windows Server 2008 R2 or SP2

When planning to upgrade your Microsoft Server 2008 operating system to Windows Server 2008 R2 or SP2, Symantec recommends performing the Windows upgrade before installing SFW 5.1 SP1. If you follow this recommendation, then no additional steps are required for the SFW 5.1 SP1 installation.

In some circumstances though, you may need to install SFW 5.1 SP1 before upgrading Windows. If you install SFW 5.1 SP1 before upgrading your Windows

Server 2008 operating system, then you must run an SFW repair installation after your Windows Server 2008 R2 or SP2 upgrade with the **Veritas Storage Foundation 5.1 SP1 for Windows (Server Components)** GUI option selected. For information about running a repair installation:

See "Repairing the installation" on page 84.

Note: This procedure also applies to an SFW Basic installation.

Installing SFW HA 5.1 SP1 and upgrading to Windows Server 2008 R2 or SP2

When planning to upgrade your Microsoft Server 2008 operating system to Windows Server 2008 R2 or SP2, Symantec recommends performing the Windows upgrade before installing SFW HA 5.1 SP1. If you follow this recommendation, then no additional steps are required for the SFW HA 5.1 SP1 installation.

In some circumstances though, you may need to install SFW HA 5.1 SP1 before upgrading Windows. If you install SFW HA 5.1 SP1 before upgrading your Windows Server 2008 operating system, then you must perform the following procedure.

SFW utility and repair procedure

1 Run the SFW utility called FixVDSKey.bat after the Windows Server 2008 R2 or SP2 upgrade.

This SFW utility is located at: %VMPATH%\FixVDSKey.bat

Note: Running this utility restarts the Storage Agent (VxVM) and VDS services.

2 Run an SFW repair installation with the **Veritas Storage Foundation 5.1 SP1 for Windows (server components)** option selected. For information about running a repair installation:

See "Repairing the installation" on page 84.

After installing SFW HA 5.1 SP1 and then upgrading to Windows Server 2008 R2 or SP2, you must access and run this utility and run a repair installation.

Installing using the Symantec product installer

The Symantec product installer enables you to install the software for Veritas Storage Foundation 5.1 SP1 for Windows (SFW) or Veritas Storage Foundation High Availability 5.1 SP1 for Windows (SFW HA).

An SFW HA installation includes Veritas Storage Foundation for Windows and Veritas Cluster Server. You may select other applicable options during the installation. The steps in this section are based on a high availability or cluster server (SFW HA) installation. While the steps for an SFW installation are similar, they are not exactly the same.

Note: When installing to SFW or SFW HA 5.1 SP1, ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.

Installing Storage Foundation HA for Windows

Follow the procedure described below to install Veritas Storage Foundation HA for Windows.

To install the product

1. Insert the DVD containing the installation software into your system's disc drive or download the installation software from the Symantec website.
2. Allow the autorun feature to start the installation or double-click **Setup.exe**.

   The Select Product screen appears.

3 Review the links on the Select Product screen.

Links on this screen access Late Breaking News, the Configuration Checker, as well as begin the process to install Storage Foundation 5.1 SP1 for Windows or Storage Foundation HA 5.1 SP1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide, Installation and Upgrade Guide, and Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Storage Foundation HA 5.1 for Windows**.

5 After clicking **Storage Foundation HA 5.1 SP1 for Windows**, the Select install type screen displays.

Do one of the following:

- Click **Complete/Custom** to begin installation.
- Click the **Administrative Console** link to install only the client components.

Note: With the **Administrative Console** option, you will not be prompted for a product license or be presented with a list of product options for SFW or SFW HA.

Click **Complete/Custom** and proceed.

6 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

7 Read the License Agreement by using the scroll arrows in the view window. If you agree to the license terms, click the radio button for **I AGREE TO the terms of the license agreement**, and then click **Next**.

8 Enter the product license key before adding license keys for features.

Enter the license key in the top field and click **Add**.

If you do not have a license key, click **Next** to use the default evaluation license key. The default evaluation license key is valid for a limited evaluation period only.

9 Repeat for additional license keys, using the following options and click **Next**.

To remove a license key	Click the key to select it and click **Remove**.
To view the license key's detail	Click the key

10 Select the appropriate SFW or SFW HA product options and click **Next**.

Note: Options differ depending on your product and environment.

The following are the available product options for SFW:

Volume Replicator (VVR)	Volume Replicator (VVR) replicates data across multiple sites for disaster recovery
FlashSnap	FlashSnap allows you to create and maintain split-mirror, persistent snapshots of volumes
VxCache	VxCache uses a portion of system memory to improve I/O performance

DMP Device Specific Modules (DSMs)	■ 3PARDATA (V3PARAA) ■ Dell EqualLogic array (VEQLOGIC) ■ EMC Symmetrix/DMX (VEMCSYMM) ■ EMC Clarion (VEMCCLAR) ■ Hitachi TagmaStore/HP XP (VHDSAA) ■ Hitachi 95xx-AMS-WM (VHDSAP) ■ HP 2000 array (VHPMSA2) ■ HP EVA-MSA (VHPEVA) ■ IBM DS8000/ESS (VIBMAADS) ■ IBM DS6000 (VIBMAP) ■ IBM DS4000/SUN 6000 (VENGAP) ■ IBM DS AP (VIBMAPDS) ■ IBM XiV Storage System (VXIV) ■ HUAWEI S5300/S2300 array (VHUAWEIAP) ■ FUJITSU ETERNUS 2000 array (VFUJITSUAA) ■ NETAPP (VNETAPP) ■ PILLAR (VPILLAR) ■ Windows Storage Server 2003 R2 iSCSI (VITARGET) ■ XioTech Array (VXIOTECH) For detailed information about DMP DSMs: See "Installing and uninstalling Veritas Dynamic Multi-pathing" on page 70. Symantec maintains a Hardware Compatibility List (HCL) for Veritas Storage Foundation and High Availability Solutions 5.1 SP1 for Windows. The HCL provides information on HBAs and firmware that have been tested with each supported array. Check the HCL for details about your hardware before installing or using DMP DSMs. The HCL is located at: http://entsupport.symantec.com/docs/302144
Cluster Option for Microsoft Cluster Service (MSCS)/Failover cluster	■ Cluster Option for Microsoft Cluster Service (MSCS) ■ Support for Microsoft Cluster Service (MSCS). You can select this option even if Microsoft clustering is not currently installed
Product Documentation	Veritas Storage Foundation for Windows Documentation.

Symantec Trusted Software Publisher Certificate	■ Symantec Trusted Software Publisher Certificate for Veritas Storage Foundation for Windows drivers that are not certified by Microsoft. Not selecting this option may cause these drivers not to install correctly for remote install on Windows Server 2008
Replace Disk Management Snap-in with SFW VEA GUI for Windows Server 2008	Replace the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator GUI for Windows Server 2008.
Veritas Storage Foundation 5.1 SP1 for Windows (Client Components)	■ Veritas Storage Foundation 5.1 SP1 for Windows (Client Components)

The following are the available options for SFW HA:

Volume Replicator (VVR)	Volume Replicator (VVR) replicates data across multiple sites for disaster recovery
FlashSnap	FlashSnap allows you to create and maintain split-mirror, persistent snapshots of volumes
VxCache	VxCache uses a portion of system memory to improve I/O performance

DMP Device Specific Modules (DSMs)	■ 3PARDATA (V3PARAA) ■ Dell EqualLogic array (VEQLOGIC) ■ EMC Symmetrix/DMX (VEMCSYMM) ■ EMC Clarion (VEMCCLAR) ■ Hitachi TagmaStore/HP XP (VHDSAA) ■ Hitachi 95xx-AMS-WM (VHDSAP) ■ HP 2000 array (VHPMSA2) ■ HP EVA-MSA (VHPEVA) ■ IBM DS8000/ESS (VIBMAADS) ■ IBM DS6000 (VIBMAP) ■ IBM DS4000/SUN 6000 (VENGAP) ■ IBM DS AP (VIBMAPDS) ■ IBM XiV Storage System (VXIV) ■ HUAWEI S5300/S2300 array (VHUAWEIAP) ■ FUJITSU ETERNUS 2000 array (VFUJITSUAA) ■ NETAPP (VNETAPP) ■ PILLAR (VPILLAR) ■ Windows Storage Server 2003 R2 iSCSI (VITARGET) ■ XioTech Array (VXIOTECH) For detailed information about DMP DSMs: See "Installing and uninstalling Veritas Dynamic Multi-pathing" on page 70. Symantec maintains a Hardware Compatibility List (HCL) for Veritas Storage Foundation and High Availability Solutions 5.1 for Windows. The HCL provides information on HBAs and firmware that have been tested with each supported array. Check the HCL for details about your hardware before installing or using DMP DSMs. The HCL is located at: http://entsupport.symantec.com/docs/302144
Global Cluster Option (GCO)	Global Cluster Option (GCO) enables you to link clusters to provide wide-area failover and disaster recovery.
High Availability Database Agents	■ Veritas Cluster Server Database Agent for SQL : The database agent for SQL enables VCS to control Microsoft SQL. ■ Veritas Cluster Server Database Agent for Oracle: The database agent for Oracle enables VCS to control Oracle.

High Availability Application Agents	■ Veritas Cluster Server Application Agent for Exchange: The enterprise agent for Exchange enables VCS to control Microsoft Exchange.
High Availability Hardware Replication Agents	■ Veritas Cluster Server Hardware Replication Agent for EMC MirrorView: The hardware replication agent for EMC MirrorView enables VCS to manage MirrorView replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for EMC SRDF: The hardware replication agent for EMC SRDF enables VCS to manage SRDF replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for EMC SRDFSTAR: The hardware replication agent for EMC SRDF enables VCS to manage SRDFSTAR replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for Hitachi TrueCopy: The hardware replication agent for Hitachi TrueCopy enables VCS to manage TrueCopy replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for MetroMirror : The hardware replication agent for MetroMirror enables VCS to manage MetroMirror replicated devices.
Enterprise Vault	■ Enterprise Vault (EV) Cluster Setup Wizard
Product Documentation	Veritas Storage Foundation HA for Windows Documentation.
Symantec Trusted Software Publisher Certificate	■ Symantec Trusted Software Publisher Certificate for Veritas Storage Foundation for Windows drivers that are not certified by Microsoft. Not selecting this option may cause these drivers not to install correctly for remote install on Windows Server 2008.
Replace Disk Management Snap-in with SFW VEA GUI for Windows Server 2008	Replace the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator GUI for Windows Server 2008.

Veritas Storage Foundation HA 5.1 SP1 for Windows (Client Components)	■ Veritas Storage Foundation HA 5.1 SP1 for Windows (Client Components)

11 Select the following for the installation and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When installing the software on multiple computers in a single installation using the product installer, all computers must have the same platform type (for example, x86 or x64). However, the computers can have different Windows operating systems. For example, you can install the software on multiple computers at once running Windows 2003 and Windows 2008.

Install Path	Optionally, change the installation path.
	■ To change the path, select a computer in the Selected computers for installation field, type the new path, and click **Change**.
	■ To restore the default path, select a computer and click **Default**.
	The default path is:
	`C:\Program Files\Veritas`
	For 64-bit installations, the default path is:
	`C:\Program Files (x86)\Veritas`

12 When the domain controller and the computer running the installation program are on different subnets, the installer may be unable to locate the target computers. In this situation, after the installer displays an error message, enter the host names or the IP addresses of the missing computers manually.

13 The installer checks the prerequisites for the selected computers and displays the results.

Review the information and click **Next**.

If a computer fails validation, address the issue, and repeat the validation. Click the computer in the list to display information about the failure. Click **Validate Again** to begin the validation process again.

14 Depending upon your earlier product installer selections and operating system, you may receive one or more of the following messages.

If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning:	The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system. If applicable to your installation, perform the above procedure.
If you are using multiple paths and selected a specific DSM on a Windows Server 2008 machine, you receive an additional message:	On Windows Server 2008, the Microsoft Multipath input/output (Microsoft MPIO) feature must be enabled before installing DMP Device Specific Modules (DSMs). If applicable to your installation, perform the above second procedure.
When installing Veritas Storage Foundation 5.1 for Windows (Server Components) with the MSCS option selected, you receive the following message:	When installing Veritas Storage Foundation 5.1 for Windows (Server Components) with the MSCS option, you may want MSCS Quorum Arbitration Time (Min and Max) to be adjusted to ensure optimal functionality with Veritas dynamic volumes with MSCS. For additional information, see the *Storage Foundation for Windows Administrator Guide* for details. If applicable to your installation, perform the above procedure.

When finished reviewing the message or messages click **OK**.

15 The Summary screen appears displaying an Install report.

Review the information in the Install report.

Click **Back** to make changes, if necessary.

Click **Install** if information is validated.

16 The Installation Status screen displays status messages and the progress of the installation.

If an installation fails, click **Next** to review the report and address the reason for failure. You may have to either repair the installation or uninstall and reinstall.

For information about repairing an installation:

See "Repairing the installation" on page 84.

17 When the installation completes, review the summary screen and click **Next**.

18 If you are installing on remote nodes, click **Reboot**. Note that you cannot reboot the local node now, and that failed nodes are unchecked by default. Click the check box next to the remote nodes that you want to reboot.

19 When the nodes have finished rebooting successfully, the Reboot Status shows Online and the **Next** button is available. Click **Next**.

20 Review the log files and click **Finish**.

21 Click **Yes** to reboot the local node.

Resetting the driver signing option procedure

If you set the Windows driver signing options before installation, then after completing the installation reset the driver signing option on each computer running Windows 2003.

To reset the driver signing options

1 Open the Control Panel, and click **System**.

2 Click the **Hardware** tab and click **Driver Signing**.

3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat for each computer.

Installing using the command line interface

You can perform a silent installation using the command line interface for the SFW and SFW HA software at the command prompt with the `Setup.exe` command. With a silent installation, you can only install on one computer at a time.

Note: For Windows Server 2008, all CLI commands must run in the command window in the "run as administrator" mode.

The following command examples are displayed at the end of this section:

- Local installation of SFW client:
  See "Silent installation example: SFW client" on page 69.
- Local installation of SFW server:
  See "Silent installation example: SFW server" on page 70.
- Remote installation of SFW server:
  See "Silent installation example: remote installation of an SFW server" on page 70.

Warning: Symantec provides an installation option to install a Symantec Trusted certificate to allow installation of Symantec drivers that are not certified by Microsoft. On Windows Server 2008, if this option is not specified, a remote install will not install any SFW drivers that are not certified by Microsoft. No notification is given and it will appear that installation was successful, but issues can arise later because the drivers were not installed.

Note: When installing SFW or SFW HA 5.1 SP1, ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.

To install from the command line

1. Log into a console session.

   Start any Remote Desktop sessions with the "console" switch by typing the following from a Windows command prompt:

   ```
   mstsc /console
   ```

2. Open a command window by clicking **Start > Run**.
3. Enter `cmd` in the Open field and click **OK**.

4 In the command window, navigate to the root directory of the Symantec DVD.

If you downloaded the installation software from the Symantec web site, then navigate to where you downloaded the installation software to and the directory where the setup.exe is located.

5 Use the following command syntax to install SFW:

```
Setup.exe /s INSTALL_MODE=InstallMode SOLUTIONS="1,2,3,..."
[LICENSEKEY="LicenseKey"] [OPTIONS="a,b,c,..."]
[DISKMGMT="0,1"] [INSTALLDIR="InstallDirPath"]
[NODE="SysA"] [REBOOT=RebootMode]
```

Where the maximum length of the argument string is 2,048 characters and the syntax is not case sensitive.

Parameters for setup.exe

Table 2-2 contains information about the possible parameter values.

Table 2-2 Parameters for setup.exe

Parameter	Use
/s	Set for silent mode. If not set, boots the product installer GUI.
INSTALL_MODE	Set to indicate an installation or uninstallation. *1* = To install *4*= To repair *5* = To uninstall Example: INSTALL_MODE=1 **Note:** The parameter, INSTALL_MODE=1 is used for both a new installation, as well as an upgrade. The installer switches to the correct mode (installation or upgrade) depending upon what has already been installed on the selected system.
SOLUTIONS	Set to the type of installation. *1* = SFW Server *2* = SFW HA Server *3* = SFW Client *4* = SFW HA Client Example: SOLUTIONS=*1*

Table 2-2 Parameters for setup.exe *(continued)*

Parameter	Use
LICENSEKEY	Set the license key for the installation. Enter multiple keys by separating them with a comma—do not put spaces around the comma. The license key must start and end with a quotation mark ("). The license key can be entered with or without hyphens. *LicenseKey* has no default setting. Example: LICENSEKEY="*1234-2345-1234-2345-3456-1234,3421-5432-2765-6789-4321-1234*"
OPTIONS	Set the desired options for the installation type. The list of options must start and end with a quotation mark ("). Example: OPTIONS="*MSCS,VVR*" **Warning:** On Windows Server 2008, if the SYMCCERT option is not selected, a remote install on Windows 2008 will not install any SFW drivers that are not certified by Microsoft. No notification is given and it will appear that installation was successful, but issues can arise later because the drivers were not installed.
DISKMGMT	Replace the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator GUI for Windows Server 2008. By default, this option is enabled and the DISKMGMT value is set to 1. To disable this option, then set DISKMGMT=0.
INSTALLDIR	Use only to set a non-default path for the installation directory. The path must start and end with a quotation mark ("). Example: INSTALLDIR="*C:\InstallationDirectory*" The default setting, used when you do not specify a path, is SystemDrive:\Program Files\Veritas If the path has blank spaces in it, the path should be set off with backslashes as in the following example: Example: INSTALLDIR=\"C:\Program Files (x86)\"

Table 2-2 Parameters for setup.exe *(continued)*

Parameter	Use
NODE	Set the node name. Specify only one node at at time. The local node is the default setting when the node is unspecified. The machine name of the node must start and end with a quotation mark ("). Example: `Node="SysA"`
REBOOT	Setting for the automatic reboot of the system at the completion of the installation. *0* = No reboot *1* = Reboot The default setting is 0 for no system reboot. Example: `REBOOT=1` **Note:** Reboot the system at the end of installation to ensure the correct installation of the SFW drivers for the server component. You do not have to reboot after installing the client components.

Options differ depending on your product and environment.

Table 2-3 shows the available options.

Table 2-3 Available options

Option	Description	SFW	SFW HA	VCS
vvr	Volume Replicator (VVR) replicates data across multiple sites for disaster recovery	✓	✓	NA
flashsnap	FlashSnap lets you create and maintain split-mirror, persistent snapshots of volumes	✓	✓	NA
vxcache	VxCache uses a portion of system memory to improve I/O performance	✓	✓	NA
mscs	Cluster option for MSCS/Failover Cluster	✓	NA	NA
EV	Enterprise Vault Cluster Setup Wizard	NA	✓	✓

Table 2-3 Available options *(continued)*

Option	Description	SFW	SFW HA	VCS
symccert	Installs Symantec Trusted Software Publisher Certificate for Veritas Storage Foundation for Windows drivers that are not certified by Microsoft. **Note:** On Windows Server 2008, if this option is not specified, a remote install on Windows 2008 will not install any SFW drivers that are not certified by Microsoft. No notification is given and it will appear that installation was successful, but issues can arise later. If installing locally on Windows Server 2008 and this option is not specified, then a driver signing popup is displayed requiring user interaction. If you specify this option when installing on Windows Server 2003, you do not need to set the driver signing options to Warn or Ignore.	✓	✓	NA
sfwdoc	Documentation for SFW solutions	✓	NA	NA
sfwhadoc	Documentation for SFW HA solutions	NA	✓	NA
veqlogic	Dell EqualLogic	✓	✓	N/A
vemcsymm	EMC Symmetrix/DMX DSM	✓	✓	NA
vemcclar	EMC Clariion DSM	✓	✓	NA
vhdsaa	Hitachi TagmaStore/HP XP DSM	✓	✓	NA
vhdsap	Hitachi 95xx-AMS-WM DSM	✓	✓	NA
vhpeva	HP EVA-MSA DSM	✓	✓	NA
vhpmsa2	HP 2000	✓	✓	NA
vibmaads	IBM DS8000/ESS DSM	✓	✓	NA
vibmap	IBM DS6000 DSM	✓	✓	NA
vengap	IBM DS4000/Sun 6000 DSM	✓	✓	NA
vxiv	IBM XiV Storage System	✓	✓	NA

Table 2-3 Available options *(continued)*

Option	Description	SFW	SFW HA	VCS
vhuaweiap	HUAWEI S5300/S2300	✓	✓	NA
vfujitsuaa	FUJITSU ETERNUS 2000	✓	✓	NA
vitarget	Windows Storage Server 2003 R2 iSCSI DSM	✓	✓	NA
vxiotech	XioTech	✓	✓	NA
v3paraa	3PARDATA DSM	✓	✓	NA
vpillar	VPILLAR DMS	✓	✓	NA
vibmapds	IBM DS AP DSM	✓	✓	NA
vnetapp	NETAPP DSM	✓	✓	NA
gco	Global Cluster Option (GCO) enables you to link clusters to provide wide-area failover and disaster recovery.	NA	✓	✓
sql	Database agent for Microsoft SQL Server	NA	✓	✓
exchange	Enterprise agent for Microsoft Exchange	NA	✓	✓
oracle	Database agent for Oracle	NA	✓	✓
srdf	Hardware replication agent for EMC SRDF	NA	✓	NA
truecopy	Hardware replication agent for Hitachi TrueCopy	NA	✓	NA
mirrorview	Hardware replication agent for EMC MirrorView	NA	✓	NA
metromirror	Hardware replication agent for MetroMirror	NA	✓	NA
srdfstar	Hardware replication agent for EMC SRDF/Star	NA	✓	NA

Silent installation example: SFW client

This sample command installs the SFW Client and states that the installation path is `C:\InstallationDirectory`. This sample command also tells the system not to reboot at the end of the installation.

```
Setup.exe /s INSTALL_MODE=1 SOLUTIONS=3
INSTALLDIR="C:\InstallationDirectory" REBOOT=0
```

Silent installation example: SFW server

This sample command installs the SFW Server with a license key of 123-234-123-234-345, with the MSCS and VVR options, and with their license keys. This sample command also states that the installation path is `C:\InstallationDirectory` and tells the system to reboot at the end of the installation.

```
Setup.exe /s INSTALL_MODE=1 SOLUTIONS=1
LICENSEKEY="123-234-123-234-345,321-543-765-789-321,321-543-765-789-789"
OPTIONS="MSCS,VVR" DISKMGMT="1"
INSTALLDIR="C:\InstallationDirectory" REBOOT=1
```

Silent installation example: remote installation of an SFW server

This sample command installs the SFW Server with a license key of 123-234-123-234-345, with the MSCS and VVR options, and with their license keys. This sample command also states that the installation path on that computer is `C:\InstallationDirectory`, that the node it is installing to is SysA, and tells the system to reboot at the end of the installation.

```
Setup.exe /s INSTALL_MODE=1 SOLUTIONS=1
LICENSEKEY="23-234-123-234-345,321-543-765-789-321,321-543-765-789-789"
OPTIONS="MSCS,VVR,SYMCCERT"  DISKMGMT="1"
INSTALLDIR="C:\InstallationDirectory" NODE="SysA" REBOOT=1
```

Installing and uninstalling Veritas Dynamic Multi-pathing

Veritas Dynamic Multi-pathing option adds fault tolerance by supporting multiple paths between a server and a storage array. Veritas Dynamic Multi-pathing (DMP) is implemented through Dynamic Multi-pathing Device Specific Modules (DMP DSMs).

DMP DSMs support the following:

- Windows Server 2003 and 2008
  DMP DSMs are Dynamic Multi-pathing drivers that work with the Microsoft Windows Multipath Input/Output framework.

- Windows Storport driver (storport.sys)
- Microsoft iSCSI Initiator
- Dynamic Least Queue Depth load balancing
- Active/Active Dynamic Multi-pathing with clustering

For additional detailed instructions about DMP DSMs, refer to the *Veritas Storage Foundation Administrator's Guide.*

Table 2-4 lists the DMP DSM installation procedures that are discussed in this section.

Table 2-4 DMP DSM installation procedures

Procedure	Description
Adding DMP DSMs (general procedure)	For information about adding DMP DSMs: See "Adding DMP DSMs" on page 72.
DMP DSMs installation on new standalone server	For information about installing DMP DSMs on a new standalone server: See "Installing DMP DSMs on a new standalone server" on page 73.
SFW HA and DMP DSMs installation on a cluster for the first time	For information about installing SFW HA and DMP DSMs on a cluster for the first time: See "Installing SFW HA and DMP DSMs on a cluster for the first time " on page 74.
SFW, Microsoft clustering, and DMP DSMs installation on a cluster for the first time	For information about installing SFW, Microsoft clustering, and DMP DSMs on a cluster for the first time: See "Installing SFW, Microsoft clustering, and DMP DSMs on a cluster for the first time " on page 75.
Adding DMP DSMs to an existing standalone server	For information about adding DMP DSMs to an existing standalone server: See "Adding DMP DSMs to an existing standalone server" on page 76.
Adding DMP DSMs to an existing SFW HA or MSCS cluster	For information about adding DMP DSMs to an existing SFW HA or MSCS cluster: See "Adding DMP DSMs to an existing SFW HA or MSCS cluster" on page 77.

Prerequisites for DMP DSM installation

Review the following prerequisites for installing DMP DSMs:

- Make sure that your host has an HBA (host bus adapter) port for each path to the SAN switch.
- Check that your host has one SCSI or fiber cable per host bus adapter port.
- For iSCSI, assign each host bus adapter port a unique SCSI ID.
- Connect no more than one path to shorten installation time.
- Ensure that the Windows Storport driver is installed.

Symantec maintains a Hardware Compatibility List (HCL) for Veritas Storage Foundation and High Availability Solutions 5.1 for Windows. The HCL provides information on HBAs and firmware that have been tested with each supported array. Check the HCL for details about your hardware before installing or using DMP DSMs.

The HCL is located at:

http://entsupport.symantec.com/docs/302144

Warning: Do not change the cable connection order after installing SFW. For example, if host bus adapter A is connected to port A on the array and host bus adapter B is connected to port B on the array, do not swap the connections between ports on the array (A to B and B to A) after installing SFW.

Adding DMP DSMs

In general, the steps for adding DMP DSMs to any configuration are described in the following procedure.

To add DMP DSMs

1. Install the new host adapter hardware.
2. To shorten installation time, make sure that no more than a single path is connected to the storage array before installation.
3. Install the software by selecting DMP DSMs as part of the SFW or SFW HA installation process.

   For information about installing SFW or SFW HA:

   See "Installing using the Symantec product installer" on page 53.

Warning: You must install the correct hardware drivers for the DMP DSMs. Refer to your hardware documentation for detailed information about hardware drivers.

Note: For Windows Server 2008 systems, enable the Microsoft Multipath I/O (MPIO) feature using the Server Manager to view the multi-path under SFW or SFW HA. The MPIO server feature must be enabled before installing DMP Device Specific Modules (DSMs) in Windows Server 2008 systems.

Installing DMP DSMs on a new standalone server

The following procedure describes how to install DMP DSMs on a new standalone server.

To install DMP DSMs on a new standalone server

1. Install the necessary hardware and the appropriate drivers.
2. Connect no more than one path from the array to the computer.
3. During the SFW or SFW HA installation using the wizard, on the Option Selection screen select **DMP Device Specific Modules (DSMs)**. Alternatively, you can expand this option to select only the appropriate DSMs for your environment.

   For information:

   See "Installing using the Symantec product installer" on page 53.

   You can also install SFW or SFW HA using the CLI. For information about using the CLI to install SFW or SFW HA and selecting the appropriate DSMs for your environment:

   See "Installing using the command line interface" on page 64.

4 Complete the installation, rebooting where instructed.

5 Physically reconnect the additional path.

Installing SFW HA and DMP DSMs on a cluster for the first time

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).

For more information on DMP DSMs load balance settings and enabling or disabling SCSI-3 PGR, refer to the *Veritas Storage Foundation Administrator's Guide*.

Warning: Failure to adhere to the following instructions results in disk signature discrepancies causing SFW HA or other applications to fail.

The following procedure describes how to install SFW HA and DMP DSMs on a cluster for the first time.

To install SFW HA and DMP DSMs on a cluster for the first time

1 Before running the installation, connect to no more than one path from the array to the computer.

2 Install SFW HA and DMP DSMs at the same time on all nodes in the cluster.

During the SFW HA installation using the wizard, on the Option Selection screen select **DMP Device Specific Modules (DSMs)**. Alternatively, you can expand this option to select only the appropriate DSMs for your environment

For information:

See "Installing using the Symantec product installer" on page 53.

You can also install SFW HA using the CLI. For information about using the CLI to install SFW HA and selecting the appropriate DSMs for your environment:

See "Installing using the command line interface" on page 64.

3 Complete the installation, reboot after installation.

4 Physically reconnect the additional path.

5 After rebooting, run the various VCS wizards to complete the VCS cluster configuration.

For more information on creating and configuring the VCS cluster, refer to the *Veritas Cluster Server Administrator's Guide*.

Installing SFW, Microsoft clustering, and DMP DSMs on a cluster for the first time

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).

For more information on DMP DSMs load balance settings and enabling or disabling SCSI-3 PGR refer to the *Veritas Storage Foundation Administrator's Guide*.

To support Microsoft clustering and DMP Device Specific Modules (DSMs) simultaneously on a cluster, perform the following procedures.

Warning: Failure to adhere to the following instructions results in disk signature discrepancies causing MSCS, Windows Failover Cluster, or other applications to fail.

The following procedure describes how to install SFW, Microsoft clustering, and DMP DSMs on a cluster for the first time.

To install Microsoft clustering and DMP DSMs for the first time on a cluster

1 Create the Microsoft cluster.

2 Before running the installation, connect to no more than one path from the array to the computer.

3 Install SFW and DMP DSMs at the same time.

During the SFW installation using the wizard, on the Option Selection screen select **DMP Device Specific Modules (DSMs)**. Alternatively, you can expand the option to select only the appropriate DSMs for your environment.

For information:

See "Installing using the Symantec product installer" on page 53.

You can also install SFW HA using the CLI. For information about using the CLI to install SFW HA and selecting the appropriate DSMs for your environment:

See "Installing using the command line interface" on page 64.

4 Complete the installation, reboot after installation.

5 Physically reconnect the additional path.

6 Set up and configure the Microsoft (MSCS or Windows Failover Cluster) cluster.

For more information about setting up and configuring the Microsoft cluster, refer to your Microsoft documentation.

Adding DMP DSMs to an existing standalone server

The following procedure describes how to add DMP DSMs to an existing standalone server.

To add DMP DSMs to an existing standalone server

1 Install the additional hardware and its appropriate drivers.

2 Connect to no more than one path from the array to the computer.

3 Open the Windows Control Panel and select **Add or Remove Programs**.

4 Select **Change or Remove Programs**.

5 Select the SFW Server Components entry and click **Change**.

6 The Symantec Product installer screen appears. Select **Add or Remove**. Click **Next**.

7 Add a license key for the new DMP DSMs.

To add a license key, click the **License Management** link.

8 In the next window that appears, enter the license key for the option and click **OK**.

9 Return to the Option Selection screen. Select **DMP Device Specific Modules (DSMs)**. Alternatively, you can expand the option to select only the appropriate DSMs for your environment.

10 Select the check box to add the option and click **Next**.

11 Reboot the system.

12 Reconnect the additional physical path.

13 Verify that the additional path exists.

Open the Veritas Enterprise Administrator console. Click the **Veritas Enterprise Administrator console** in the Symantec Solutions Configuration Center or click **Start | All Programs | Symantec | Veritas Storage Foundation | Veritas Enterprise Administrator**.

14 In the System field, expand the Disks tree.

15 Click any external hard disk.

16 Above the console, click the DMP tab.

17 Verify that the path exists.

Adding DMP DSMs to an existing SFW HA or MSCS cluster

The following procedure describes how to add DMP DSMs to an existing SFW HA or MSCS cluster.

Note: Symantec recommends that you perform a rolling upgrade and install SFW or SFW HA and DMP DSMs on each node separately.

To add DMP DSMs to an existing SFW HA or MSCS cluster

1 Move resources to another node or take the resources offline.

2 Install the additional hardware and its appropriate drivers.

3 Connect no more than one path from the array to the computer.

4 Open the Windows Control Panel and select **Add or Remove Programs**.

5 Select **Change or Remove Programs**.

6 Select the SFW HA Server Components entry and click **Change**.

7 The Symantec Product installer screen appears. Select **Add or Remove**. Click **Next**.

8 Add a license key for the new DMP DSMs.

To add a license key, click the **License Management** link.

9 In the next window that appears, enter the license key for the option and click **OK**.

10 Return to the Option Selection screen. Select **DMP Device Specific Modules (DSMs)**. Alternatively, you can expand the option to select only the appropriate DSMs for your environment.

11 Select the check box to add the option.

12 Click **Next.**

13 Reconnect the additional physical path.

14 Reboot the system.

15 Verify that the additional path exists.

Open the Veritas Enterprise Administrator console. Click the **Veritas Enterprise Administrator console** in the Symantec Solutions Configuration Center or **click Start | All Programs | Symantec | Veritas Storage Foundation | Veritas Enterprise Administrator**.

16 In the System field, expand the Disks tree and click any external hard disk.

17 Above the console, click the DMP tab.

18 Verify that the path exists.

Uninstalling DMP DSMs

To uninstall DMP DSMs, use **Add or Remove** through the installer.

See "Adding or removing features" on page 82.

Chapter 3

Configuring SFW or SFW HA

This chapter includes the following topics:

Possible configuration tasks

Depending upon your SFW or SFW HA 5.1 SP1 installation and initial configuration, the following additional configuration tasks may be required:

- Changing the default password after installing VCS client:
  See "Changing the default password after installing VCS client" on page 80.
- Registering Veritas Volume Manager Disk Group resource type:
  See "Registering Veritas Volume Manager Disk Group resource type" on page 80.
- Configuring an SFW HA cluster:
  See "Configuring an SFW HA cluster" on page 81.
- Configuring an iSCSI SAN with SFW:
  See "Configuring an iSCSI SAN with SFW" on page 82.

Changing the default password after installing VCS client

When you install and configure the VCS client components (Java GUI), if you do not choose the secure mode during cluster configuration, the Veritas Cluster Server Configuration Wizard (VCW) creates a user with default credentials of user name "admin" and password "password".

Make sure that when you configure the cluster using VCW, you create a unique user name and password during the configuration process instead of accepting the default values.

Registering Veritas Volume Manager Disk Group resource type

The Cluster Option for Microsoft Cluster Service (MSCS)/Failover Cluster option can be selected when installing Storage Foundation 5.1 for Windows, whether or not the machine where the install is taking place is a member of a Microsoft cluster.

If the machine later becomes the first node in a Microsoft cluster, the Veritas Volume Manager Disk Group resource type must be manually registered with the Microsoft cluster. This installation kit contains a script for use in this case.

To register the Veritas Volume Manager Disk Group resource type

1. Open a command window by clicking **Start > Run** and then typing **cmd**.
2. Type **cd %vmpath%\VM5INF**.
3. Once there, type **clusReg.cmd**.

   This step registers the Volume Manager Disk Group resource type for use on the cluster.
4. Verify successful registration with the command `cluster restype`.

   The command output should include the Volume Manager Disk Group. You must open a new command window to run the command, because executing the script closes the command window it runs in.

Cluster regtype command example

The following is example output of the `cluster regtype` command, listing all available resource types:

Display Name	Resource Type Name
IP Address	IP Address
Network Name	Network Name
Physical Disk	Physical Disk

DHCP Service	DHCP Service
Distributed Transaction Coordinator	Distributed Transaction Coordinator
File Share	File Share
Generic Application	Generic Application
Generic Script	Generic Script
Generic Service	Generic Service
Local Quorum	Local Quorum
Majority Node Set	Majority Node Set
Message Queuing	MSMQ
Print Spooler	Print Spooler
Volume Shadow Copy Service Task	Volume Shadow Copy Service Task
WINS Service	WINS Service
Volume Manager Disk Group	Volume Manager Disk Group

It is unnecessary to run the script on a machine where Storage Foundation for Windows 5.1 is installed with Cluster Option for Microsoft Cluster Service (MSCS)/Failover Cluster selected, and the machine is then joined to an existing MSCS cluster with the "Veritas Volume Manager Disk Group" resource type already registered.

Configuring an SFW HA cluster

After installing SFW HA 5.1 SP1, run the VCS Configuration Wizard to complete the VCS cluster configuration.

For more information:

See "Planning an SFW HA installation" on page 43.

Information on cluster configuration and optional VCS features can be found in the following guides:

- *Veritas Cluster Server Administrator's Guide*
- *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange*
- *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL*

- *Veritas Storage Foundation and High Availability Solutions, Solutions Guide*

Configuring an iSCSI SAN with SFW

After installing SFW 5.1 SP1, refer to the *Veritas Storage Foundation™ Administrator's Guide* for information about setting up and configuring an iSCSI SAN.

Updating SFW or SFW HA

After an SFW or SFW HA 5.1 SP1 installation, you many need to update your components. The product installer lets you update the installed client and server components.

To update SFW and SFW HA

1. Open the Windows Control Panel and click **Add or Remove Programs**.
2. Select **Change or Remove Programs**.
3. Select the option for the Veritas Storage Foundation (Server Components). For example, for SFW HA select **Veritas Storage Foundation HA 5.1 SP1 for Windows (Server Components**) and click **Change**.
4. The Symantec Product Installer screen appears. Select **LiveUpdate**. Click **Next**.
5. The LiveUpdate screen appears. Choose to check if updates are available automatically by selecting **On (automatically check for updates)** or choose to check if updates are available manually by selecting **Off (manually check for updates)**.
6. Choose a LiveUpdate mode. If **On (automatically check for updates)** is selected, you have a choice to select **Express** to have updates automatically downloaded and installed, or select **Interactive** to view a list of available updates and choose which to download and install on your computer.
7. Select **Check for latest update after "Finish" is clicked**. Click **Finish**.

Adding or removing features

After an SFW or SFW HA 5.1 SP1 installation, you may need to add or remove features to your SFW or SFW HA application. The product installer lets you add or remove features.

Note: You can only add or remove features on the local system.

To add or remove features

1. Open the Windows Control Panel and click **Add or Remove Programs**.
2. Select **Change or Remove Programs**.
3. Select the option for the Veritas Storage Foundation (Server Components).

   For example, for SFW HA select **Veritas Storage Foundation HA 5.1 SP1 for Windows (Server Components)** and click **Change**.
4. The Symantec Product Installer screen appears. Select **Add or Remove**.

   Click **Next**.
5. The Option Selection screen appears. Select or clear the option check boxes in the tree navigation structure to add or remove a component respectively.

   Proceed to the following procedure.

To add a license key for an option

1. In the Option Selection screen, right-click on the option and select **Add License**.
2. In the pop-up window that appears, enter the license key for the option and click **OK**.

   Select the check box to add the option.
3. Click **Next**.

   Proceed to the following procedure.

Validation and Summary

1. On the Validation screen, the installer checks the prerequisites for the selected options and displays the results. Review the information and click **Next**.

   If a system fails validation, click the system in the systems list to display information about the failure. Address the problem and click **Validate Again** to repeat the validation process.
2. On the Summary screen, review the information and click **Update** to begin the product update.
3. On the Update Status screen, status messages are displayed and the progress updated.
4. When complete, review the summary and click **Next**.
5. On the Thank You screen, click **Finish**.
6. In the message box, click **Yes** to reboot your system.

Repairing the installation

The product installer can repair an existing installation of the SFW and SFW HA 5.1 SP1 client and server components.

The **Repair** option restores the installation to its original state. This option fixes missing or corrupt files, shortcuts, and registry entries on the local computer.

When repairing an SFW HA installation, you must first stop the VERITAS High Availability Engine. To stop the VERITAS High Availability Engine, type the following on the command prompt:

```
C:\>hastop -local
```

Note: Before running the above command, you should also take steps to save your configuration to another system for safe keeping, and failover the service groups for your applications to another node.

Note: You can only repair the installation on the local system.

To repair the installation

1. Open the Windows Control Panel and click **Add or Remove Programs**.
2. Select **Change or Remove Programs**.
3. Select the option for the Veritas Storage Foundation (Server Components).

   For example, for SFW HA select **Veritas Storage Foundation HA SP1 5.1 for Windows (Server Components)** and click **Change**.
4. The Symantec Product Installer screen appears. Select **Repair**. Click **Next**.
5. On the Validation screen, the installer checks the prerequisites for the systems and displays the results. Review the information and click **Next**.

   If a system fails validation, click the system in the systems list to display information about the failure. Address the problem and click **Validate Again** to repeat the validation process.
6. On the Summary screen, review the information and click **Repair** to begin the repair process.
7. On the Repair Status screen, review the status messages and the progress of the repair.

   If a repair fails, click **Next** to review the report and address the reason for failure. You may have to uninstall and reinstall the software.

8 When complete, review the repair summary and click **Next**.

9 On the Thank You screen, click **Finish**.

10 In the message box, click **Yes** to reboot your system.

Recovery tools

Symantec provides clean-up and recovery tools and scripts in case of failed SFW or SFW HA 5.1 SP1 installs, uninstalls, or upgrades. These clean-up and recovery tools and scripts can be downloaded from the following Symantec link:

http://entsupport.symantec.com/docs/336367

The above Symantec link also provides tech notes and FAQs about SFW or SFW HA 5.1 installs, uninstalls, upgrades, and troubleshooting issues.

License management

The product installer lets you add or remove license keys for SFW and SFW HA 5.1 SP1 client and server components.

To manage your license

1 Open the Windows Control Panel and click **Add or Remove Programs**.

2 Select **Change or Remove Programs**.

3 Select the option for the Veritas Storage Foundation (Server Components).

For example, for SFW HA select **Veritas Storage Foundation HA 5.1 SP1 for Windows (Server Components)** and click **Change**.

4 The Symantec Product Installer screen appears.

Select **License Management**.

Click **Next**.

5 The license key screen appears. Enter the license key you want to add and click **Update**.

If you want to remove a license key, select the license key in the Licenses field and click **Remove**.

6 Click **Finish**.

Chapter 4

Uninstalling SFW or SFW HA

This chapter includes the following topics:

Uninstalling using the product installer

You can use the Symantec product installer to uninstall SFW or SFW HA 5.1 SP1. In order to uninstall the software from remote computers, the local computer where you uninstall must have SFW or SFW HA installed on it.

The installation or upgrade path used to install or upgrade to SFW or SFW HA 5.1 SP1 determines the Veritas programs displayed in the **Add or Remove Programs** window.

If you installed both the Veritas server and client components for SFW or SFW HA 5.1 SP1, then you are presented with options in the **Add or Remove Programs** window to uninstall both. By clicking **Veritas Storage Foundation 5.1 SP1 for Windows (Server Components)** or **Veritas Storage Foundation HA 5.1 SP1 for Windows (Server Components)** respectively and proceeding with uninstalling the server components, you can also uninstall the client components.

If you performed a Major Upgrade from SFW 4.3 MP2 or 5.0.x to SFW 5.1 SP1, then you are presented with options in the **Add or Remove Programs** window to uninstall both the server and client components. By clicking **Veritas Storage Foundation 5.1 SP1 for Windows (Server Components)** and proceeding with uninstalling the server components, you can also uninstall the client components.

If you performed a Minor Upgrade from SFW 5.1.x to SFW 5.1 SP1, then you are presented with options to uninstall the server and client components, as well as

an additional option to uninstall Service Pack 1. Select the option **Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows** to only remove Service Pack 1. This option rolls back your system to its earlier state (SFW 5.1 or 5.1 AP1).

If you want to uninstall SFW completely after performing a minor upgrade from SFW 5.1.x to 5.1 SP1, it is not necessary to uninstall SP1 and then uninstall SFW 5.1. You need to select the option, **Veritas Storage Foundation 5.1 SP1 for Windows (Server Components)**. This option removes both SP1 and 5.1 (client and server components).

If you performed a Major Upgrade from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1, then you are presented with options in the **Add or Remove Programs** window to uninstall both the server and client components. By clicking **Veritas Storage Foundation HA SP1 for Windows (Server Components)** and proceeding with uninstalling the server components, you also can uninstall the client components.

If you performed a Minor Upgrade from SFW HA 5.1.x to SFW HA 5.1 SP1, then you are presented with several options in the **Add or Remove Programs** window:

- Select the option **Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows** to only remove Service Pack 1. This option rolls back your system to its earlier state (SFW HA 5.1 or 5.1 AP1).
- Select the option **Veritas Storage Foundation HA 5.1 for Windows (Server Components)** to completely uninstall SFW HA after upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1. By clicking **Veritas Storage Foundation HA 5.1 for Windows (Server Components)** and proceeding with uninstalling the server components, you can also uninstall the client components.

Note: You can use the Symantec product installer to uninstall SFW or SFW HA 5.1 SP1 from multiple systems.

The following procedure describes the steps required to uninstall SFW server and client components from a Windows 2003 system. The steps required to uninstall client components and a high availability server are similar.

For uninstalling SFW HA, you must first unconfigure the cluster. Use the Veritas Cluster Wizard (VCW) to unconfigure the cluster. See the *Veritas Cluster Server Administrator's Guide* for more information.

Note: Uninstalling SFW, SFW HA, or SFW DMP DDI-x also uninstalls DMP DSM from the system, and there is no rolling back of DMP DSM to a previous version of DMP DSM. If the DMP DSM feature needs to be enabled after rolling back to a previous SFW or SFW HA version, the DMP DSM feature needs to be reinstalled through SFW, SFW HA, or SFW DMP DDI-x.

Note: The changes made to types.cf file after upgrading from SFW HA 5.1 to SFW HA 5.1 SP1 are lost if you choose to uninstall SFW HA 5.1 SP1 and roll back to SFW HA 5.1. Take a back up of the types.cf file before you uninstall SFW HA 5.1 SP1 and re-import the same after the roll back is complete.

To uninstall using the product installer

1. In the Windows Control Panel, select **Add or Remove Programs**.
2. Click **Veritas Storage Foundation SP1 for Windows (Server Components)**.
3. Click **Remove**.
4. Review the information on the Welcome screen and then click **Next**.
5. On the Options Selection screen, select the checkboxes to uninstall both the client components and the server components.

   Click **Next**.
6. On the Computer Selection screen, select the systems that you want to uninstall from the Domain and Computer drop-down menus and click **Add**. Optionally, type the computer's name in the Computer field. Repeat to uninstall from other systems.

   To remove a system from the **Selected computers for uninstallation** list, click the system and click **Remove**.
7. Click **Next**.
8. On the Validation screen, the installer checks the prerequisites for the selected systems and displays the results. Review the information and click **Next**.

   If a system fails validation, click the system in the systems list to display information about the failure. Address the problem and click **Validate Again** to repeat the validation process.

   Click **Next**.
9. The Summary screen appears and displays the settings and systems selected for uninstallation.

   Click **Uninstall**.
10. The Uninstall Status screen displays status messages and the progress of the installation.

    If an uninstallation fails, the status screen shows a failed uninstallation. Click **Next** to review the report, address the reason for failure, and retry this step on that computer.
11. When complete, review the Uninstall summary and click **Next**.

12 Reboot the remote nodes.

Note: You must not reboot the local node now.

13 Select the check box next to the remote nodes that you want to reboot and click **Reboot**.

14 When the remote nodes have finished rebooting successfully, the Reboot Status shows Online and the **Next** button is available. Click **Next**.

15 Once the remote nodes have rebooted, click **Next**.

16 On the Thank You screen, click the link to review the log file, review the log file, and then click **Finish**.

17 Click **Yes** to reboot the local system.

Uninstalling from the command line

You can silently uninstall the SFW software from the command prompt using the `setup.exe` command.

The `setup.exe` command syntax is as follows:

```
Setup.exe /s INSTALL_MODE=InstallMode
SOLUTIONS="1,2,3,..."   [REBOOT=RebootMode] [NODE="SysA"]
```

Table 4-1 displays information about the possible parameter values for uninstalling the SFW software:

Table 4-1 Parameters for uninstalling the software

Parameter	Use
`/s`	Set for silent mode.
`INSTALL_MODE`	Set to indicate an install or uninstall. *1* = To install *4*= To repair *5* = To uninstall The default setting is 1 to install. Set this parameter to 5 for uninstall. Example: `INSTALL_MODE=5`

Table 4-1 Parameters for uninstalling the software *(continued)*

Parameter	Use
SOLUTIONS	Set to the type of uninstallation. *1* = SFW Server *2* = SFW HA Server *3* = SFW Client *4* = SFW HA Client The default setting is *1* for SFW Server. Example: SOLUTIONS=*1*
REBOOT	Setting for the automatic reboot of the system at the completion of the installation. *0* = No reboot *1* = Reboot The default setting is *0* for no system reboot. Example: REBOOT=*1*
NODE	Set the node name. You can enter only one node at a time. The local node is the default setting when the node is unspecified. The machine name of the node must start and end with a quotation mark ("). Example: Node="*SysA*" **Note:** Reboot the system at the end of uninstallation to ensure that the SFW drivers for the server component are installed correctly. You do not have to reboot after uninstalling the client.

The following procedure describes how to uninstall the software from the command prompt.

Note: The changes made to types.cf file after upgrading from SFW HA 5.1 to SFW HA 5.1 SP1 are lost if you choose to uninstall SFW HA 5.1 SP1 and roll back to SFW HA 5.1. Take a back up of the types.cf file before you uninstall SFW HA 5.1 SP1 and re-import the same after the roll back is complete.

To uninstall from the command prompt

1. Log into a console session.

   Start any Remote Desktop sessions with the "console" switch. This can be done by typing the following from a Windows command prompt:

   ```
   mstsc /console
   ```

2. Open a command window by clicking **Start > Run**.
3. Enter `cmd` in the Open field and click **OK**.
4. In the command window, navigate to the root directory of the product DVD.
5. Use the following command syntax to silently uninstall SFW:

   Setup.exe /s INSTALL_MODE=*InstallMode*
   SOLUTIONS="*1,2,3,...***"**
   [REBOOT=*RebootMode***] [NODE="***SysA***"]**

Uninstall command examples

The following uninstall command example completely uninstalls the SFW client components, and reboots the system at the end of the uninstall process:

```
Setup.exe /s INSTALL_MODE=5 SOLUTIONS=3 REBOOT=1
```

The following uninstall command example completely uninstalls the SFW server components, and reboots the system at the end of the uninstall process:

```
Setup.exe /s INSTALL_MODE=5 SOLUTIONS=1 REBOOT=1
```

Section 2

Upgrade

Chapter 5

Preparing for Upgrade

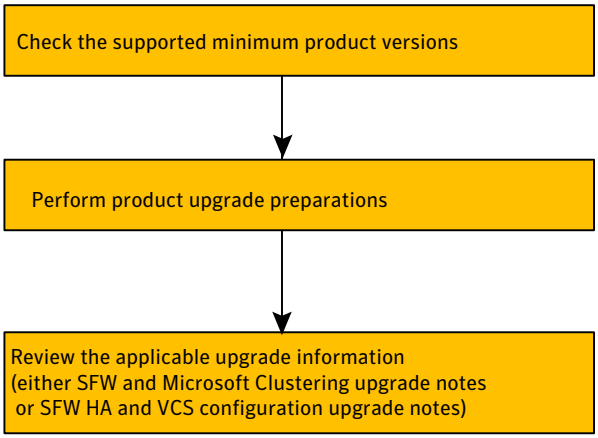
This chapter includes the following topics:

About preparing for upgrade

This chapter covers the general upgrade preparations that must be taken before upgrading to Veritas Storage Foundation 5.1 SP1 for Windows (SFW 5.1 SP1) or Veritas Storage Foundation High Availability 5.1 SP1 for Windows (SFW HA 5.1 SP1).

Figure 5-1 displays the general preparations for an upgrade.

Figure 5-1 General preparations for upgrade



Checking the supported minimum product versions

Before upgrading, you need to make sure that your systems meet the minimum product versions. You must also do some general preparation for the upgrade.

Warning: Rules created using the SFW 4.x Rule Manager will not automatically be upgraded and will not work in SFW 5.x. For additional information, see: http://entsupport.symantec.com/docs/303042

To upgrade to SFW or SFW HA 5.1 SP1, your system must have version 4.3 MP2 or higher of SFW or SFW HA already installed. The previously installed version of SFW or SFW HA must meet this minimum product version, which the product installer checks before it upgrades.

If your current installation does not meet the minimum level required by the installer, you must manually apply the appropriate product upgrades to meet the minimum product level required before proceeding with the installer. You can get intermediate versions of the products on the Symantec Support site:

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

For license keys, contact Symantec Sales. You can also uninstall the older versions of the product and install the new product.

Product upgrade preparations

When upgrading the product, perform the following tasks:

- Back up all your data in a safe location.
- Back up the system state.
- Check the hardware requirements for the software upgrade. For information about hardware requirements:
  http://entsupport.symantec.com/docs/302144
- Ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.
- Run the Configuration Checker or access the VIAS website to verify whether the systems in your environment meet the requirements to upgrade the Veritas Storage Foundation and High Availability software:
  See "Using the Configuration Checker" on page 35.
- If you are running Veritas NetBackup™ version 6.0 or 6.5 on systems where you are upgrading to SFW HA 5.1 SP1, then you must shut down the OpsCenterServer service prior to the upgrade. Both NetBackup and SFW HA 5.1 SP1 share the same AT broker and client, and for this reason the OpsCenterServer service must by shut down prior to an upgrade.
- On Windows Server 2003 systems, set the Windows driver signing options:
  See "Changing the driver signing options" on page 98.
- On Windows Server 2008 systems and for an SFW HA 5.1 SP1 upgrade, enable the Computer Browser Service:
  See "Enabling the Computer Browser service for Windows Server 2008" on page 99.
- On Windows Server 2008 systems, activate Microsoft Windows:
  See "Activating Microsoft Windows on your server" on page 99.
- On Windows Server 2008 systems that you also plan to upgrade, review additional upgrade procedures that may be required depending upon the order in which you upgrade Microsoft Windows 2008 and upgrade to SFW or SFW HA 5.1 SP1:
  See "Upgrading Microsoft Windows Server 2008 after upgrading to SFW or SFW HA 5.1 SP1" on page 99.
- Check to see if you need to update the Microsoft Active Directory to support the upgraded software. For example, upgrading from Microsoft Exchange 2000 to Exchange 2003 requires updating the Active Directory.
- Test the system after each upgrade, especially after applying product upgrades to meet the minimum version required. An incremental upgrade eases the troubleshooting process.

Note: For an SFW HA 5.1 SP1 upgrade, back up all PrintShare registry keys before upgrading from SFW HA 4.3. MP2 or 5.0.x to SFW HA 5.1 SP1. PrintShare is changed in SFW HA 5.1 SP1 in that there no longer is a REGREP resource. Note that this step is not required when upgrading to SFW HA 5.1 SP1 in an Exchange or SQL Server cluster.

Changing the driver signing options

Some drivers provided by Symantec may not be signed by Microsoft. Depending upon your installation options, these unsigned drivers may stop your installation.

When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

Table 5-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers.

Table 5-1 Installation behavior with unsigned drivers

Driver Signing Setting	Installation behavior on the local system	Installation behavior on remote systems
Ignore	Always allowed	Always allowed
Warn	Warning message, user interaction required	Installation proceeds. The user must log on locally to the remote system to respond to the dialog box to complete the installation.
Block	Never allowed	Never allowed

On local systems set the driver signing option to either Ignore or Warn. On remote systems set the option to Ignore to allow the installation to proceed without user interaction.

To change the driver signing options on each system

1. Log on locally to the system.
2. Open the Control Panel and click **System**.
3. Click the **Hardware** tab and click **Driver Signing**.
4. In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.

5 Click **OK**.

6 Repeat for each computer.

If you do not change the driver signing option, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing option to its previous state.

Enabling the Computer Browser service for Windows Server 2008

The Microsoft Computer Browser service helps maintain an updated list of domains, workgroups, and server computers on the network and supplies this list to client computers upon request. This service must be enabled for the Symantec product installer to discover and display all domain members during an SFW HA 5.1 SP1 installation.

By default, systems running Windows Server 2008 (x86/x64/IA64) disable the Computer Browser service. With this service disabled, remote domain members in the computer lists do not display during an SFW HA 5.1 SP1 upgrade.

Enable the Computer Browser Service on your Windows Server 2008(x86/x64/IA64) systems before performing an upgrade to SFW HA 5.1 SP1.

Refer to your Microsoft documentation for information about enabling the Computer Browser service.

Activating Microsoft Windows on your server

Before proceeding with an upgrade on a system running Windows Server 2008, Symantec recommends that you activate Microsoft Windows.

If you do not activate Microsoft Windows before an upgrade, an "Optional update delivery is not working message" may appear. You can ignore this message, click **Close**, and continue with the upgrade.

Upgrading Microsoft Windows Server 2008 after upgrading to SFW or SFW HA 5.1 SP1

This section describes additional procedures required when performing the followings tasks::

- Upgrading from SFW 5.1 to SFW 5.1 SP1, and then upgrading your Windows Server 2008 operating system to Windows Server 2008 R2 or SP2
- Upgrading from SFW HA 5.1 to SFW HA 5.1 SP1, and then upgrading your Windows Server 2008 operating system to Windows Server 2008 R2 or SP2

Upgrading to SFW 5.1 SP1 and upgrading to Windows Server 2008 R2 or SP2

When upgrading your Microsoft Windows Server 2008 operating system to Windows Server 2008 R2 or SP2, Symantec recommends performing the Windows upgrade before upgrading from SFW 5.1 to SFW 5.1 SP1. If you follow this recommendation, then no additional steps are required for the SFW 5.1 SP1 upgrade.

In some circumstances though, you may need to upgrade to SFW 5.1 SP1 before upgrading Windows. If you upgrade from SFW 5.1 to SFW 5.1 SP1 before upgrading your Windows Server 2008 operating system to R2 or SP2, then you must run the following SFW repair installations:

- First, run the SFW repair installation with the **Veritas Storage Foundation 5.1 SP1 for Windows (Server Components)** option selected.
  For information about running a repair installation:
  See "Repairing the installation" on page 84.
- After this repair installation, run a second SFW repair installation with the **Service Pack 1 for SFW 5.1, SFWHA 5.1, and VCS 5.1 for Windows** option selected.

Note: This procedure also applies to an SFW Basic installation.

Upgrading to SFW HA 5.1 SP1 and upgrading to Windows Server 2008 R2 or SP2

When upgrading your Microsoft Windows Server 2008 operating system to Windows Server 2008 R2 or SP2, Symantec recommends performing the Windows upgrade before upgrading from SFW HA 5.1 to SFW HA 5.1 SP1. If you follow this recommendation, then no additional steps are required for the SFW HA 5.1 SP1 upgrade.

In some circumstances though, you may need to upgrade to SFW HA 5.1 SP1 before upgrading Windows. If you upgrade from SFW HA 5.1 to SFW HA 5.1 SP1 before upgrading your Windows Server 2008 operating system, then you must perform the following procedure.

SFW utility and repair procedure

1 Run the SFW utility called FixVDSKey.bat after the Windows Server 2008 R2 or SP2 upgrade. This SFW utility is located at: %VMPATH%\FixVDSKey.bat

Note: Running this utility restarts the Storage Agent (VxVM) and VDS services.

2 Run an SFW repair installation with the **Veritas Storage Foundation 5.1 SP1 for Windows (server components)** option selected. For information about running a repair installation:

See "Repairing the installation" on page 84.

After upgrading to SFW HA 5.1 SP1 and then upgrading to Windows Server 2008 R2 or SP2, you must access and run this utility and then perform a repair installation.

SFW and Microsoft Clustering upgrade notes

Note the following information for upgrading with SFW and Microsoft clustering:

- During an upgrade, you may encounter messages while the installer validates the selected systems. These informational messages do not indicate an error. If an error occurs, the system's status confirms the problem.
- To perform this upgrade, use a rolling upgrade procedure that involves installing SFW 5.1 on inactive nodes of the cluster. You then use the `Move Group` command in MSCS or Microsoft failover clustering to move the active node and install SFW on the cluster's remaining nodes.

SFW HA and VCS configuration upgrade notes

While upgrading an SFW HA and VCS configuration, the product installer performs the following tasks:

- Replaces the attribute types and names in the VCS 4.x configuration with those compatible with an SFW HA 5.1 configuration. For example, the Exchange application agent attribute E2kService is upgraded to ExchService.
- Maps the default attribute values in a VCS 4.x configuration to the default attribute values in a VCS 5.1 configuration.
- Deletes the attributes that are no longer required by SFW HA 5.1. For example, the wizard removes the AgentDebug attribute.

- Updates user passwords. Using a different encryption mechanism, SFW HA 5.1 decrypts the passwords and re-encrypts them using the VCS 5.1 encryption mechanism.

Chapter 6

Upgrading to SFW 5.1 SP1

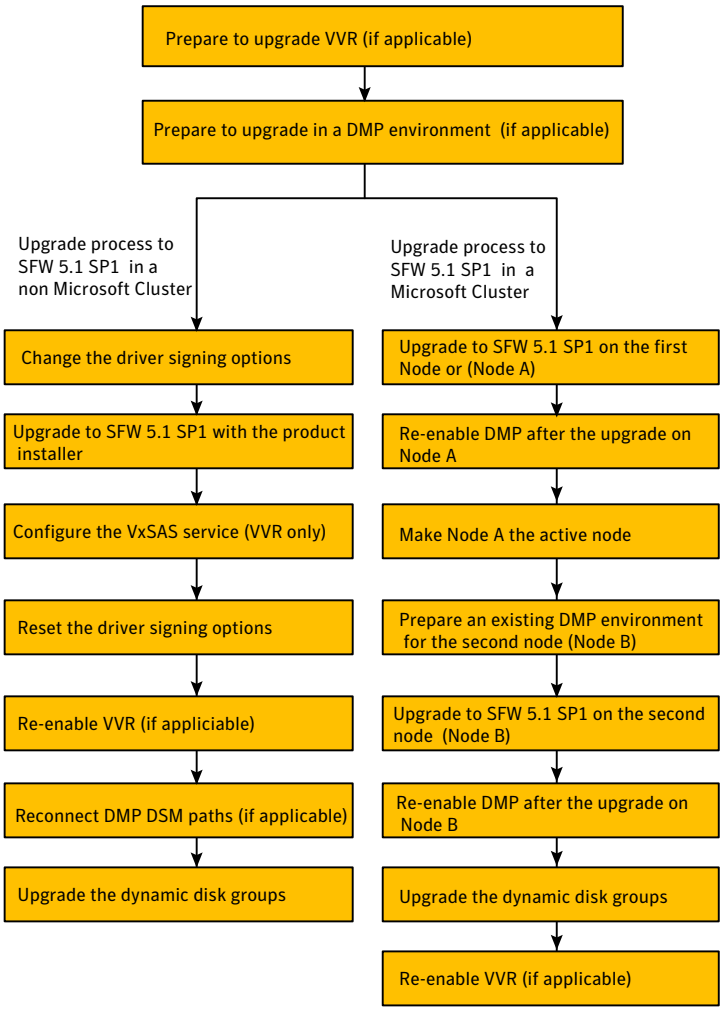
This chapter includes the following topics:

About upgrading to SFW 5.1 SP1

This chapter discusses upgrading to SFW 5.1 SP1.

Figure 6-1 displays the general SFW 5.1 SP1 upgrade tasks for both a Microsoft cluster environment and a non-Microsoft cluster environment.

Figure 6-1 SFW 5.1 SP1 general upgrade tasks



Note: If you have already installed and configured Veritas Volume Replicator (VVR) or DMP, the upgrade process includes additional procedures before and after the upgrade to SFW 5.1 SP1.

Depending upon your configuration, use the following sequence of tasks that are appropriate:

- If your configuration is running VVR, then prepare to upgrade VVR.
- If your upgrade is to occur in a DMP environment, then prepare to upgrade in a DMP environment.
- Upgrade from an earlier SFW 4.3 MP2, 5.0.x , or 5.1.x versions to SFW 5.1 SP1 in a non-Microsoft cluster (if applicable).
- Upgrade to SFW 5.1 SP1 in a Microsoft cluster environment (if applicable).
- Re-enable VVR in a non-Microsoft clustered environment or in a Microsoft clustered environment.
- Reconnect DMP DSM paths after the upgrade.
- Upgrade dynamic disk group versions.

Preparing to upgrade to SFW 5.1 SP1 in a VVR environment

Table 6-1 displays the different upgrade paths for SFW 5.1 SP1 in a VVR environment.

Review the following appropriate sections for your configuration if upgrading to SFW 5.1 SP1 in a VVR environment:

Table 6-1 SFW 5.1 SP1 VVR environment upgrade paths

Upgrade path	Description
Upgrade to in a non-clustered VVR environment from SFW 4.3 MP2 to SFW 5.1 SP1	For information about this upgrade path: See "Preparing non-clustered VVR environment for upgrade from SFW 4.3 MP2" on page 106.
Upgrade in a non-clustered VVR environment from SFW 5.0.x or 5.1.x to SFW 5.1 SP1	For information about this upgrade path: See "Preparing non-clustered VVR environment for upgrade from SFW 5.0.x or 5.1.x" on page 109.
Upgrade in a Microsoft clustered VVR environment from SFW 4.3 MP2 to SFW 5.1 SP1	For information about this upgrade path: See "Preparing Microsoft clustered VVR environment for upgrade from SFW 4.3 MP2" on page 110.

Table 6-1 SFW 5.1 SP1 VVR environment upgrade paths *(continued)*

Upgrade path	Description
Upgrade in a Microsoft clustered VVR environment from SFW 5.0.x or 5.1.x to SFW 5.1 SP1	For information about this upgrade path: See "Preparing Microsoft clustered VVR environment for upgrade from SFW 5.0.x or 5.1.x" on page 114.

Preparing non-clustered VVR environment for upgrade from SFW 4.3 MP2

If you use VVR to replicate data from a primary site to a secondary site, use the following procedures to stop the replicated volume group (RVG) and detach the replication links (RLINKs). For VVR related details, refer *Veritas Storage Foundation Volume Replicator, Administrator's Guide*.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

To prepare the primary site

1. Stop the application that uses VVR to replicate data between the sites.
2. Open a command window by clicking **Start > Run**. In the Open field, enter **cmd**, and click **OK**.
3. To get the list of RLINK and RVG records, run the following command on the primary site:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

4. Stop the RVG to prevent the application from accessing or modifying the volumes during the upgrade by performing one of the following procedures:
   - From the Veritas Enterprise Administrator (VEA) console, right-click the RVG and select the **Disable Data Access** option.
     The Disable Data Access operation prevents the user or application from writing any data to the data volumes.
   - From the command line, type:

     ```
     vxrvg stop [-g diskgroup_name] rvg_name
     ```

     This command disables Input/Output access to the associated data volumes.

5 Verify that the data on the Replicator Log is written to the secondary site by running the following command on the primary site:

```
vxrlink [-g diskgroup_name] status rlink_to_secondary
```

This command displays the replication status of the secondary represented by the specified RLINK. This command can be run only on the primary site. Verify that the data volumes on the secondary are consistent and up-to-date with the primary before proceeding to the next step.

6 Detach the RLINK to prevent VVR from replicating data to the secondary site by performing one of the following procedures:

- From the VEA console, right-click the secondary RVG and select the **Stop Replication** option.
  The Stop Replication option is available only when selecting the secondary RVG. When this operation is performed the connection between the primary and secondary RVG is broken.
- From the command line, type:

  ```
  vxrlink [-g diskgroup_name] det rlink_name
  ```

  This command detaches the RLINK from the RVG.

7 Disassociate the Replicator Log volume from the RVG by performing one of the following procedures:

- From the VEA console, right-click the Replicator Log and select the **Dissociate Replicator Log** option.
- From the command line, type:

  ```
  vxrvg [-f] [-g diskgroup] [-r rvg_name] dis volume_name
  ```

This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary is completely up-to-date with the primary. Otherwise this option can cause data corruption.

To prepare the secondary site

1. Open a command window by clicking **Start > Run** in the task bar. In the Open field, enter **cmd**, and click **OK**.
2. To get a list of RLINK and RVG records, run the following command:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

3. Stop the RVG to prevent the application from accessing or modifying the volumes during the upgrade by performing one of the following procedures:
   - From the VEA console, right-click the RVG and select the **Disable Data Access** option.
     The Disable Data Access operation prevents the user or application from writing any data to the data volumes.
   - From the command line, type:

     ```
     vxrvg [-g diskgroup_name] stop rvg_name
     ```

     This command disables Input/Output access to the associated data volumes.
4. If you used VEA to stop replication on the primary site, then you do not need to perform this step on the secondary site. However, if you used the command line to detach RLINK while preparing the primary site, then you should perform this action on the secondary site as well.

   From the command line, type:

   ```
   vxrlink [-g diskgroup] det rlink_name
   ```

   This command detaches an RLINK from the secondary RVG.
5. Disassociate the Replicator Log from the RVG by performing one of the following procedures:
   - From the VEA console, right-click the Replicator Log and select the **Dissociate Replicator Log** option.
     This option is available for selection only if the Replicator Log is associated with an RVG.
   - From the command line, type:

     ```
     vxrvg [-f] [-g diskgroup] [-r rvg_name] dis volume_name
     ```

     This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary site is completely up-to-date with the primary. Otherwise this option can cause data corruption.

Preparing non-clustered VVR environment for upgrade from SFW 5.0.x or 5.1.x

VVR 5.0.x and VVR 5.1 are interoperable; hence an upgrade can be performed on the secondary site while applications are kept running on the primary site.

The overall sequence is as follows:

- Upgrade the existing secondary site to SFW 5.1 SP1. No preparation is needed on the secondary site for a non-clustered VVR environment before performing the upgrade:
  See "Upgrading to SFW 5.1 SP1" on page 120.
- Prepare the existing primary site for the upgrade using the procedure in this section. The preparation includes migrating the primary role so that the existing primary site becomes the secondary site.
- Upgrade the old primary (now in the secondary role) to SFW 5.1 SP1.
- If desired, migrate the primary role back to the original primary site:
  See "Post-upgrade task for a non-clustered VVR environment after upgrading from 5.0.x or 5.1.x" on page 145.

The following procedure assumes that you have upgraded the secondary site to SFW 5.1 SP1. Now you must prepare the primary site for the upgrade.

To prepare the primary site

1. On the primary site, stop the application that uses VVR to replicate data between the sites.
2. From the command line, type:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

   This command lists the RLINK and RVG records.

3 Verify that the data on the Replicator Log is written to the secondary site by running the following command on the primary site:

```
vxrlink [-g diskgroup_name] status rlink_to_secondary
```

This command displays the replication status of the secondary site represented by the specified RLINK.

Verify that the data volumes on the secondary site are consistent and up-to-date with the primary site before proceeding to the next step.

4 Migrate the primary RVG by performing one of the following procedures:

- From the Veritas Enterprise Administrator (VEA) console, right-click the primary RVG and select the **Migrate** option. Select the required secondary host from the Secondary Name option list.
  Click **OK** to migrate the primary role to the secondary. The primary and secondary roles will be interchanged.
- From the command line, type:

  ```
  vxrds [-g diskgroup_name] migrate local_rvg new_primary_hostname
  ```

  Where the secondary host is specified by the *new_primary_hostname* parameter.

5 Perform any necessary steps to start the applications on the new primary (old secondary).

6 If the existing replication settings are configured to use TCP, change the settings to use UDP. After both the primary and DR sites are upgraded to 5.1, you can switch the replication settings back to TCP.

You can now upgrade the nodes on the old primary site (now the secondary site) to SFW 5.1 SP1:

See "Upgrading to SFW 5.1 SP1" on page 120.

After the upgrade you can switch the primary role back to the original primary site:

See "Post-upgrade task for a non-clustered VVR environment after upgrading from 5.0.x or 5.1.x" on page 145.

Preparing Microsoft clustered VVR environment for upgrade from SFW 4.3 MP2

Use the following procedures to prepare VVR in an MSCS environment on Windows Server 2003 before upgrading from SFW 4.3 MP2 to SFW 5.1 SP1. Follow the procedures in the given order while upgrading.

Refer to the *Veritas Storage Foundation Volume Replicator, Administrator's Guide* for details on VVR.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

To prepare the primary site in an MSCS environment

1. Offline the Application resource on the primary site by performing one of the following procedures:
   - From the Cluster Administrator console, right-click the Application resource and select the **Offline** option.
   - From the command prompt, type:

```
[cluster resourcename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

2. Take the RVG resource offline by performing one of the following procedures:
   - From the Cluster Administrator console, right-click the RVG resource and select the **Offline** option.
   - From the command prompt, type:

```
[cluster resourcename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

3. From the command prompt, type:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

   This command lists the RLINK and RVG records.

4. Verify that the data in the Replicator Log is written to the secondary site by running the following command on the primary:

   ```
   vxrlink [-g diskgroup_name] status rlink_to_secondary
   ```

   This command displays the replication status of the secondary represented by the specified RLINK. Verify that the data volumes on the secondary site are consistent and up-to-date with the primary before proceeding to the next step.

5. Detach the RLINK to prevent VVR from replicating data to the secondary site by performing one of the following procedures:
   - From the Veritas Enterprise Administrator (VEA) console, right-click the secondary RVG and select the **Stop Replication** option to stop VVR from replicating to the secondary site.

The Stop Replication option is available only on selecting the secondary RVG. When this operation is performed the connection between the primary and secondary RVG is broken.

- From the command prompt, type:

```
vxrlink [-g diskgroup] det rlink_name
```

This command detaches the RLINK from the RVG.

6 Dissociate the Replicator Log volume from the RVG by performing one of the following procedures:

- From the VEA console, right-click the Replicator Log volume and select the **Dissociate Replicator Log** option.
- From the command prompt, type:

```
vxrvg [-f] [-g diskgroup_name] [-r rvg_name] dis volume_name
```

This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary site is completely up-to-date with the primary. Otherwise this option can cause data corruption.

---

7 Take the Disk Group resource offline on the primary site by performing one of the following procedures:

- From the Cluster Administrator console, right-click the Disk Group resource and select the **Offline** option.
- From the command prompt, type:

```
[cluster resourcename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

Repeat the step to offline the IP resource and then the Network Name resource.

To prepare the secondary site in an MSCS environment

1 Take the RVG resource offline by performing one of the following:

- From the Cluster Administrator console, right-click the RVG resource and select the **Offline** option.
- From the command prompt, type:

```
[cluster resourcename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

2. To get the list of RVG and RLINK records from the command prompt, type:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

3. If you used VEA to stop replication on the primary site, then you do not need to perform this step on the secondary site. However, if you used the command line to detach RLINK while preparing the primary site, then you should perform this action on the secondary site as well.

   To do so from the command prompt, type:

   ```
   vxrlink {-g diskgroup] det rlink_name
   ```

4. Dissociate the Replicator Log volume from the RVG by performing one of the following procedures:

   - From the VEA console, right-click the Replicator Log volume and select the **Dissociate Replicator Log** option from the menu that appears.
   - From the command prompt, type:

     ```
     vxrvg [-f] [-g diskgroup_name] [-r rvg_name] dis volume_name
     ```

     This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

   Warning: Use the -f option only when you are sure that the secondary site is completely up-to-date with the primary. Otherwise this option can cause data corruption.

   ---

5. Offline the Disk Group, IP, and Network Name resources on the secondary site by performing one of the following procedures:

   - From the Cluster Administrator console, right-click the Disk Group resource and select the **Offline** option from the context-menu that appears.
   - From the command prompt, type:

```
[cluster resourename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

   Repeat the step to offline the IP resource and then the Network Name resource.

Preparing Microsoft clustered VVR environment for upgrade from SFW 5.0.x or 5.1.x

Since VVR 5.0.x and VVR 5.1 versions are interoperable, an upgrade can be performed on the DR (secondary) site while applications are kept running on the primary site.

Use the following overall sequence:

- Prepare the nodes on the secondary (DR) site to upgrade from SFW 5.0.x or 5.1.x to 5.1 SP1:
  See "Preparing the secondary (DR) site for the upgrade from SFW 5.0.x or 5.1.x" on page 114.
- Upgrade the cluster nodes on the secondary site to SFW 5.1 SP1:
  See "Upgrading to SFW 5.1 SP1" on page 120.
- Re-enable VVR on the upgraded secondary site:
  See "Re-enabling VVR in a Microsoft clustered environment after upgrade from 5.0.x or 5.1.x" on page 148.
- Prepare the nodes on the primary site for the upgrade. The preparation includes migrating the primary role so that the existing primary site becomes the secondary site:
  See "Preparing the primary site for the upgrade from SFW 5.0.x or 5.1.x" on page 115.
- Upgrade the old primary site (now the secondary site) to SFW 5.1 SP1:
  See "Upgrading to SFW 5.1 SP1" on page 120.
- Re-enable VVR on the upgraded nodes. The procedures include steps for migrating the primary role back to the original primary site:
  See "Re-enabling VVR in a Microsoft clustered environment after upgrade from 5.0.x or 5.1.x" on page 148.

Preparing the secondary (DR) site for the upgrade from SFW 5.0.x or 5.1.x

Follow the procedure to prepare the secondary site in an MSCS clustered VVR environment to upgrade from SFW 5.0.x or 5.1.x to SFW 5.1 SP1.

To prepare the secondary (DR) site

1 Take the RVG resource offline by performing one of the following procedures:

- From the Cluster Administrator console, right-click the RVG resource and select the **Offline** option
- From the command line, type:

```
[cluster resourcename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

2 Take the Disk Group resource offline on the secondary site by performing one of the following procedures:

- From the Cluster Administrator console, right-click the Disk Group resource, and select the **Offline** option.
- From the command prompt, type:

```
[cluster resourcename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

Repeat step 2 to offline the IP resource and then the Network Name resource.

Warning: Taking the DG (Disk Group) resource offline pauses replication, and if applications continue to run on the primary for too long, this may cause a possible replicator log overflow.

---

3 If the existing replication settings are configured to use TCP, change the settings to use UDP. After both the primary and DR sites are upgraded to 5.1, you can switch the replication settings back to TCP.

You can now upgrade all nodes on the DR site:

See "Upgrading to SFW 5.1 SP1" on page 120.

After the upgrade, you can re-enable VVR on the DR site:

See "Re-enabling VVR in a Microsoft clustered environment after upgrade from 5.0.x or 5.1.x" on page 148.

Next, continue with the procedure to prepare the primary site for the upgrade.

Preparing the primary site for the upgrade from SFW 5.0.x or 5.1.x

Once the DR site has been upgraded to SFW 5.1 SP1, the primary site can be prepared for upgrade by migrating the primary role to the DR site.

Follow the procedure described below to prepare the primary site in an MSCS clustered VVR environment to upgrade from SFW 5.0.x or 5.1.x to SFW 5.1 SP1.

To prepare the primary site

1 Offline the Application resource on the primary site by performing one of the following procedures:

- From the Cluster Administrator console, right-click the Application resource and select the **Offline** option.
- From the command line, type:

```
[cluster resourcename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

2. From the command line, type:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

   This command lists the RLINK and RVG records.

3. Verify that the data on the Replicator Log is written to the secondary site by running the following command on the primary:

   ```
   vxrlink [-g diskgroup_name] status rlink_to_secondary
   ```

   This command displays the replication status of the secondary represented by the specified RLINK.

   Verify that the data volumes on the secondary site are consistent and up-to-date with the primary before proceeding to the next step.

4. Migrate the primary RVG by performing one of the following procedures:

   - From the Veritas Enterprise Administrator (VEA) console, right-click the primary RVG and select the **Migrate** option. Select the required secondary host from the Secondary Name option list.
     Click **OK** to migrate the primary role to the secondary. The primary and secondary roles will be interchanged.
   - From the command line, type:

     ```
     vxrds [-g diskgroup_name] migrate local_rvg new_primary_hostname
     ```

     Where the secondary host is specified by the *new_primary_hostname* parameter.

5. Bring online the Application resource on the new primary by performing one of the following procedures:

   - From the Cluster Administrator console, right-click the Application resource and select the **Online** option.
   - From the command line, type:

```
[cluster resourcename] /Online [:node name] [/Wait[:timeoutin seconds]]
```

6 If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on the options available in your environment, these tasks may include mounting the databases or manually starting the application.

7 On the old primary site, which now has the secondary role, perform the steps described in the following section:

See "Preparing the secondary (DR) site for the upgrade from SFW 5.0.x or 5.1.x" on page 114.

You can then upgrade the old primary site to SFW 5.1 SP1:

See "Upgrading to SFW 5.1 SP1" on page 120.

After the upgrade on the old primary site, you can re-enable VVR on the site. If desired you can then migrate the primary role back to the old primary site:

See "Re-enabling VVR in a Microsoft clustered environment after upgrade from 5.0.x or 5.1.x" on page 148.

Preparing to upgrade in a DMP environment

This section covers the steps that must be taken to prepare to upgrade Veritas Storage Foundation 5.1 for Windows (SFW 5.1 SP1) in a DMP environment. If you are upgrading in a DMP environment, then follow the directions in this section.

When preparing to upgrade in a DMP environment, the following options are available:

- Prepare to add DMP DSMs to the upgraded environment when upgrading to SFW 5.1 SP1:
  See "Preparing to add DMP DSMs to upgraded environment when upgrading to SFW 5.1 SP1" on page 117.
- Prepare your existing DMP DSM environment for upgrade:
  See " DMP DSM environment" on page 118.
- Prepare your existing DMP ASL environment for upgrade:
  See " DMP ASL environment" on page 119.

Preparing to add DMP DSMs to upgraded environment when upgrading to SFW 5.1 SP1

If you do not have DMP DSMs in your existing environment, but plan to add this feature when upgrading to SFW 5.1 SP1, add the HBA (host bus adapter) hardware before performing the upgrade.

Refer to the Hardware Compliance List on the Symantec Support web site to determine the approved hardware for SFW.

See:http://entsupport.symantec.com/docs/302144

For more information about the hardware and software prerequisites for DMP DSM installation:

- See "Installing and uninstalling Veritas Dynamic Multi-pathing" on page 70.
- See *Veritas Storage Foundation Administrator's Guide*.

Connect no more than one path from the new HBA to the storage array before upgrading to SFW 5.1 SP1 and installing DMP DSMs. Select the DMP DSM option or the appropriate DMP DSMs while running the installer.

In a Microsoft cluster environment, you prepare the inactive node for the upgrade.

See "Upgrading to SFW 5.1 SP1 in a Microsoft cluster environment" on page 134.

Preparing an existing DMP environment for upgrading to SFW 5.1 SP1

Previous DMP environments are either DMP DSM or DMP ASL. The preparations for upgrade are different for each.

In a Microsoft cluster environment, you prepare DMP on the inactive node for the upgrade.

See "Upgrading to SFW 5.1 SP1 in a Microsoft cluster environment" on page 134.

DMP DSM environment

If you are preparing to upgrade an existing DMP DSM environment, it is recommended to physically disconnect all but one path of the multipath storage to shorten upgrade time.

No other DMP preparation is required except as follows.

When upgrading from SFW 4.3.x, and in the following cases only, you must uninstall DMP DSM before the upgrade (and reinstall it during the upgrade):

- SFW 4.3 with DMP option installed and no SFW 4.3 DDI-x has ever been applied
- SFW 4.3 DMP with DDI-1, DDI-3, DDI-4, DDI-5, or DDI-6 installed

Before uninstalling DMP DSM from a node in a cluster environment, the cluster resources should be moved to another node.

To uninstall the DMP or the DDI package

1. Make sure that only one path is attached for each array managed by DMP DSM.
2. Open the Windows Add/Remove Programs to uninstall the DDI. Select the Symantec support for DMP DSM entry and click **Remove** to begin the uninstallation.
3. Reboot the system when the uninstall process completes.

DMP ASL environment

DMP ASLs are no longer supported on SFW 5.1 SP1. Therefore, you must uninstall DMP ASLs before the upgrade to 5.1 SP1.

It is important that you detach all but one path to the storage array before you uninstall.

Warning: Failure to limit DMP ASLs to a single path before uninstalling can lead to data corruption.

Warning: Always back up your data before upgrading.

To prepare an existing DMP ASL environment for upgrade

1. Physically remove all but one path from each multiple-path array.
2. In the VEA, exclude each multiple-path array from DMP ASLs management.
3. In the tree view under the Disks folder, select a disk from the storage array that you are excluding.
4. In the right pane, click the Paths tab for the disk.
5. Right-click a path and select Array Settings from the path context menu that appears.
6. In the Array Settings screen, check the **Exclude** check box.
7. Click **OK**. The array is now excluded from DMP control.
8. Select **Actions > Rescan** from the VEA menu bar. Veritas Storage Foundation for Windows rescans the array and updates the display.
9. Uninstall the DMP ASLs using the Add or Remove function through the installer.

   See "Adding or removing features" on page 82.

10 After the uninstall process is complete, reboot the system.

11 If you want to install DMP DSMs during the upgrade, review the following information for more information on prerequisites for DMP DSMs:

- See "Installing and uninstalling Veritas Dynamic Multi-pathing" on page 70.
- *Veritas Storage Foundation Administrator's Guide.*

Upgrading to SFW 5.1 SP1

This section describes how to upgrade to SFW 5.1 SP1 from earlier SFW versions.

Table 6-2 describes the procedures that are used to upgrade to SFW 5.1 SP1.

Table 6-2 Upgrading to SFW 5.1 SP1 procedures

Step	Description
1	Change the driver signing options: See "Changing driver signing options" on page 121.
2	Upgrade to SFW 5.1 SP1 using the product installer: See "Upgrading using the product installer" on page 121.
3	Configure VxSAS server (VVR only): See "Configuring the VxSAS service (VVR only)" on page 131.
4	Reset the driver signing options: See "Resetting the driver signing options" on page 133.
5	Re-enable VVR: See "Re-enabling VVR in a non-clustered environment" on page 143.
6	Reconnect the DMP DSM paths: See "Reconnecting DMP DSM paths after the upgrade" on page 150.
7	Upgrade the dynamic disk groups: See "Upgrading dynamic disk group versions" on page 150.

Changing driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

For information on how to change the driver signing options on each system:

See "Changing the driver signing options" on page 98.

Upgrading using the product installer

Follow the appropriate product installer procedures for your upgrade:

- Upgrading from SFW 4.3 MP2 or 5.0.x to SFW 5.1 SP1 (Major Upgrade) using the product installer:
  See "Upgrading from SFW 4.3 MP2 or 5.0.x to SFW 5.1 SP1 using the product installer" on page 121.
- Upgrading from SFW 5.1.x to SFW 5.1 SP1 (Minor Upgrade) using the product installer:
  See "Upgrading from SFW 5.1.x to SFW 5.1 SP1 using the product installer" on page 127.

Upgrading from SFW 4.3 MP2 or 5.0.x to SFW 5.1 SP1 using the product installer

The following procedure describes how to upgrade from SFW 4.3 MP2 or 5.0.x to SFW 5.1 SP1 using the product installer. This procedure is called a Major Upgrade.

To upgrade from SFW 4.3 MP2 or 5.0.x to SFW 5.1 SP1 using the product installer

1. Insert the DVD containing the Major Upgrade software into your system or download the Major Upgrade software from the Symantec website.

   Allow the autorun feature to start the upgrade or double-click **Setup.exe**.

   The Select Product screen appears.

2. Review the links on the Select Product screen.

   Links on this screen access Late Breaking News, the Configuration Checker, as well as begin the process to install Storage Foundation 5.1 SP1 for Windows or Storage Foundation HA 5.1 SP1 for Windows.

   Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

   The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide, Installation and Upgrade Guide, and Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

3. Click **Storage Foundation 5.1 SP1 for Windows**.
4. Click the **Complete/Custom** link. The **Administrative Console** link lets you install only the Client components.

   The installer starts to copy files.

5. Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

   Click **Next**.

6 Read the License Agreement. If you agree to the license terms, click the **I AGREE TO the terms of the license agreement** radio button, and click **Next**.

7 Enter license keys for each Symantec product option that you are upgrading or installing:

- Enter the license key in the top field.
- To add a key, click **Add**. To remove a key, click the key to select it, and click **Remove**.
- Repeat the first two bulleted steps for each Symantec product and feature that you want to install. Click a key to see its details.
- Click **Next**.

8 Choose the options that you want to install by selecting or clearing the appropriate check boxes. You must select all currently installed options for upgrade. Click **Next**.

Displayed at the bottom of the screen is the total hard disk space required for the installation. When you add or remove an option, the total space changes.

When upgrading multiple computers in a single installation using the product installer, all the selected options for the multiple computers should be the same. This is only an issue if you are upgrading on more than one computer at once, and these computers have different options installed. However, if a superset of options is selected for the computers during the upgrade, then the upgrade proceeds as normal and all selected options (superset of options) will be installed on all the computers.

9 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows 2003 and Windows 2008.
Install Path	The install path cannot be changed for the upgrade.

10 The product installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

11 Depending upon your earlier product installer selections and operating system, you may receive one or more of the following messages.

If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning:	The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system. If you are upgrading in a cluster environment, you must configure the Veritas Scheduler Service on all nodes to allow the automatic transfer of Capacity Monitoring and Automatic Volume Growth settings. Refer to the Capacity Monitoring and Automatic Volume Growth sections of the SFW Administrator's Guide for more information. If applicable to your installation, perform the above procedures.
If you are using multiple paths and selected a specific DSM on a Windows Server 2008 machine, you receive an additional message:	On Windows Server 2008, the Microsoft Multipath input/output (Microsoft MPIO) feature must be enabled before installing DMP Device Specific Modules (DSMs). If applicable to your installation, perform the above second procedure.

When installing Veritas Storage Foundation 5.1 for Windows (Server Components) with the MSCS option selected, you receive another message:	When installing Veritas Storage Foundation 5.1 for Windows (Server Components) with the MSCS option, you may want MSCS Quorum Arbitration Time (Min and Max) to be adjusted to ensure optimal functionality with Veritas dynamic volumes with MSCS. For additional information, see the *Storage Foundation for Windows Administrator Guide*for details. If applicable to your installation, perform the above procedure to adjust the MSCS Quorum Arbitration Time.

When you are finished reviewing the message or messages click **OK**.

12 Review the pre-upgrade summary. Click **Back** to make changes if necessary.

Click **Install**.

13 If the installation is successful on all computers, the installer automatically proceeds to the summary page described in the next step .

If an installation fails, click **Next** to review the report and address the reason for failure. You may have to either repair the installation or uninstall and reinstall. If a security alert asks you to accept the Symantec driver software, click **Yes**.

14 A report summarizing the upgrade appears. Review it and click **Next**.

15 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default.

16 Select the upgrade remote computers.

17 Click **Reboot**.

18 Click **Next**.

19 Click **Finish**.

20 Click **Yes** to reboot the local computer.

- If you upgraded or installed the Volume Replicator (VVR) option, you can launch the wizard for Veritas Volume Replicator Security Service (VxSAS) after the reboot to configure security services for all computers. This step is required for VVR if you are upgrading from 4.3 versions. If you are upgrading from 5.0.x and VxSAS was already configured for 5.0.x, you do not need to configure it again.
  See "Configuring the VxSAS service (VVR only)" on page 131.

For details on this required service for VVR:
See the *Veritas Storage Foundation Volume Replicator, Administrator's Guide*.

- After upgrading, reset the driver signing option to its original setting. Failure to do this can compromise system security. If you are performing more upgrades, do not reset the options until you have completed the upgrade.
  See "Resetting the driver signing options" on page 133.

Upgrading from SFW 5.1.x to SFW 5.1 SP1 using the product installer

The following procedure describes how to upgrade from SFW 5.1.x to SFW 5.1 SP1 using the product installer. This procedure is called a Minor Upgrade.

Note: When upgrading from SFW 5.1.x to SFW 5.1 SP1, the product installer replaces the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator (VEA) GUI for Windows Server 2008. To change this default, access the VEA GUI after the upgrade completes and proceed to restore the Disk Management Snap-in. For information about using the VEA GUI, see *Veritas Storage Foundation™ Administrator's Guide*.

To upgrade from SFW 5.1.x to SFW 5.1 SP1 using the product installer

1. Insert the DVD containing the Minor Upgrade software into your system's disc drive or download the Minor Upgrade software from the Symantec website.
2. Allow the autorun feature to start the upgrade or double-click **Setup.exe**.

   The Select Product screen appears.

3 Review the links on the Select Product screen.

There are links on this screen to access Late Breaking News, Configuration Checker, and to begin the process to install Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide and the Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows**.

5 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

6 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows 2003 and Windows 2008.
Install Path	The install path cannot be changed for the upgrade.

7 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

8 Depending upon your earlier product installer selections, you may receive one or more of the following messages.

If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning stating the following:	The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system. If you are upgrading in a cluster environment, you must configure the Veritas Scheduler Service on all nodes to allow the automatic transfer of Capacity Monitoring and Automatic Volume Growth settings. Refer to the Capacity Monitoring and Automatic Volume Growth sections of the SFW Administrator's Guide for more information . If applicable to your installation, perform the above procedures.
When installing Veritas Storage Foundation 5.1 for Windows (Server Components) with the MSCS option selected, you receive another message:	When installing Veritas Storage Foundation 5.1 for Windows (Server Components) with the MSCS option, you may want MSCS Quorum Arbitration Time (Min and Max)to be adjusted to ensure optimal functionality with Veritas dynamic volumes with MSCS. For additional information, see the *Storage Foundation for Windows Administrator Guide*for details. If applicable to your installation, perform the above procedure.

Click **OK**.

9 Review the pre-upgrade summary. Click **Back** to make changes if necessary.

Click **Install**.

10 If the installation is successful on all nodes, the installer automatically proceeds to the summary page described in the next step.

   If the installation fails, click **Next** to review the report and address the reason for failure. You may have to either repair the installation or uninstall and reinstall. If a security alert asks you to accept the Symantec driver software, click **Yes**.

11 A report summarizing the upgrade appears. Review it and click **Next**.

12 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default.

13 Select the upgraded remote computers.

14 Click **Reboot**.

   Wait for the remote computer to come back online.

15 Click **Next**.

16 Click **Finish**.

17 Click **Yes** to reboot the local node.

   After upgrading, reset the driver signing option to its original setting. Failure to do this can compromise system security. If you are performing more upgrades, do not reset the options until you have completed the upgrade.

   See "Resetting the driver signing options" on page 133.

Configuring the VxSAS service (VVR only)

The procedure to configure the VxSAS service for VVR has the following prerequisites:

- You must be logged on with administrative privileges on the server for the wizard to be launched.
- The account you specify must have administrative and log-on as service privileges on all the specified hosts.
- Avoid specifying blank passwords. In a Windows Server environment, accounts with blank passwords are not supported for log-on service privileges.
- Make sure that the hosts on which you want to configure the VxSAS service are accessible from the local host.

The VxSAS wizard will not be launched automatically after installing SFW or SFW HA. You must launch this wizard manually to complete the VVR security service configuration.

For details on this required service, see the *Veritas Storage Foundation Veritas Volume Replicator Administrator's Guide*.

To configure the VxSAS service

1 To launch the wizard, select **Start > All Programs > Symantec > Veritas Storage Foundation > Configuration Wizards > VVR Security Service Configuration Wizard** or run `vxsascfg.exe` from the command prompt of the required machine.

Read the information provided on the Welcome page and click **Next**.

2 Complete the Account Information panel as follows:

Account name (domain\account)	Enter the administrative account name.
Password	Specify a password.

If you have already configured the VxSAS service for one host that is intended to be a part of the RDS, make sure you specify the same username and password when configuring the VxSAS service on the other hosts.

Click **Next**.

3 On the Domain Selection panel, select the domain to which the hosts that you want to configure belong:

Selecting domains	The Available domains pane lists all the domains that are present in the Windows network neighborhood. Move the appropriate name from the Available domains list to the Selected domains list, either by double-clicking it or using the arrow button.
Adding a domain	If the domain name that you require is not displayed, click **Add domain**. This displays a dialog that lets you specify the domain name. Click **Add** to add the name to the Selected domains list.

Click **Next**.

4 On the Host Selection panel, select the required hosts:

Selecting hosts	The Available hosts pane lists the hosts that are present in the specified domain. Move the appropriate host from the Available hosts list to the Selected hosts list, either by double-clicking it or using the arrow button. Use the Shift key with the up or down arrow keys to select multiple hosts.
Adding a host	If the host name you require is not displayed, click **Add host**. In the Add Host dialog specify the required host name or IP in the **Host Name** field. Click **Add** to add the name to the Selected hosts list.

After you have selected a host name, the **Configure** button is enabled. Click **Configure** to proceed with configuring the VxSAS service.

5 After the configuration completes, the Configuration Results page displays whether or not the operation was successful. If the operation was not successful, the page displays the details on why the account update failed, along with the possible reasons for failure and recommendations on getting over the failure.

Click **Back** to change any information you had provided earlier.

6 Click **Finish** to exit the wizard.

Resetting the driver signing options

After completing the installation sequence, reset the driver signing option (set prior to upgrade) on each computer running Windows 2003.

To reset the driver signing options

1 Open the Control Panel, and click **System**.

2 Click the Hardware tab and click **Driver Signing**.

3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat for each computer.

Upgrading to SFW 5.1 SP1 in a Microsoft cluster environment

In a Microsoft cluster (MSCS) environment, you can upgrade from SFW 4.3 MP2, SFW 5.0.x, or SFW 5.1.x to SFW SP1. This section applies to all of these upgrades.

When you upgrade from SFW 4.3 MP2, SFW 5.0.x, or SFW 5.1.x with a Microsoft cluster (MSCS) to SFW 5.1 SP1, SFW requires a reboot. Rebooting an active cluster node causes it to fail over. To avoid this, you upgrade first on an inactive cluster node, switch the active cluster node to a second node, and then upgrade the first node.

In the following example procedure, the two nodes in the cluster are Node A and Node B. Initially, Node A is the inactive cluster node and Node B is the active cluster node. After completing the following upgrade steps, Node A becomes the active cluster node. You can use the Cluster Administrator (Windows 2003) console to make Node B the active cluster node after finishing the upgrade.

Table 6-3 displays the tasks required to upgrade from SFW 4.3 MP2, SFW 5.0.x, or SFW 5.1.x to SFW 5.1 SP1 in a Microsoft cluster environment.

Table 6-3 Upgrade process to SFW 5.1 SP1 in a Microsoft cluster environment

Step	Task	Description
1	Prepare a VVR environment for the upgrade.	If VVR is installed and configured on your existing configuration, then make sure that you have prepared VVR for the upgrade by following specific procedures on the active cluster node. See "Preparing to upgrade to SFW 5.1 SP1 in a VVR environment" on page 105. **Note:** The procedures to prepare VVR for the upgrade must be carried out on the active node of the cluster and are done only once; they are not repeated when you switch the active cluster node.

Table 6-3 Upgrade process to SFW 5.1 SP1 in a Microsoft cluster environment *(continued)*

Step	Task	Description
2	Prepare an existing DMP environment for upgrading on Node A.	For Node A (the inactive node), prepare DMP if you have DMP installed. Make sure that the active node of the cluster is Node B before starting this process. See "Preparing to upgrade in a DMP environment" on page 117.
3	Upgrade to SFW 5.1 SP1 on Node A.	For Node A, upgrade to SFW 5.1 SP1. See "Upgrading to SFW SP1 on Node A " on page 136.
4	Re-enable DMP after the upgrade on Node A.	For Node A, re-enable DMP if you have DMP installed. Make sure that the active node of the cluster is Node B before starting this process. See "Reconnecting DMP DSM paths after the upgrade" on page 150.
5	Make Node A the active node.	Move the active node. See "Making Node A the active node" on page 143.
6	Prepare an existing DMP environment for upgrading on Node B.	For Node B, prepare DMP if you have DMP installed. Make sure that the active node of the cluster is Node A before starting this process. See "Preparing to upgrade in a DMP environment" on page 117.
7	Upgrade SFW 5.1 SP1 on Node B (Node A active).	For Node B, upgrade to SFW 5.1 SP1. Make sure that the active node of the cluster is Node A before starting this task. To upgrade SFW 5.1 on Node B, refer to the guidelines for Node A. See See "Upgrading to SFW SP1 on Node A " on page 136.

Table 6-3 Upgrade process to SFW 5.1 SP1 in a Microsoft cluster environment *(continued)*

Step	Task	Description
8	Re-enable DMP after the upgrade on Node B.	For Node B, re-enable DMP if you have DMP installed. Make sure that the active node of the cluster is Node A before starting this task. See "Reconnecting DMP DSM paths after the upgrade" on page 150.
9	Upgrade the dynamic disk groups (Node A active).	Upgrade the dynamic disk groups if necessary. Make sure that the active node of the cluster is Node A before starting this task. **Note:** The steps for this procedure must be performed on the active node (Node A). See "Upgrading dynamic disk group versions" on page 150.
10	Re-enable VVR after upgrading all nodes.	In a VVR configuration, once the upgrade is complete on all cluster nodes, re-enable VVR on the active node. See "Re-enabling VVR in a Microsoft clustered environment" on page 146.

Upgrading to SFW SP1 on Node A

Before you begin the upgrade do the following:

- Make sure that the active node of the cluster is Node B.
- Set the Windows driver signing options to ignore warning messages.

Changing driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

For information on how to change the driver signing options on each system:

See "Changing the driver signing options" on page 98.

Upgrading to SFW 5.1 SP1 on Node A

Follow the appropriate product installer procedure for your upgrade:

- Upgrading from SFW 4.3 MP2 or SFW 5.0.x to SFW 5.1 SP1 (Major Upgrade) using the product installer:
  See "Upgrading from SFW 4.3 MP2 or SFW 5.0.x to SFW 5.1 SP1 using the product installer" on page 137.
- Upgrading from SFW 5.1.x to SFW 5.1 SP1 (Minor Upgrade) using the product installer:
  See "Upgrading from SFW 5.1.x to SFW 5.1 SP1 using the product installer" on page 140.

Upgrading from SFW 4.3 MP2 or SFW 5.0.x to SFW 5.1 SP1 using the product installer

The following procedure describes how to upgrade from SFW 4.3 MP2 or SFW 5.0.x to SFW 5.1 SP1 using the product installer on Node A. This procedure is called a Major Upgrade.

To upgrade from SFW 4.3 MP2 or SFW 5.0.x to SFW 5.1 SP1 on Node A

1. Insert the DVD containing the Major Upgrade software into your system's disc drive or download the Major Upgrade software from the Symantec website.
2. Allow the autorun feature to start the upgrade or double-click **Setup.exe**.

   The Select Product screen appears.

3 Review the links on the Select Product screen. Links on this screen access Late Breaking News, the Configuration Checker, as well as begin the process to install Storage Foundation 5.1 SP1 for Windows or Storage Foundation HA 5.1 SP1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide, Installation and Upgrade Guide, and Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Storage Foundation SP1 for Windows**.

5 Click **Complete/Custom** to upgrade the server components and optional client components.

6 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

7 Read the License Agreement. If you agree to the license terms, click the **I AGREE TO the terms of the license agreement** radio button, and click **Next**.

8 Enter a license key and click **Add**. To delete a key from the license key list, select it and click **Remove**.

Make sure that you have a Symantec license for each product that you are upgrading. Select a key in the key list to view details about the specified license.

Click **Next**.

9 The Option Selection screen appears.

You must select all currently installed options for upgrade, including the Cluster Option for Microsoft Cluster Service (MSCS)/Failover Cluster. If appropriate for your current configuration, also select the DMP Device Specific Modules (DSM) option.

Select the option to install client components and click **Next**.

10 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows 2003 and Windows 2008.
Install Path	The install path cannot be changed for the upgrade.

11 After the installer validates the systems for the installation, click **Next**.

If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

12 Click **OK** to ensure optimal arbitration time settings for the dynamic quorum.

The minimum and maximum time settings define the period that MSCS allows 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 the cluster.

13 Review the pre-upgrade summary information and click **Install**. If necessary, click **Back** to make any necessary changes.

14 The progress meter indicates the status of the installation. If a security alert asks you to accept the Symantec driver software, click **Yes**.

If the installation is successful on the system, the install report screen appears.

If an installation is not successful on any one of the systems, the status screen shows that the installation failed. Click **Next** to view the install report and take action where necessary.

15 Review the report and click **Next**.

16 Click **Finish**.

17 Reboot the local node.

After upgrading, reset the driver signing option to its original setting if you are running Windows Server 2003. Failure to do this can compromise system security. If you are performing more upgrades, do not reset the options until you have completed the upgrade.

Upgrading from SFW 5.1.x to SFW 5.1 SP1 using the product installer

The following section describes how to upgrade from SFW 5.1.x to SFW 5.1 SP1 using the product installer on Node A. This procedure is called a Minor Upgrade.

Note: When upgrading from SFW 5.1.x to SFW 5.1 SP1, the product installer replaces the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator (VEA) GUI for Windows Server 2008. To change this default, access the VEA GUI after the upgrade completes and proceed to restore the Disk Management Snap-in. For information about using the VEA GUI, see *Veritas Storage Foundation™ Administrator's Guide*.

To upgrade from SFW 5.1.x to SFW 5.1 SP1 on Node A

1 Insert the DVD containing the Minor Upgrade software into your system's disc drive or download the Minor Upgrade software from the Symantec website.

2 Allow the autorun feature to start the upgrade or double-click **Setup.exe**.

The Select Product screen appears.

3 Review the links on the Select Product screen.

There are links on this screen to access Late Breaking News, Configuration Checker, and to begin the process to install Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide and the Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Service Pack 1 for SFW 5.1, SFW HA5.1, and VCS 5.1 for Windows**.

5 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

6 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows 2003 and Windows 2008.
Install Path	The install path cannot be changed for the upgrade.

7 After the installer validates the systems for the installation, click **Next**.

If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

8 Click **OK** to ensure optimal arbitration time settings for the dynamic quorum.

The minimum and maximum time settings define the period that MSCS allows 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 the cluster.

9 Review the pre-upgrade summary information and click **Install**. If necessary click **Back** to make any necessary changes.

10 The progress meter indicates the status of the installation. If a security alert asks you to accept the Symantec driver software, click **Yes**.

If the installation is successful on the system, the install report screen appears.

If an installation is not successful on any one of the systems, the status screen shows that the installation failed. Click **Next** to view the install report and to take action where necessary.

11 Review the report and click **Next**.

12 Click **Finish**.

13 Reboot the local node.

After upgrading, reset the driver signing option to its original setting if you are running Windows Server 2003. Failure to do this can compromise system security. If you are performing more upgrades, do not reset the options until you have completed the upgrade.

Resetting the driver signing options

After completing the installation sequence, reset the driver signing option (set prior to upgrade) on each computer running Windows 2003.

To reset the driver signing options

1 Open the Control Panel, and click **System**.

2 Click the **Hardware** tab and click **Driver Signing**.

3 In the **Driver Signing Options** dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat the procedure for each computer.

Making Node A the active node

Perform the following steps to make node A the active node.

To make Node A the active node

1 From the Cluster Administrator (Windows 2003) console, navigate to the Cluster Group.

2 Right-click the Cluster Group and click **Move Group**.

This procedure moves the resources and the Resource Owner changes to Node A.

Re-enabling VVR in a non-clustered environment

After upgrading in a non-clustered environment where VVR replicates data from a primary site to a secondary site, you must re-enable VVR.

Use one of the following procedures:

- Re-enabling a non-clustered VVR environment after upgrading from 4.3 MP2
- Post-upgrade task for a non-clustered VVR environment after upgrading from 5.0.x or 5.1.x

Re-enabling a non-clustered VVR environment after upgrading from 4.3 MP2

After you have upgraded to SFW 5.1 SP1 from a 4.3 MP2 version, you must re-enable VVR. Follow the procedures in the given order.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

To enable the updated objects

1. To associate the dissociated Replicator Log again, perform one of the following procedures:

   - From the VEA console on the primary site, expand the RDS. Right-click on the RVG and select the **Associate Replicator Log** option. Select the correct Replicator Log volume from the dialog box and click **OK**.
   - From the command line, type:

     ```
     vxrvg [-g diskgroup_name] [-f] aslog rvg_name volume_name
     ```

     This command associates the specified Replicator Log with the RVG. Replication is not possible without a Replicator Log.

2. To attach the RLINK, run the following command:

   ```
   vxrlink -f [-g diskgroup_name] att rlink_name
   ```

   This command attaches one or more RLINKs to an RVG. If the -f option is used, then it forcefully associates the volumes.

   The RLINK must already be associated with the RVG before the attach as shown in step 1. For the attach to succeed, ensure that the data volumes on the secondary site are of the same name and size as on the primary site.

   Warning: Use the -f option only when you are sure that the secondary site is completely up-to-date with the primary. Otherwise this option can cause data corruption.

   ---

3. To enable data access and prepare the volumes to receive the writes from the application, perform one of the following procedures:

   - From the VEA console, select the primary RVG and then select **Enable Data Access** option from the right-click menu.
   - From the command line, type:

```
vxrvg [-g diskgroup_name] start rvg_name
```

This command enables Input/Output access to the specified data volumes.

4 Repeat step 1 through step 3 on the secondary site.

5 If needed, perform any necessary tasks to start the replication. Depending on options available in your environment, these tasks may include mounting databases or manually starting the application.

Post-upgrade task for a non-clustered VVR environment after upgrading from 5.0.x or 5.1.x

In the procedure for preparing the primary site for upgrade from SFW 5.0.x or 5.1.x to 5.1 SP1, you migrated the primary role to the secondary site.

After both the primary and secondary sites have been upgraded to SFW 5.1 SP1, you may want to migrate the role of the primary back to the original primary site. To do this, you perform a Migrate operation again as described in the following procedure.

To migrate the applications back to the original primary

1 On the current primary site, stop the application that uses VVR to replicate data between the sites.

2 From the command line, type:

```
vxprint -lVP [-g diskgroup_name]
```

This command lists the RLINK and RVG records.

3 Verify that the data on the Replicator Log is written to the secondary site by running the following command on the primary

```
vxrlink [-g diskgroup_name] status rlink_to_secondary
```

This command displays the replication status of the secondary represented by the specified RLINK.

Verify that the data volumes on the secondary site are consistent and up-to-date with the primary before proceeding to the next step.

4 To migrate the primary RVG perform one of the following procedures:

- From the VEA, right-click the primary RVG and select the **Migrate** option. Select the required secondary host from the Secondary Name option list. Click **OK** to migrate the primary role to the secondary.
  The primary and secondary roles will be interchanged.

- From the command line, type:

```
vxrds [-g diskgroup_name] migrate local_rvg new_primary_hostname
```

Where the secondary host is specified by the *new_primary_hostname* parameter.

5 Perform any necessary steps to start the applications on the new primary (old secondary).

Re-enabling VVR in a Microsoft clustered environment

In a Microsoft clustered environment, after you have completed installing the SFW upgrade on all cluster nodes, re-enable VVR on the active cluster node.

Depending upon your environment, follow one of the procedures listed below:

- Re-enabling VVR in a Microsoft clustered environment after upgrade from 4.3 MP2
- Re-enabling VVR in a Microsoft clustered environment after upgrade from 5.0.x or 5.1.x

Re-enabling VVR in a Microsoft clustered environment after upgrade from 4.3 MP2

After performing an upgrade from SFW 4.3 MP2 to SFW 5.1 SP1, re-enable VVR in the Microsoft cluster. Use the following procedures in order when re-enabling VVR after upgrading from 4.3 MP2.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

Note: Refer to the appropriate Microsoft documentation for details on how to offline and online resources through the command line interface.

To enable the updated objects (Windows Server 2003)

1 Bring online the Disk Group, IP, and Network Name resources in the MSCS resource group by performing one of the following procedures:

- From the Cluster Administrator console, right-click the Disk Group resource and select the **Online** option.
- From the command line, type:

```
[cluster resourcename] /Online [:node name] [/Wait[:timeoutin seconds]]
```

Repeat the step to bring online the IP resource and then the Network Name resource.

2. Associate the dissociated Replicator Log volume to the RVG again by performing one of the following procedures:
   - From the VEA, right-click the Replicator Log volume and select the **Associate Replicator Log** option.
   - From the command line, type:

     ```
     vxrvg [-g diskgroup_name] [-f] aslog rvg_name volume_name
     ```

3. To attach the RLINK, run the following command:

   ```
   vxrlink -f [-g diskgroup_name] att RLINK_name
   ```

   This command associates the specified Replicator Log to the RVG.
4. Repeat step 1 through step 3 on both the primary and secondary sites.
5. Bring online the RVG resource by performing one of the following procedures:
   - From the Cluster Administrator console, right-click the RVG resource and select the **Online** option on both the primary and secondary.
   - From the command line, type:

```
[cluster resourcename] /Online [:node name] [/Wait[:timeoutin seconds]]
```

Run this command on both the primary and secondary sites.

6. Bring online the Application resource on the primary by performing one of the following procedures:
   - From the Cluster Administrator console, right-click the Application resource and select the **Online** option.
   - From the command line, type:

```
[cluster resourcename] /Online [:node name] [/Wait[:timeoutin seconds]]
```

7. If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on options in your environment, these tasks may include mounting databases or manually starting the application. For VVR environments with multiple secondary sites, any operations that need to be performed on a secondary site must be repeated on all secondary sites.

Re-enabling VVR in a Microsoft clustered environment after upgrade from 5.0.x or 5.1.x

After performing an upgrade from SFW 5.0.x or 5.1.x to SFW 5.1 SP1, re-enable VVR in the Microsoft cluster. Follow the procedures in order when re-enabling VVR after upgrading from 5.0.x or 5.1.x to SFW 5.1 SP1.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

Note: Refer to the appropriate Microsoft documentation for details on how to offline and online resources through the command line interface.

To enable the updated objects on the secondary (DR) site (Windows Server 2003)

1. Bring online the Disk Group, IP, and Network Name resource in the MSCS resource group.
2. Bring online the RVG resource by performing one of the following procedures:
   - From the Cluster Administrator console, right-click the RVG resource and select the **Online** option on the secondary.
   - From the command line, type:

```
[cluster resourcename] /online [:node name] [/wait[:timeoutin seconds]]
```

Note: For VVR environments with multiple secondary sites, any operations that need to be performed on a secondary site should be repeated on all secondary sites.

If you are performing this procedure on the original secondary site, you now continue with the procedure to prepare the primary site.

See "Preparing the primary site for the upgrade from SFW 5.0.x or 5.1.x" on page 115.

Otherwise, if you completed the upgrades on both primary and secondary sites, you can now migrate the primary role back to the original primary:

See "Migrating the applications back to the original primary" on page 149.

Migrating the applications back to the original primary

After both the primary and secondary sites have been upgraded to SFW 5.1 SP1, you may want to migrate the primary role back to the original primary site.

To do this, perform a Migrate operation again as described in the following procedure.

To migrate the applications back to the original primary

1. Offline the Application resource on the current primary site by performing one of the following procedures:
   - From the Cluster Administrator console, right-click the Application resource and click **Offline**.
   - From the command prompt, type:

```
[cluster resourcename] /Offline [:node name] [/Wait[:timeoutin seconds]]
```

2. From the command prompt, type

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

   This command lists the RLINK and RVG records.

3. Verify that the data on the Replicator Log is written to the secondary site by issuing the following command on the primary:

   ```
   vxrlink [-g diskgroup_name] status rlink_to_secondary
   ```

   This command displays the replication status of the secondary represented by the specified RLINK.

   Verify that the data volumes on the secondary site are consistent and up-to-date with the primary before proceeding to the next step.

4. To migrate the primary RVG, perform one of the following procedures:
   - From the VEA, right-click the primary RVG and click **Migrate**. Select the required secondary host from the Secondary Name option list.
     Click **OK** to migrate the primary role to the secondary. The primary and secondary roles will be interchanged.
   - From the command line, type:

     ```
     vxrds [-g diskgroup_name] migrate local_rvg new_primary_hostname
     ```

Where the secondary host is specified by the *new_primary_hostname* parameter.

5 If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on the options available in your environment, these tasks may include mounting databases or manually starting the application.

Reconnecting DMP DSM paths after the upgrade

After you complete the upgrade for an existing DMP DSM environment or if you have added DMP DSMs during the upgrade, proceed to reconnect the DMP DSM paths:

To reconnect DMP DSM paths after the upgrade

1 Physically connect any additional paths that were disconnected before the upgrade.

2 In the VEA, rescan the disks.

Upgrading dynamic disk group versions

If your previous installation included Volume Manager 4.x, upgrade the disk group types to make use of the current program features.

For information about the current program features, see the *Veritas Storage Foundation 5.1 Administrator's Guide*.

Note: If you upgrade a disk group to SFW 5.1, you cannot import it to another server that is running an earlier version of Volume Manager or Disk Management. After upgrading a disk group, the group cannot revert to an earlier version.

To upgrade a dynamic disk group version

1 Open up the VEA.

In the tree view, right-click the disk group you want to upgrade and select **Upgrade Dynamic Disk Group Version**.

2 Click **Yes** to upgrade the dynamic disk group.

Chapter 7

Upgrading to SFW HA 5.1 SP1

This chapter includes the following topics:

About upgrading to SFW HA 5.1 SP1

This chapter describes upgrading from SFW HA 4.3 MP2, 5.0.x, 5.1.x to SFW HA 5.1 SP1.

Information on upgrading SFW HA in Microsoft Exchange, Microsoft SQL Server, and Oracle environments are described in the following chapters:.

- For upgrade procedures for a Microsoft Exchange Server cluster:
  See "About upgrading an Exchange Server cluster" on page 175.
- For upgrade procedures for a Microsoft SQL Server cluster:
  See "About upgrading a SQL Server cluster" on page 201.
- For upgrade procedures for Oracle environments:
  See "About upgrading an Oracle cluster" on page 269.

The required procedures for upgrading to SFW HA 5.1 SP1 depend upon your environment. For example, if you have installed and configured VVR or DMP, you must take additional steps before and after the upgrade to SFW HA 5.1 SP1.

The following procedures describe the upgrade process to SFW HA 5.1 SP1:

- Pre-upgrade tasks:
  See "About preparing for upgrade" on page 95.
- Preparing VVR in a VCS environment for upgrade:
  See "Preparing VVR in a VCS environment for upgrade" on page 152.
- Preparing to upgrade in a DMP environment:
  See "Preparing to upgrade for a DMP environment" on page 159.
- Preparing the VCS cluster for upgrade:
  See "Preparing the VCS cluster for upgrade" on page 161.
- Upgrading to SFW HA 5.1 SP1:
  See "Upgrading to SFW HA 5.1 SP1" on page 165.
- Post-upgrade tasks:
  See "About tasks after the SFW HA 5.1 SP1 upgrade" on page 235.

Preparing VVR in a VCS environment for upgrade

If you use VVR in a VCS environment to replicate data from a primary site to a secondary site, then follow the appropriate set of procedures below for your configuration:

- Upgrade from SFW HA 4.3.x to SFW HA 5.1 SP1:
  See "Preparing VVR for upgrade from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1" on page 152.
- Upgrade from SFW HA 5.0.x or 5.1.x to SFW HA 5.1 SP1:
  See "Preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x versions to SFW HA 5.1 SP1" on page 156.

Preparing VVR for upgrade from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1

Follow the procedures in the given order while upgrading from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

To prepare the primary site

1. Take the application service group offline on the primary site, by performing one of the following procedures:
   - From the Cluster Manager (Java Console), right-click the application service group and select the **Offline** menu option.
   - From the command line, type:

     ```
     hagrp -offline group_name -sys system_name
     ```

2. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and select the **Offline** option.
   - From the command line, type:

     ```
     hares -offline resource_name -sys system_name
     ```

3. To get the list of RVG and RLINK records, type the following from the command line:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

4. Verify that the data on the Replicator Log is written to the secondary site by running the following command on the primary site.

   ```
   vxrlink [-g diskgroup_name] status rlink_to_secondary
   ```

   This command displays the replication status of the secondary represented by the specified RLINK. This command can be run only on the primary site. Verify that the data volumes on the secondary are consistent and up-to-date with the primary before proceeding to the next step.

5. Detach the RLINK to prevent VVR from replicating data to the secondary site, by performing one of the following procedures:
   - From the VEA console, right-click the secondary RVG and select the **Stop Replication** option to stop VVR from replicating to the secondary site. The Stop Replication option is available only when selecting the secondary RVG. When this operation is performed the connection between the primary and secondary RVG is broken.
   - From the command line, type:

     ```
     vxrlink [-g diskgroup_name] det rlink_name
     ```

     This command detaches the RLINK from the RVG.

6 Dissociate the Replicator Log volume from the RVG, by performing one of the following procedures:

- From the VEA console, right-click the Replicator Log volume and select the **Dissociate Replicator Log** option from the menu.
- From the command line, type:

```
vxrvg [-f] [-g diskgroup_name] [-r rvg_name] dis volume_name
```

This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary is completely up-to-date with the primary. Otherwise this option can cause data corruption.

---

7 Bring the Disk Group and IP resources offline in a VCS cluster setup, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and select the **Offline** option from the menu.
- From the command line, type:

```
hares -offline resource_name -sys system_name
```

Repeat the above step to offline the IP resource.

To prepare the secondary site

1 Take the RVG resource offline, by performing one of the following procedures:

- From the Cluster Manager console, right-click the RVG resource and select the **Offline** option.
- From the command line, type:

```
hares -offline resource_name -sys system_name
```

2 To get the list of RVG and RLINK records, type the following from the command line:

```
vxprint -lVP [-g diskgroup_name])
```

3 If you used the VEA console to stop replication on the primary site, then you need not perform this step on the secondary site. However, if you used the command line to detach the RLINK while preparing the primary site, then you must perform this action on the secondary site as well.

From the command line, type:

```
vxrlink [-g diskgroup_name] det rlink_name]
```

This command detaches an RLINK from the secondary RVG.

4 Dissociate the Replicator Log volume from the RVG, by performing one of the following procedures:

- From the VEA console, right-click the Replicator Log volume and select the **Dissociate Replicator Log** option from the menu that appears.

This option is available for selection only if the Replicator Log is associated with an RVG.

- From the command line, type:

```
vxrvg [-f] [-g diskgroup_name] [-r rvg_name] dis volume_name
```

This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary site is completely up-to-date with the primary. Otherwise this option can cause data corruption.

---

5 Offline the Disk Group and IP resources in a VCS cluster setup, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and select the **Offline** option from the context-menu that appears.
- From the command line, type:

```
hares -offline resource_name -sys system_name
```

Repeat the above step to offline the IP resource.

Preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x versions to SFW HA 5.1 SP1

Since VVR 5.0.x and VVR 5.1 versions are interoperable, you can keep the applications running on the primary site while upgrading the secondary site.

Table 7-1 displays the tasks and their recommended sequence for this process.

Table 7-1 Preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x versions to SFW HA 5.1 SP1

Step	Description
1	Prepare VVR on the secondary (DR) site to upgrade from SFW HA 5.0.x or 5.1.x to 5.1 SP1: See "Preparing VVR on the secondary (DR) site for upgrade" on page 157.
2	Prepare the VCS cluster on the secondary site for upgrade: See "Preparing the VCS cluster for upgrade" on page 161.
3	Upgrade the cluster nodes on the secondary site to SFW HA 5.1: See "Upgrading to SFW HA 5.1 SP1" on page 165.
4	Re-enable VVR on the upgraded secondary site: See "Re-enabling VVR after upgrading to SFW HA 5.1 SP1" on page 246.
5	Once the secondary (DR) site has been upgraded, prepare the primary site for upgrade. The procedure includes migrating the primary role to the DR site: See "Preparing the primary site for upgrade" on page 158.
6	Prepare the VCS cluster on the old primary site (now the secondary site) for upgrade: See "Preparing the VCS cluster for upgrade" on page 161.
7	Upgrade the nodes on the old primary site to SFW HA 5.1 SP1: See "Upgrading to SFW HA 5.1 SP1" on page 165.
8	Re-enable VVR on the upgraded site. The topic includes a procedure for migrating the applications back to the original primary site: See "Re-enabling VVR after upgrading to SFW HA 5.1 SP1" on page 246.

Preparing VVR on the secondary (DR) site for upgrade

When preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x to 5.1 SP1, you begin by preparing the secondary site.

To prepare the secondary (DR) site

1. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and click **Offline**.
   - From the command line, type the following command:

     ```
     hares -offline resource_name -sys system_name
     ```

2. If the existing replication settings are configured to use TCP, change the settings to use UDP.

   After both the primary and DR sites are upgraded to 5.1 SP1, you can switch the replication settings back to TCP.

3. Offline the Disk Group and IP resources, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the Disk Group resource and click **Offline**.
   - From the command line, type the following command:

     ```
     hares -offline resource_name -sys system_name
     ```

     Repeat the above step to offline the IP resource.

Warning: Taking the DG (Disk Group) resource offline will pause replication, and if applications continue to run on the primary for too long, this may cause a possible replicator log overflow.

After you have completed these secondary (DR) site preparation steps, continue with the VVR upgrade preparation steps in sequence as described in Table 7-1.

These steps include:

- Preparing the VCS cluster on the secondary site for upgrade.
- Upgrading the secondary site nodes to SFW HA 5.1 SP1
- Re-enabling VVR on the secondary site
- Preparing the primary site for upgrade

Preparing the primary site for upgrade

This section discusses preparing the primary site for upgrade.

After upgrading the secondary (DR) site to SFW HA 5.1 SP1 and re-enabling VVR on that site, you prepare the primary site for upgrade. The procedure steps first use the remote switch operation to migrate the applications to the current secondary site, thus switching the roles so that the primary site becomes the secondary.

You then prepare VVR for upgrade.

To prepare the primary site

1. In the Service Groups tab of the Cluster Manager, right-click the application service group that is online at the primary site.
2. Click **Switch To**, and click **Remote switch**.
3. In the Switch global group dialog box, click the cluster of the secondary site to switch the group.
4. Click the specific system where you want to bring the global application service group online, and then click **OK**.
5. If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on the options available in your environment, these tasks may include mounting the databases or manually starting the application.

   Once the applications are online, the sites have now switched roles, so that the former secondary site is now the primary site, and the old primary has the role of the secondary.

   Therefore, on the old primary (now the secondary) complete the following steps, which are the same as when preparing the original secondary site for the upgrade.
6. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and click **Offline**.
   - From the command line, type the following command:

     ```
     hares -offline resource_name -sys system_name
     ```
7. Offline the Disk Group and IP resources, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the Disk Group resource and click **Offline**.

- From the command line, type the following command:

  ```
  hares -offline resource_name -sys system_name
  ```

  Repeat the above step to offline the IP resource.

Warning: Taking the DG (Disk Group) resource offline will pause replication, and if applications continue to run on the primary for too long, this may cause a possible replicator log overflow.

After you have completed these primary site preparation steps, continue with the VVR upgrade preparation steps in sequence as described in Table 7-1.

These steps include:

- Preparing the cluster for upgrade
- Upgrading the cluster nodes to SFW HA 5.1 SP1
- Re-enabling VVR
- Migrating the applications back to the original primary site

Preparing to upgrade for a DMP environment

When preparing to upgrade for a DMP environment, perform one of the following procedures suitable to your environment:

- Prepare to add DMP DSMs to an upgraded environment:
  See "Preparing to add DMP DSMs to the upgraded environment " on page 159.
- Prepare your existing DMP DSM environment for upgrade:
  See " DMP DSM environment" on page 160.
- Prepare your existing DMP ASL environment for upgrade:
  See " DMP ASL environment " on page 160.

Preparing to add DMP DSMs to the upgraded environment

If you do not have DMP DSMs in your existing environment, but plan to add this feature while upgrading to SFW HA 5.1 SP1, add the HBA (host bus adapter) hardware before upgrading the SFW HA 5.1 SP1 software.

To determine the approved SFW HA hardware, refer to the Hardware Compliance List on the Symantec Support web site at:

http://entsupport.symantec.com/docs/302144

For more information on the hardware and software prerequisites for DMP DSM installation, see the following:

- Installing and uninstalling Veritas Dynamic Multi-pathing
- *Veritas Storage Foundation Administrator's Guide.*

Do not connect paths from the new HBA (host bus adapters) to the storage array before upgrading to SFW HA 5.1 SP1 and installing DMP. Select the DMP option in the Options screen while running the installer.

Preparing an existing DMP environment for upgrading

Previous DMP environments are either DMP DSM or DMP ASL. The preparations for upgrade are different for each.

DMP DSM environment

If you are preparing to upgrade an existing DMP DSM environment, it is recommended to physically disconnect all but one path of the multipath storage to shorten upgrade time.

No other DMP preparation is required except as follows.

In upgrading from 4.3.x, in the following cases only, you must uninstall DMP DSM before the upgrade (and reinstall it during the upgrade):

- SFW 4.3 with DMP option installed and no SFW 4.3 DDI-x has ever been applied
- SFW 4.3 DMP with DDI-1, DDI-3, DDI-4, DDI-5, or DDI-6 installed

Before uninstalling DMP DSM from a node in a cluster environment, the cluster resources should be moved to another node.

To uninstall the DMP or the DDI package

1. Make sure that only one path is attached for each array that is managed by DMP DSM.
2. Open the Windows Add/Remove Programs to uninstall the DDI. Select the Symantec support for DMP DSM entry and click **Remove** to begin the uninstallation.
3. Reboot the system after the uninstall process completes.

DMP ASL environment

DMP ASLs are no longer supported on SFW HA 5.1 SP1. Therefore, you must uninstall DMP ASLs before the upgrade to SFW HA 5.1 SP1.

It is important that you detach all but one path to the storage array before you uninstall.

Warning: Failure to limit DMP ASLs to a single path before uninstalling can lead to data corruption.

Warning: Always back up your data before upgrading.

To prepare an existing DMP ASL environment for upgrade

1. Physically remove all but one path from each multiple-path array.
2. In the VEA, exclude each multiple-path array from DMP ASLs management.
3. Display the Array Settings screen for the array you are excluding.
4. In the tree view under the Disks folder, select a disk from the storage array that you are excluding.
5. In the right pane, click the Paths tab for the disk.
6. Right-click a path and select Array Settings from the path context menu that appears.
7. In the Array Settings screen, check the **Exclude** check box.
8. Click **OK**. The array is now excluded from DMP control.
9. Select **Actions > Rescan** from the VEA menu bar. Veritas Storage Foundation for Windows rescans the array and updates the display.
10. Uninstall the DMP ASLs using the Add or Remove function through the installer.

    See "Adding or removing features" on page 82.
11. After the uninstall process is complete, reboot the system.
12. If you want to install DMP DSMs during the upgrade, review the following information for more information on prerequisites for DMP DSMs:
    - Installing and uninstalling Veritas Dynamic Multi-pathing
    - *Veritas Storage Foundation Administrator's Guide.*

Preparing the VCS cluster for upgrade

This section covers the procedures to prepare the VCS cluster for the upgrade.

If your configuration uses a VCS cluster, then follow the procedures in this section to prepare the VCS cluster for upgrade:

- Removing VCS Management Console 5.1:
  See "Removing VCS Management Console 5.1" on page 162.
- Saving and closing the cluster configuration:
  See "Saving and closing the cluster configuration" on page 162.
- Taking the service groups offline:
  See "Taking the service groups offline" on page 163.
- Closing SFW HA clients:
  See "Closing SFW HA clients" on page 163.
- Stopping VCS services:
  See "Stopping VCS services" on page 163.
- Backing up customized type definitions:
  See "Backing up customized type definitions" on page 165.

Removing VCS Management Console 5.1

If one or more nodes in the VCS cluster have Veritas Cluster Server Management Console 5.1 installed, you must remove the management console before upgrading SFW HA. You can reinstall the management console after the upgrade.

See "Reinstalling VCS Management Console 5.1" on page 237.

To remove VCS Management Console 5.1

1. Stop the VCS Management Console. If the management console is clustered, take the CMC_MS service group offline.
2. Back up the console's data directory and datadir.conf files. Typically, the files are located at one of the following paths:
   - `C:\Program Files\Symantec\VRTScmcm`
   - `C:\Program Files (x86)\Symantec\VRTScmcm`
3. Remove VCS Management Console 5.1 from all nodes in the cluster using the Windows Add/Remove Programs.

Saving and closing the cluster configuration

Before starting the upgrade process, use the VCS Java Console to "save and close" the VCS configuration. This operation involves saving the latest configuration to disk and changing the configuration state to read-only mode. You must also stop VCS before attempting the upgrade process.

In a VVR environment, perform the following procedure on both the VVR primary and secondary clusters.

To save and close the cluster configuration

- Perform one of the following tasks:
  - From the VCS Java Console, click **Save and Close Configuration** on the Cluster Explorer toolbar.
  - From the command prompt, type the following command.
    C:\>`haconf -dump -makero`

Taking the service groups offline

Take all service groups offline before the upgrade.

To take the service groups offline

1. From the command prompt, type:

   ```
   C:\>hagrp -offline group_name -sys system_name
   ```

   where *group_name* is the name of the service group and *system_name* is the node on which the group is online.
2. Repeat this command for all service groups that are online.

Closing SFW HA clients

Exit all instances of the Veritas Enterprise Administrator (VEA), Cluster Manager (Java Console), and Cluster Management Console (Single Cluster Mode) before the upgrade.

To close SFW HA clients

1. From the VEA, click **File > Exit** and then click **Yes** on the confirmation dialog box.
2. From the Cluster Manager (Java Console), click **File > Logout** on the Cluster Explorer window and then click **File > Exit** on the Cluster Monitor window.
3. If CMC was not uninstalled in the earlier procedure and resides on a server outside of the VCS cluster, click **Logout** on the title bar of the Cluster Management Console.

Stopping VCS services

Stop the VCS services before the upgrade.

To stop VCS services

1. Stop HAD on all the cluster nodes. Type the following on the command prompt:

   ```
   C:\>hastop -all -force
   ```

2. Stop the Veritas VCSComm Startup service on all the cluster nodes. Type the following on the command prompt:

   ```
   C:\>net stop vcscomm
   ```

3. Stop the Veritas Command Server service on all the cluster nodes. Type the following on the command prompt:

   ```
   C:\>net stop cmdserver
   ```

4. Stop GAB and LLT on all the cluster nodes. Type the following on the command prompt:

   ```
   C:\>net stop gab
   C:\>net stop llt
   ```

5. Stop the Veritas Enterprise Administrator Service on all the cluster nodes. Type the following on the command prompt:

   ```
   C:\>net stop vxob
   ```

6. If the Windows Indexing Service is installed, then type the following on the command prompt to stop this service:

   ```
   C:\>net stop cisvc
   ```

7. If upgrading from SFW HA 5.0.x, stop the Symantec Private Branch Exchange service, Veritas Storage Agent, Veritas GridNode, and the Veritas Action Agent services on all the cluster nodes.

   Type the following commands on the command prompt:

   ```
   C:\>net stop VRTSpbx
   C:\>net stop vxvm
   C:\>net stop vxgn
   C:\>net stop actionagent
   ```

Backing up customized type definitions

The cluster type definitions are reset to their default values after the upgrade. If you have modified the values of type definitions in the cluster, make a backup copy of the `types.cf` file before the upgrade. The `types.cf` file is typically located at `%VCS_HOME%\conf\config`.

The variable `%VCS_HOME%` is the default installation directory for VCS, typically `C:\Program Files\VERITAS\Cluster Server`.

After you complete the upgrade, refer to the backup copy of the `types.cf` file and use the Cluster Manager (Java Console) to change the type definition default values with the values you had originally set in the cluster.

Note: After the upgrade, do not replace the `types.cf` file with the backup copy. Use the backup copy only as a reference for the customized type definition values in the cluster.

Upgrading to SFW HA 5.1 SP1

This section describes the upgrade procedures from SFW HA 4.3 MP2, 5.0.x, or 5.1.x to SFW HA 5.1 SP1 using the product installer. For information about supported minimum product versions:

See "Checking the supported minimum product versions" on page 96.

Note: If the cluster has VCS enterprise agents and options, make sure to select the same enterprise agents and options while upgrading to SFW HA 5.1 SP1. If you do not want to include the enterprise agents and options in the upgraded cluster, uninstall the agents from the cluster before proceeding.

This procedure consists of the following tasks:

- Changing the driver signing options:
  See "Changing driver signing options" on page 166.
- Upgrading to SFW HA 5.1 SP1 using the product installer:
  See "Upgrading using the product installer" on page 166.
- Configuring VxSAS service (if applicable to your configuration):
  See "Configuring the VxSAS service (VVR only)" on page 173.
- Resetting the driver signing options:
  See "Resetting the driver signing options" on page 173.

Changing driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

For information on how to change the driver signing options on each system:

See "Changing the driver signing options" on page 98.

Upgrading using the product installer

Follow the appropriate product installer procedures for your upgrade:

- Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 (Major Upgrade) using the product installer:
  See "Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer" on page 166.
- Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 (Minor Upgrade) using the product installer:
  See "Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer" on page 170.

Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer

The following procedure describes how to upgrade from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer. This procedure is called a Major Upgrade.

To upgrade from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer

1. Insert the DVD containing the Major Upgrade software into your system's disc drive or download the Major Upgrade software from the Symantec website.
2. Allow the autorun feature to start the upgrade or double-click **Setup.exe.**

   The Select Product screen appears.

3 Review the links on the Select Product screen. Links on this screen access Late Breaking News, the Configuration Checker, as well begin the process to install Storage Foundation 5.1 SP1 for Windows or Storage Foundation HA 5.1 SP1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide, Installation and Upgrade Guide, and Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Storage Foundation HA SP1 5.1 for Windows**.

5 Click **Complete/Custom** to begin installation. The **Administrative Console** link lets you install only the Client components.

6 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

7 Read the License Agreement by using the scroll arrows in the view window.If you agree to the terms of the license agreement, click **I AGREE TO the terms of the license agreement**, and then click **Next**.

8 Enter the license key for each Symantec product option that you are upgrading or installing in the top field.

9 To add a key, click **Add**.

To remove a key, click the key to select it, and click **Remove**.

10 Repeat step 8 and step 9 for each Symantec product and feature that you want to install. Click a key to see its details.

11 Click **Next**.

12 Select the appropriate Storage Foundation HA options and click **Next**.

If any previous VCS agents and options are installed on the node, make sure you select the same agents and options while upgrading. If you do not want to include the agents and options in the upgraded cluster, uninstall them from the cluster before proceeding.

When upgrading multiple computers in a single installation using the product installer, all selected options for the multiple computers should be the same. This is only an issue if you are trying to upgrade on more than one computer at once, and these computers have different options installed. However, if a superset of options is selected for the computers during the upgrade, then the upgrade proceeds as normal and all selected options (superset of options) will be installed on all the computers.

13 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows Server 2003 and Windows Server 2008.
Install Path	The install path cannot be changed for the upgrade.

14 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

15 Depending upon your earlier product installer selections and operating system, you may receive one or more of the following messages.

If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning stating the following:	The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system. If you are upgrading in a cluster environment, you must configure the Veritas Scheduler Service on all nodes to allow the automatic transfer of Capacity Monitoring and Automatic Volume Growth settings. Refer to the Capacity Monitoring and Automatic Volume Growth sections of the SFW Administrator's Guide for more information. If applicable to your installation, perform the above procedures.
On a Windows Server 2008 machine, you receive an additional warning:	On Windows Server 2008, the Microsoft Multipath input/output (Microsoft MPIO) feature must be enabled before installing DMP Device Specific Modules (DSMs). If applicable to your installation, perform the above procedure.

Click **OK**.

16 Review the pre-upgrade summary. Click **Back** to make changes if necessary. Click **Install**.

17 If the installation is successful on all nodes, the installer automatically proceeds to the summary page.

Click **Next** after the progress indicator shows the installation is complete to proceed to the summary report to review the details of the failed installation.

Note: If a security alert asks you to accept the Symantec driver software, click **Yes**.

---

18 Review the installation report, taking action where necessary, and click **Next**.

19 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Select the upgraded remote computers and click **Reboot**.

Wait for the remote computer to come back online. Click **Next**.

20 Click **Finish**.

21 Click **Yes** to reboot the local node.

Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer

The following procedure describes how to upgrade from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer. This procedure is called a Minor Upgrade.

Note: When upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1, the product installer replaces the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator (VEA) GUI for Windows Server 2008. To change this default, access the VEA GUI after the upgrade completes and proceed to restore the Disk Management Snap-in. For information about using the VEA GUI, see *Veritas Storage Foundation™ Administrator's Guide*.

To upgrade from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer

1 Insert the DVD containing the Minor Upgrade software into your system's disc drive or download the Minor Upgrade software from the Symantec website.

2 Allow the autorun feature to start the upgrade or double-click **Setup.exe**.

The Select Product screen appears.

3 Review the links on the Select Product screen.

There are links on this screen to access Late Breaking News, Configuration Checker, and to begin the process to install Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide and the Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Service Pack 1 for SFW 5.1, SFWHA 5.1, and VCS 5.1 for Windows**

5 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

6 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows Server 2003 and Windows Server 2008.
Install Path	The install path cannot be changed for the upgrade.

7 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

8 If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning stating the following:

- The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system.
  If you are upgrading in a cluster environment, you must configure the Veritas Scheduler Service on all nodes to allow the automatic transfer of Capacity Monitoring and Automatic Volume Growth settings. Refer to the Capacity Monitoring and Automatic Volume Growth sections of the SFW Administrator's Guide for more information.

If applicable to your installation, perform the above procedures.

Click **OK**.

9 Review the pre-upgrade summary. Click **Back** to make changes if necessary. Click **Install**.

10 If the installation is successful on all nodes, the installer automatically proceeds to the summary page.

   Click **Next** after the progress indicator shows the installation is complete to proceed to the summary report to review the details of the failed installation. Note that if a security alert asks you to accept the Symantec driver software, click **Yes**.

11 Review the installation report, taking action where necessary, and click **Next**.

12 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Select the upgraded remote computers and click **Reboot**.

   Wait for the remote computer to come back online. Click **Next**.

13 Click **Finish**.

14 Click **Yes** to reboot the local node.

Configuring the VxSAS service (VVR only)

If you upgraded or installed the Volume Replicator (VVR) option, you can launch the wizard for Veritas Volume Replicator Security Service (VxSAS) after the reboot to configure security services for all nodes. This step is required for VVR if you are upgrading from the SFW HA 4.3 MP2 version.

If you are upgrading from SFW HA 5.0.x or 5.1.x versions to 5.1 SP1 and VxSAS was already configured for 5.0.x or 5.1.x, you do not need to configure it again.

Resetting the driver signing options

After completing the installation sequence, reset the drive signing options on each computer.

Resetting the driver signing option procedure

1 Open the Control Panel, and click **System**.

2 Click the **Hardware** tab and click **Driver Signing**.

3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat this procedure for each computer.

Performing tasks required after the upgrade

Perform the tasks required for your configuration after the SFW HA 5.1 SP1 upgrade.

For information about the tasks required after an upgrade:

See “About tasks after the SFW HA 5.1 SP1 upgrade” on page 235.

Chapter 8

Upgrading an Exchange Server cluster

This chapter includes the following topics:

About upgrading an Exchange Server cluster

Table 8-1 presents possible scenarios for upgrading from SFW HA versions 4.3 MP2, 5.0.x, and 5.1.x to an SFW HA 5.1 SP1 cluster running Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007.

If upgrading Exchange 2007 to Exchange 2007 SP1, upgrade SFW HA first and then upgrade Exchange. For information about service pack upgrades:

See "Upgrading the Microsoft Exchange Service Pack" on page 253.

For the latest information on supported software, see the Software Compatibility list at:

http://entsupport.symantec.com/docs/302145

Table 8-1 Exchange Server cluster upgrade

Upgrade from this configuration ...	To this configuration ...
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, and 5.1 ■ Windows Server 2003 SP1 ■ Exchange 2003 SP2	■ SFW HA 5.1 SP1 ■ Windows Server 2003 SP2 ■ Exchange 2003 SP2
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, and 5.1 ■ Windows Server 2003 R2 ■ Exchange 2003 SP2	■ SFW HA 5.1 SP1 ■ Windows Server 2003 R2 SP2 ■ Exchange 2003 SP2
■ SFW HA 5.0 RP2 and 5.1 ■ Windows Server 2003 (x64) ■ Exchange 2007 (only x64)	■ SFW HA 5.1 SP1 ■ Windows Server 2003 (x64) ■ Exchange 2007 (only x64)
■ SFW HA 5.1 ■ Windows Server 2008 (x64) ■ Exchange 2007 (only x64)	■ SFW HA 5.1 SP1 ■ Windows Server 2008 (x64) ■ Exchange 2007 (only x64)

Overview of tasks

Upgrading an Exchange configuration in a VCS cluster requires you to upgrade the VCS Application Agent for Microsoft Exchange from version 4.3x or 5.0.x to version 5.1. To do this, you must upgrade to SFW HA 5.1.

Upgrading Microsoft Exchange Server in a VCS cluster involves pre-upgrade, Microsoft Exchange Server upgrade, and post-upgrade tasks.

Note: After you have upgraded Microsoft Exchange in the VCS cluster, make sure that all failover nodes for an Exchange virtual server have the same version of Microsoft Exchange. All failover nodes must also have the same enterprise agent version.

Table 8-2 displays the steps required to upgrade to an SFW HA 5.1 SP1 cluster with Microsoft Exchange.

Table 8-2 Upgrade to an SFW HA 5.1 SP1 cluster with Microsoft Exchange

Step	Description
1	Prepare to upgrade to SFW HA 5.1 SP1 by reviewing the general upgrade preparations and stopping VCS services: See "About preparing for upgrade" on page 95.
2	Prepare to upgrade VVR for SFW HA 5.1 SP1: See "Preparing VVR in a VCS environment for upgrading" on page 177. **Note:** This step is optional, depending upon your current configuration. If you have previously installed and configured VVR, you must take additional steps before and after the upgrade.
3	Prepare to upgrade in a DMP environment: See "Preparing to upgrade for a DMP environment" on page 185. **Note:** This step is optional, depending upon your current configuration.
4	Prepare the VCS cluster for upgrade: See "Preparing the VCS cluster for upgrade" on page 187.
5	Upgrade VCS and the VCS application for Exchange from 4.x to version 5.1 by upgrading to SFW HA 5.1 SP1: See "Upgrading to SFW HA 5.1 SP1" on page 191.
6	Reset the driver signing options: See "Resetting the driver signing options" on page 199.
7	Assign VEA administrative privileges: See "Assigning VEA administrative privileges" on page 199.
8	Perform additional post-upgrade tasks as required depending upon your VCS cluster configuration: See "About tasks after the SFW HA 5.1 SP1 upgrade" on page 235.
9	If appropriate to your configuration, upgrade the Microsoft Exchange Server service pack: See "Upgrading the Microsoft Exchange Service Pack" on page 253.

Preparing VVR in a VCS environment for upgrading

If you use VVR in a VCS environment to replicate data from a primary site to a secondary site, then follow the appropriate set of procedures below:

- Upgrade from SFW HA 4.3 MP2 to SFW HA 5.1 SP1:
  See "Preparing VVR for upgrade from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1" on page 178.
- Upgrade from SFW HA 5.0.x or 5.1.x to SFW HA 5.1 SP1:
  See "Preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x versions to SFW HA 5.1 SP1" on page 181.

Preparing VVR for upgrade from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1

Follow the procedures in the given order while upgrading from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

To prepare the primary site

1. Take the application service group offline on the primary site, by performing one of the following procedures:
   - From the Cluster Manager (Java Console), right-click the application service group and select the **Offline** menu option.
   - From the command line, type:

     ```
     hagrp -offline group_name -sys system_name
     ```

2. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and select the **Offline** option.
   - From the command line, type:

     ```
     hares -offline resource_name -sys system_name
     ```

3. To get the list of RVG and RLINK records, type the following from the command line:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

4 Verify that the data on the Replicator Log is written to the secondary site by running the following command on the primary site:

```
vxrlink [-g diskgroup_name] status rlink_to_secondary
```

This command displays the replication status of the secondary represented by the specified RLINK. This command can be run only on the primary site. Verify that the data volumes on the secondary are consistent and up-to-date with the primary before proceeding to the next step.

5 Detach the RLINK to prevent VVR from replicating data to the secondary site, by performing one of the following procedures:

- From the VEA console, right-click the secondary RVG and select the **Stop Replication** option to stop VVR from replicating to the secondary site. The Stop Replication option is available only when selecting the secondary RVG. When this operation is performed the connection between the primary and secondary RVG is broken.
- From the command line, type:

  ```
  vxrlink [-g diskgroup_name] det rlink_name
  ```

  This command detaches the RLINK from the RVG.

6 Dissociate the Replicator Log volume from the RVG, by performing one of the following procedures:

- From the VEA console, right-click the Replicator Log volume and select the **Dissociate Replicator Log** option from the menu.
- From the command line, type:

  ```
  vxrvg [-f] [-g diskgroup_name] [-r rvg_name] dis volume_name
  ```

This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary is completely up-to-date with the primary. Otherwise this option can cause data corruption.

---

7 Bring the Disk Group and IP resources offline in a VCS cluster setup, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and select the **Offline** option from the menu.

- From the command line, type:

  ```
  hares -offline resource_name -sys system_name
  ```

Repeat the above step to offline the IP resource.

To prepare the secondary site

1. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and select the **Offline** option.
   - From the command line, type:

     ```
     hares -offline resource_name -sys system_name
     ```

2. To get the list of RVG and RLINK records, type the following from the command line:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

3. If you used the VEA console to stop replication on the primary site, then you need not perform this step on the secondary site. However, if you used the command line to detach the RLINK while preparing the primary site, then you must perform this action on the secondary site as well. From the command line, type:

   ```
   vxrlink [-g diskgroup_name] det rlink_name]
   ```

   This command detaches an RLINK from the secondary RVG.

4. Dissociate the Replicator Log volume from the RVG, by performing one of the following procedures:
   - From the VEA console, right-click the Replicator Log volume and select the Dissociate Replicator Log option from the menu that appears.
     This option is available for selection only if the Replicator Log is associated with an RVG.
   - From the command line, type:

     ```
     vxrvg [-f] [-g diskgroup_name] [-r rvg_name] dis volume_name
     ```

     This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary site is completely up-to-date with the primary. Otherwise this option can cause data corruption.

5 Offline the Disk Group and IP resources in a VCS cluster setup, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and select the **Offline** option from the context-menu that appears.
- From the command line, type:

  ```
  hares -offline resource_name -sys system_name
  ```

  Repeat the above step to offline the IP resource.

Preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x versions to SFW HA 5.1 SP1

Since VVR 5.0.x and VVR 5.1 versions are interoperable, you can keep the applications running on the primary site while upgrading the secondary site.

Table 8-3 displays the recommended steps for this process.

Table 8-3 Preparing VVR for upgrade from 5.0.x or 5.1.x versions to SFW HA 5.1 SP1 for an Exchange cluster

Step	Description
1	Prepare VVR on the secondary (DR) site to upgrade from SFW HA 5.0.x or 5.1.x to SFW HA 5.1 SP1: See "Preparing VVR on the secondary (DR) site for upgrade" on page 182.
2	Prepare the VCS cluster on the secondary site for upgrade: See "About preparing for upgrade" on page 95.
3	Upgrade the cluster nodes on the secondary site to SFW HA 5.1 SP1: See "Upgrading to SFW HA 5.1 SP1" on page 191.
4	Re-enable VVR on the upgraded secondary site: See "Re-enabling VVR after upgrading to SFW HA 5.1 SP1" on page 246.

Table 8-3 Preparing VVR for upgrade from 5.0.x or 5.1.x versions to SFW HA 5.1 SP1 for an Exchange cluster *(continued)*

Step	Description
5	Once the secondary (DR) site has been upgraded, prepare the primary site for upgrade: See "Preparing the primary site for upgrade" on page 183. **Note:** The procedure includes migrating the primary role to the DR site.
6	Prepare the VCS cluster on the old primary site (now the secondary site) for upgrade: See "About preparing for upgrade" on page 95.
7	Upgrade the nodes on the old primary site to SFW HA 5.1 SP1: See "Upgrading to SFW HA 5.1 SP1" on page 191.
8	Re-enable VVR on the upgraded site: See "Re-enabling VVR after upgrading to SFW HA 5.1 SP1" on page 246. This procedure includes migrating the applications back to the original primary site.

Preparing VVR on the secondary (DR) site for upgrade

When preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x to SFW HA 5.1 SP1, you begin by preparing the secondary site.

To prepare the secondary (DR) site for upgrade

1. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and click **Offline**.
   - From the command line, type the following command:

     ```
     hares -offline resource_name -sys system_name
     ```

2. If the existing replication settings are configured to use TCP, change the settings to use UDP.

   After both the primary and DR sites are upgraded to 5.1 SP1 you can switch the replication settings back to TCP.

3. Offline the Disk Group and IP resources, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and click **Offline**.
- From the command line, type the following command:

  ```
  hares -offline resource_name -sys system_name
  ```

  Repeat the above step to offline the IP resource.

Warning: Taking the DG (Disk Group) resource offline pauses replication, and if applications continue to run on the primary for too long, this may cause a possible replicator log overflow.

After you have completed these secondary (DR) site preparation steps, continue with the VVR upgrade preparation steps in sequence as described in Table 8-3.

These steps include:

- Prepare the VCS cluster on the secondary site for upgrade.
- Upgrade the secondary site nodes to SFW HA 5.1 SP1
- Re-enable VVR on the secondary site
- Prepare the primary site for upgrade

Preparing the primary site for upgrade

After upgrading the secondary (DR) site to SFW HA 5.1 SP1 and re-enabling VVR on that site, you prepare the primary site for upgrade. The procedure steps first use the remote switch operation to migrate the applications to the current secondary site, thus switching the roles so that the primary site becomes the secondary. You then prepare VVR for upgrade.

To prepare the primary site for upgrade

1. In the Service Groups tab of the Cluster Manager, right-click the application service group that is online at the primary site.
2. Click **Switch To**, and click **Remote** switch.
3. In the Switch global group dialog box, click the cluster of the secondary site to switch the group.
4. Click the specific system where you want to bring the global application service group online, and then click **OK**.

5 If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on the options available in your environment, these tasks may include mounting the databases or manually starting the application.

Once the applications are online, the sites have now switched roles, so that the former secondary site is now the primary site, and the old primary has the role of the secondary.

Therefore, on the old primary (now the secondary) complete the following steps, which are the same as when preparing the original secondary site for the upgrade.

6 Take the RVG resource offline, by performing one of the following procedures:

- From the Cluster Manager console, right-click the RVG resource and click **Offline**.
- From the command line, type the following command:

```
hares -offline resource_name -sys system_name
```

7 Offline the Disk Group and IP resources, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and click **Offline**.
- From the command line, type the following command:

```
hares -offline resource_name -sys system_name
```

Repeat the above step to offline the IP resource.

Warning: Taking the DG (Disk Group) resource offline pauses replication, and if applications continue to run on the primary for too long, this may cause a possible replicator log overflow.

After you have completed these primary site preparation steps, continue with the VVR upgrade preparation steps in sequence as described in Table 8-3.

These steps include:

- Preparing the cluster for upgrade
- Upgrading the cluster nodes to SFW HA 5.1 SP1
- Re-enabling VVR
- Migrating the applications back to the original primary site

Preparing to upgrade for a DMP environment

When preparing to upgrade for a DMP environment, perform one of the following procedures suitable to your environment:

- Prepare to add DMP DSMs to an upgraded environment:
  See "Preparing to add DMP DSMs to the upgraded environment" on page 185.
- Prepare your existing DMP DSM environment for upgrade:
  See "DMP DSM environment" on page 185.
- Prepare your existing DMP ASL environment for upgrade:
  See "DMP ASL environment" on page 186.

Preparing to add DMP DSMs to the upgraded environment

If you do not have DMP DSMs in your existing environment, but plan to add this feature while upgrading to SFW HA 5.1 SP1, add the HBA (host bus adapter) hardware before upgrading the SFW HA 5.1 SP1 software.

To determine the approved SFWHA hardware, refer to the Hardware Compliance List on the Symantec Support web site at:

http://entsupport.symantec.com/docs/302144

For more information on the hardware and software prerequisites for DMP DSM installation, see the following:

- Installing and uninstalling Veritas Dynamic Multi-pathing
- *Veritas Storage Foundation Administrator's Guide*

Do not connect paths from the new HBA to the storage array before upgrading to SFW HA 5.1 SP1 and installing DMP. Select the DMP option in the Options screen while running the installer.

Preparing an existing DMP environment for upgrading

Previous DMP environments are either DMP DSM or DMP ASL. The preparations for upgrade are different for each.

DMP DSM environment

If you are preparing to upgrade an existing DMP DSM environment, it is recommended to physically disconnect all but one path of the multipath storage to shorten upgrade time.

No other DMP preparation is required except as follows.

In upgrading from 4.3.x, in the following cases only, you must uninstall DMP DSM before the upgrade (and reinstall it during the upgrade):

- SFW 4.3 with DMP option installed and no SFW 4.3 DDI-x has ever been applied
- SFW 4.3 DMP with DDI-1, DDI-3, DDI-4, DDI-5, or DDI-6 installed

Before uninstalling DMP DSM from a node in a cluster environment, the cluster resources should be moved to another node.

To uninstall the DMP or the DDI package

1. Make sure that only one path is attached for each array managed by DMP DSM.
2. Open the Windows Add/Remove Programs to uninstall the DDI. Select the Symantec support for DMP DSM entry and click **Remove** to begin the uninstallation.
3. Reboot the system when the uninstall process completes.

DMP ASL environment

DMP ASLs are no longer supported on SFW HA 5.1 SP1. Therefore, you must uninstall DMP ASLs before the upgrade to SFW HA 5.1 SP1.

It is important that you detach all but one path to the storage array before you uninstall.

Warning: Failure to limit DMP ASLs to a single path before uninstalling can lead to data corruption.

Warning: Always back up your data before upgrading.

To prepare an existing DMP ASL environment for upgrade

1. Physically remove all but one path from each multiple-path array.
2. In the VEA, exclude each multiple-path array from DMP ASLs management.
3. Display the Array Settings screen for the array you are excluding.
4. In the tree view under the Disks folder, select a disk from the storage array that you are excluding.
5. In the right pane, click the Paths tab for the disk.
6. Right-click a path and select Array Settings from the path context menu that appears.

7 In the Array Settings screen, check the **Exclude** check box.

8 Click **OK**. The array is now excluded from DMP control.

9 Select **Actions**>**Rescan** from the VEA menu bar. Veritas Storage Foundation for Windows rescans the array and updates the display.

10 Uninstall the DMP ASLs using the Add or Remove function through the installer.

See "Adding or removing features" on page 82.

11 After the uninstall process is complete, reboot the system.

12 If you want to install DMP DSMs during the upgrade, review the following information for more information on prerequisites for DMP DSMs:

- See "Installing and uninstalling Veritas Dynamic Multi-pathing" on page 70.
- *Veritas Storage Foundation Administrator's Guide*

Preparing the VCS cluster for upgrade

This section covers the procedures to prepare the VCS cluster for the upgrade.

If your configuration uses a VCS cluster, then follow the procedures in this section to prepare the VCS cluster for upgrade:

- Removing VCS Management Console 5.1:
  See "Removing VCS Management Console 5.1" on page 188.
- Saving and closing the cluster configuration:
  See "Saving and closing the cluster configuration" on page 188.
- Taking the service groups offline:
  See "Taking the service groups offline" on page 188.
- Closing SFW HA clients:
  See "Closing SFW HA clients" on page 189.
- Stopping VCS services:
  See "Stopping VCS services" on page 189.
- Backing up customized type definitions:
  See "Backing up customized type definitions" on page 190.

Removing VCS Management Console 5.1

If one or more nodes in the VCS cluster have Veritas Cluster Server Management Console 5.1 installed, you must remove the management console before upgrading SFW HA. You can reinstall the management console after the upgrade.

See "Reinstalling VCS Management Console 5.1" on page 237.

To remove VCS Management Console 5.1

1. Stop the VCS Management Console. If the management console is clustered, take the CMC_MS service group offline.
2. Back up the console's data directory and datadir.conf files. Typically, the files are located at one of the following paths:
   - `C:\Program Files\Symantec\VRTScmcm`
   - `C:\Program Files (x86)\Symantec\VRTScmcm`
3. Remove VCS Management Console 5.1 from all nodes in the cluster using Windows Add/Remove Programs.

Saving and closing the cluster configuration

Before starting the upgrade process, use the VCS Java Console to "save and close" the VCS configuration. This operation involves saving the latest configuration to disk and changing the configuration state to read-only mode. You must also stop VCS before attempting the upgrade process.

In a VVR environment, perform these steps on both the VVR primary and secondary clusters.

To save and close the cluster configuration

- Perform one of the following tasks:
  - From the VCS Java Console, click **Save and Close Configuration** on the Cluster Explorer toolbar.
  - From the command prompt, type the following command.

    ```
    C:\>haconf -dump -makero
    ```

Taking the service groups offline

Take all service groups offline before the upgrade.

To take the service groups offline

1 From the command prompt, type:

```
C:\>hagrp -offline group_name -sys system_name
```

where group_name is the name of the service group and system_name is the node on which the group is online.

2 Repeat this command for all service groups that are online.

Closing SFW HA clients

Exit all instances of the Veritas Enterprise Administrator (VEA), Cluster Manager (Java Console), and Cluster Management Console (Single Cluster Mode) before the upgrade.

To close SFW HA clients

1 From the VEA, click **File**>**Exit** and then click **Yes** on the confirmation dialog box.

2 From the Cluster Manager (Java Console), click **File** > **Logout** on the Cluster Explorer window and then click **File** > **Exit** on the Cluster Monitor window.

3 If CMC was not uninstalled in the earlier procedure and resides on a server outside of the VCS cluster, then click **Logout** on the title bar of the Cluster Management Console.

Stopping VCS services

Stop the VCS services before the upgrade.

To stop VCS services

1 Stop HAD on all the cluster nodes. Type the following on the command prompt:

```
C:\>hastop -all -force
```

2 Stop the Veritas VCSComm Startup service on all the cluster nodes. Type the following on the command prompt:

```
C:\>net stop vcscomm
```

3 Stop the Veritas Command Server service on all the cluster nodes. Type the following on the command prompt:

```
C:\>net stop cmdserver
```

4 Stop GAB and LLT on all the cluster nodes. Type the following on the command prompt:

```
C:\>net stop gab
C:\>net stop llt
```

5 Stop the Veritas Enterprise Administrator Service on all the cluster nodes. Type the following on the command prompt:

```
C:\>net stop vxob
```

6 If the Windows Indexing Service is installed, then type the following on the command prompt to stop this service:

```
C:\>net stop cisvc
```

7 If upgrading from SFW HA 5.0.x, stop the Symantec Private Branch Exchange service, Veritas Storage Agent, Veritas Grid Node, and the Veritas Action Agent services on all the cluster nodes.

Type the following commands on the command prompt:

```
C:\>net stop VRTSpbx
C:\>net stop vxvm
C:\>net stop vxgn
C:\>net stop actionagent
```

Backing up customized type definitions

The cluster type definitions are reset to their default values after the upgrade. If you have modified the values of type definitions in the cluster, make a backup copy of the types.cf file before the upgrade.

The types.cf file is typically located at %VCS_HOME%\conf\config. The variable %VCS_HOME% is the default installation directory for VCS, typically C:\Program Files\VERITAS\Cluster Server.

After you complete the upgrade, refer to the backup copy of the types.cf file and use the Cluster Manager (Java Console) to change the type definition default values with the values you had originally set in the cluster.

Note: After the upgrade, do not replace the types.cf file with the backup copy. Use the backup copy only as a reference for the customized type definition values in the cluster.

Upgrading to SFW HA 5.1 SP1

This section describes the upgrade procedures from SFW HA 4.3 MP2, 5.0.x, or 5.1.x to SFW HA 5.1 SP1 using the product installer. For information about supported minimum product versions:

See "Checking the supported minimum product versions" on page 96.

Note: If the cluster has VCS enterprise agents and options, make sure to select the same enterprise agents and options while upgrading to SFW HA 5.1 SP1. If you do not want to include the enterprise agents and options in the upgraded cluster, uninstall the agents from the cluster before proceeding.

This procedure consists of the following tasks:

- Changing the driver signing options:
  See "Changing driver signing options" on page 191.
- Upgrading to SFW HA 5.1 SP1 using the product installer:
  See "Upgrade using the product installer" on page 191.
- Resetting the driver signing options:
  See "Resetting the driver signing options" on page 199.
- Assigning VEA administrative privileges:
  See "Assigning VEA administrative privileges" on page 199.

Changing driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

For information on how to change the driver signing options on each system:

See "Changing the driver signing options" on page 98.

Upgrade using the product installer

Follow the appropriate product installer procedures for your upgrade:

- Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 (Major Upgrade) using the product installer:
  See "Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer" on page 192.

- Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 (Minor Upgrade) using the product installer:
  See "Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer" on page 196.

Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer

The following procedure describes how to upgrade from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer. This procedure is called a Major Upgrade.

To upgrade from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer

1. Insert the DVD containing the Major Upgrade software into your system's disc drive or download the Major Upgrade software from the Symantec website.
2. Allow the autorun feature to start the upgrade or double-click **Setup.exe.**

   The Symantec product selection screen appears.

3 Review the links on the Select Product screen. Links on this screen access Late Breaking News, the Configuration Checker, as well begin the process to install Storage Foundation 5.1 SP1 for Windows or Storage Foundation HA 5.1 SP1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide, Installation and Upgrade Guide, and Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Storage Foundation HA 5.1 SP1 for Windows**.

5 Click **Complete/Custom** to begin installation. The **Administrative Console** link lets you install only the Client components.

6 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

7 Read the License Agreement by using the scroll arrows in the view window.If you agree to the terms of the license agreement, click **I AGREE TO the terms of the license agreement**, and then click **Next**.

8 Enter the license key for each Symantec product option that you are upgrading or installing in the top field.

9 To add a key, click **Add**.

To remove a key, click the key to select it, and click **Remove**.

10 Repeat the above license key steps for each Symantec product and feature that you want to install. Click a key to see its details.

11 Click **Next**.

12 Select the appropriate Storage Foundation HA options and click **Next**.

If any previous VCS agents and options are installed on the node, make sure you select the same agents and options while upgrading. If you do not want to include the agents and options in the upgraded cluster, uninstall them from the cluster before proceeding.

When upgrading multiple computers in a single installation using the product installer, all selected options for the multiple computers should be the same. This is only an issue if you are trying to upgrade on more than one computer at once, and these computers have different options installed. However, if a superset of options is selected for the computers during the upgrade, then the upgrade proceeds as normal and all selected options (superset of options) will be installed on all the computers.

13 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows Server 2003 and Windows Server 2008.
Install Path	The install path cannot be changed for the upgrade.

14 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

15 Depending upon your earlier product installer selections and operating system, you may receive one or more of the following messages.

If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning stating the following:	The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system. If you are upgrading in a cluster environment, you must configure the Veritas Scheduler Service on all nodes to allow the automatic transfer of Capacity Monitoring and Automatic Volume Growth settings. Refer to the Capacity Monitoring and Automatic Volume Growth sections of the SFW Administrator's Guide for more information. If applicable to your installation, perform the above procedures.
On a Windows Server 2008 machine, you receive an additional warning:	On Windows Server 2008, the Microsoft Multipath input/output (Microsoft MPIO) feature must be enabled before installing DMP Device Specific Modules (DSMs). If applicable to your installation, perform the above procedure.

Click **OK**.

16 Review the pre-upgrade summary. Click **Back** to make changes if necessary. Click **Install**.

17 If the installation is successful on all nodes, the installer automatically proceeds to the summary page.

Click **Next** after the progress indicator shows the installation is complete to proceed to the summary report to review the details of the failed installation.

Note: If a security alert asks you to accept the Symantec driver software, click **Yes**.

---

18 Review the installation report, taking action where necessary, and click **Next**.

19 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Select the upgraded remote computers and click **Reboot**.

Wait for the remote computer to come back online. Click **Next**.

20 Click **Finish**.

21 Click **Yes** to reboot the local node.

For an Exchange server cluster configuration, if you upgraded or installed the Volume Replicator (VVR) option, you can launch the wizard for Veritas Volume Replicator Security Service (VxSAS) after the reboot to configure security services for all nodes. This step is required for VVR if you are upgrading from the SFW HA 4.3 MP2 version. If you are upgrading from SFW HA 5.0.x or 5.1.x to 5.1 SP1 and VxSAS was already configured for 5.0.x or 5.1.x, you do not need to configure it again.

See "Configuring the VxSAS service (VVR only)" on page 131.

Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer

The following procedure describes how to upgrade from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer. This procedure is called a Minor Upgrade.

Note: When upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1, the product installer replaces the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator (VEA) GUI for Windows Server 2008. To change this default, access the VEA GUI after the upgrade completes and proceed to restore the Disk Management Snap-in. For information about using the VEA GUI, see *Veritas Storage Foundation™ Administrator's Guide*.

To upgrade from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer

1. Insert the DVD containing the Minor Upgrade software into your system's disc drive or download the Minor Upgrade software from the Symantec website.
2. Allow the autorun feature to start the upgrade or double-click **Setup.exe**.

   The Symantec product selection screen appears.
3. Review the links on the Select Product screen.

   There are links on this screen to access Late Breaking News, Configuration Checker, and to begin the process to install Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows.

   Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

   The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide and the Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4. Click **Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows**
5. Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

   Click **Next**.

6 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows Server 2003 and Windows Server 2008.
Install Path	The install path cannot be changed for the upgrade.

7 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

8 If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning stating the following:

- The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system.
  If you are upgrading in a cluster environment, you must configure the Veritas Scheduler Service on all nodes to allow the automatic transfer of Capacity Monitoring and Automatic Volume Growth settings. Refer to the Capacity Monitoring and Automatic Volume Growth sections of the SFW Administrator's Guide for more information.

If applicable to your installation, perform the above procedures.

Click **OK**.

9 Review the pre-upgrade summary. Click **Back** to make changes if necessary.

Click **Install**.

10 If the installation is successful on all nodes, the installer automatically proceeds to the summary page.

Click **Next** after the progress indicator shows the installation is complete to proceed to the summary report to review the details of the failed installation. Note that if a security alert asks you to accept the Symantec driver software, click **Yes**.

11 Review the installation report, taking action where necessary, and click **Next**.

12 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Select the upgraded remote computers and click **Reboot**.

Wait for the remote computer to come back online. Click **Next**.

13 Click **Finish**.

14 Click **Yes** to reboot the local node.

Resetting the driver signing options

After completing the installation sequence, reset the driver signing option (set before upgrade) on each computer running Windows 2003.

To reset the driver signing options

1 Open the Control Panel, and click **System**.

2 Click the **Hardware** tab and click **Driver Signing**.

3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat the procedure for each computer.

Assigning VEA administrative privileges

After the Exchange Server cluster upgrade is complete, to avoid permission issues, you must manually assign the VEA administrative privileges to the admin user and the Administrators group on each cluster node.

Perform the following steps on all the cluster nodes, one node at a time.

To assign the VEA administrative privileges

1. Take the Exchange service group offline or fail over to another node in the cluster.
2. On the node on which the Exchange service group is offline, type the following at the command prompt:

   ```
   veaconfig -c add_user -r Administrator -n
   Administrator@<EVS_Name>.<Domain_Name>.com.nt -o localhost
   ```

   Here, *<EVS_Name>* is the Exchange virtual server name.

   Ensure that the command is successful.
3. On the node on which the Exchange service group is offline, type the following at the command prompt:

   ```
   veaconfig -c add_user -r Administrator -n
   Administrators@<EVS_Name>.<Domain_Name>.com.nt -g -o localhost
   ```

   Ensure that the command is successful.

Performing tasks required after the upgrade

Perform the tasks required for your Microsoft Exchange cluster configuration after upgrading to SFW HA 5.1 SP1.

For information about the tasks required after an upgrade:

See "About tasks after the SFW HA 5.1 SP1 upgrade" on page 235.

Chapter 9

Upgrading a SQL Server cluster

This chapter includes the following topics:

About upgrading a SQL Server cluster

Table 9-1 presents possible scenarios for upgrading from SFW HA versions 4.3 MP2, 5.0, 5.0 RP1a, 5.0RP2, 5.1, and 5.1 AP1 to an SFW HA 5.1 SP1 cluster with SQL Server.

For the latest information on supported software, see the Software Compatibility list at:

http://entsupport.symantec.com/docs/302145

Table 9-1 Upgrade matrix for SQL Server cluster

Upgrade from this configuration ...	To this configuration ...
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, 5.1, and 5.1 AP1 ■ Windows Server 2003 SP1 ■ SQL Server 2005	■ SFW HA 5.1 SP1 ■ Windows Server 2003 SP2 ■ SQL Server 2005 SP2
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, 5.1, and 5.1 AP1 ■ Windows Server 2003 R2 ■ SQL Server 2000 SP4	■ SFW HA 5.1 SP1 ■ Windows Server 2003 R2 SP2 ■ SQL Server 2005 SP2
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, 5.1, and 5.1 AP1 ■ Windows Server 2003 SP1 ■ SQL Server 2005	■ SFW HA 5.1 SP1 ■ Windows Server 2003 R2 ■ SQL Server 2005 SP2
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, 5.1, and 5.1 AP1 ■ Windows Server 2003 R2 ■ SQL Server 2000 SP4	■ SFW HA 5.1 SP1 ■ Windows Server 2003 R2 ■ SQL Server 2005 SP2
■ SFW HA 5.1, and 5.1 AP1 ■ Windows Server 2008 ■ SQL Server 2005	■ SFW HA 5.1 SP1 ■ Windows Server 2008 ■ SQL Server 2005
■ SFW HA 5.1 and 5.1 AP1 ■ Windows Server 2008 ■ SQL Server 2008	■ SFW HA 5.1 SP1 ■ Windows Server 2008 ■ SQL Server 2008
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, 5.1, and 5.1 AP1 ■ Windows Server 2003 ■ SQL Server 2008	■ SFW HA 5.1 SP1 ■ Windows Server 2003 ■ Microsoft SQL Server 2008

Overview of tasks

Table 9-2 displays the steps required to upgrade to an SFW HA 5.1 SP1 cluster with Microsoft SQL Server.

If you plan to upgrade both Microsoft SQL Server and SFW HA, first upgrade Microsoft SQL Server, and then follow with the upgrade to SFW HA 5.1. For additional information:

- See "Upgrading from Microsoft SQL Server 2000 to SQL Server 2005" on page 226.
- See "Upgrading from Microsoft SQL Server 2000/2005 to Microsoft SQL Server 2008" on page 228.

Table 9-2 Upgrade to an SFW HA 5.1 SP1 cluster with SQL Server

Step	Description
1	Prepare to upgrade to SFW HA 5.1 SP1 by reviewing the general upgrade preparations and stopping VCS services: See "About preparing for upgrade" on page 95.
2	Prepare to upgrade VVR for SFW HA 5.1 SP1: See "Preparing VVR in a VCS environment for upgrade" on page 204. **Note:** This step is optional, depending upon your current configuration. If you have previously installed and configured VVR, you must take additional steps before and after the upgrade.
3	Prepare to upgrade in a DMP environment: See "Preparing to upgrade for a DMP environment" on page 211. **Note:** This step is optional, depending upon your current configuration.
4	Prepare the VCS cluster for upgrade: See "Preparing the VCS cluster for upgrade" on page 213.
5	Back up customized type definitions: See "Backing up customized type definitions" on page 216.
6	Upgrade to SFW HA 5.1 SP1: See "Upgrading to SFW HA 5.1 SP1" on page 217.
7	Reset the driver signing options: See "Resetting the driver signing options" on page 225.
8	Perform any additional post-upgrade tasks depending upon your configuration, after upgrading to SFW HA 5.1: See "About tasks after the SFW HA 5.1 SP1 upgrade" on page 235.
9	If appropriate to your configuration, upgrade the Microsoft SQL Server service pack: See "Upgrading the Microsoft SQL Service Pack" on page 258.

Preparing VVR in a VCS environment for upgrade

If you use VVR in a VCS environment to replicate data from a primary site to a secondary site, then follow the appropriate set of procedures below:

- Upgrade from SFW HA 4.3 MP2 to SFW HA 5.1 SP1:
  See "Preparing VVR for upgrade from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1" on page 204.
- Upgrade from SFW HA 5.0.x or 5.1.x to SFW HA 5.1 SP1:
  See "Preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x versions to SFW HA 5.1 SP1" on page 207.

Preparing VVR for upgrade from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1

Follow the procedures in the given order while upgrading from SFW HA 4.3 MP2 versions to SFW HA 5.1 SP1.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

To prepare the primary site

1. Take the application service group offline on the primary site, by performing one of the following procedures:
   - From the Cluster Manager (Java Console), right-click the application service group and select the **Offline** menu option.
   - From the command line, type:

     ```
     hagrp -offline group_name -sys system_name
     ```

2. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and select the **Offline** option.
   - From the command line, type:

     ```
     hares -offline resource_name -sys system_name
     ```

3. To get the list of RVG and RLINK records, type the following from the command line:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

4 Verify that the data on the Replicator Log is written to the secondary site by running the following command on the primary site.

```
vxrlink [-g diskgroup_name] status rlink_to_secondary
```

This command displays the replication status of the secondary represented by the specified RLINK. This command can be run only on the primary site. Verify that the data volumes on the secondary are consistent and up-to-date with the primary before proceeding to the next step

5 Detach the RLINK to prevent VVR from replicating data to the secondary site, by performing one of the following procedures:

- From the VEA console, right-click the secondary RVG and select the **Stop Replication** option to stop VVR from replicating to the secondary site. The Stop Replication option is available only when selecting the secondary RVG. When this operation is performed the connection between the primary and secondary RVG is broken.
- From the command line, type:

  ```
  vxrlink [-g diskgroup_name] det rlink_name
  ```

  This command detaches the RLINK from the RVG.

6 Dissociate the Replicator Log volume from the RVG, by performing one of the following procedures:

- From the VEA console, right-click the Replicator Log volume and select the **Dissociate Replicator Log** option from the menu.
- From the command line, type:

  ```
  vxrvg [-f] [-g diskgroup_name] [-r rvg_name] dis volume_name
  ```

  This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary is completely up-to-date with the primary. Otherwise this option can cause data corruption.

---

7 Bring the Disk Group and IP resources offline in a VCS cluster setup, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and select the **Offline** option from the menu.

- From the command line, type:

  ```
  hares -offline resource_name -sys system_name
  ```

  Repeat the above step to offline the IP resource.

To prepare the secondary site

1. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and select the **Offline** option.
   - From the command line, type:

     ```
     hares -offline resource_name -sys system_name
     ```

2. To get the list of RVG and RLINK records, type the following from the command line:

   ```
   vxprint -lVP [-g diskgroup_name]
   ```

3. If you used the VEA console to stop replication on the primary site, then you need not perform this step on the secondary site. However, if you used the command line to detach the RLINK while preparing the primary site, then you must perform this action on the secondary site as well.

   From the command line, type:

   ```
   vxrlink [-g diskgroup_name] det rlink_name]
   ```

   This command detaches an RLINK from the secondary RVG.

4. Dissociate the Replicator Log volume from the RVG, by performing one of the following procedures:
   - From the VEA console, right-click the Replicator Log volume and select the **Dissociate Replicator Log** option from the menu that appears. This option is available for selection only if the Replicator Log is associated with an RVG.
   - From the command line, type:

     ```
     vxrvg [-f] [-g diskgroup_name] [-r rvg_name] dis volume_name
     ```

     This command dissociates the specified Replicator Log from the RVG. If the -f option is used, it forcefully dissociates the volumes.

Warning: Use the -f option only when you are sure that the secondary site is completely up-to-date with the primary. Otherwise this option can cause data corruption.

5 Offline the Disk Group and IP resources in a VCS cluster setup, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and select the **Offline** option from the context-menu that appears.
- From the command line, type:

  ```
  hares -offline resource_name -sys system_name
  ```

  Repeat the above step to offline the IP resource.

Preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x versions to SFW HA 5.1 SP1

Since VVR 5.0.x and VVR 5.1 versions are interoperable, you can keep the applications running on the primary site while upgrading the secondary site.

Table 9-3 displays the recommended steps for this process.

Table 9-3 Preparing VVR for upgrade from 5.0.x or 5.1.x versions to SFW HA 5.1 SP1 for a SQL cluster

Step	Description
1	Prepare VVR on the secondary (DR) site to upgrade from SFW HA 5.0.x or 5.1.x to SFW HA 5.1 SP1: See "Preparing VVR on the secondary (DR) site for upgrade" on page 208.
2	Prepare the VCS cluster on the secondary site for upgrade: See "About preparing for upgrade" on page 95.
3	Upgrade the cluster nodes on the secondary site to SFW HA 5.1 SP1: See "Upgrading to SFW HA 5.1 SP1" on page 217.
4	Re-enable VVR on the upgraded secondary site: See "Re-enabling VVR after upgrading to SFW HA 5.1 SP1" on page 246.

Table 9-3 Preparing VVR for upgrade from 5.0.x or 5.1.x versions to SFW HA 5.1 SP1 for a SQL cluster *(continued)*

Step	Description
5	Once the secondary (DR) site has been upgraded, prepare the primary site for upgrade: See "Preparing the primary site for upgrade" on page 209. **Note:** This procedure includes migrating the primary role to the DR site.
6	Prepare the VCS cluster on the old primary site (now the secondary site) for upgrade: See "About preparing for upgrade" on page 95.
7	Upgrade the nodes on the old primary site to SFW HA 5.1 SP1: See "Upgrading to SFW HA 5.1 SP1" on page 217.
8	Re-enable VVR on the upgraded site: See "Re-enabling VVR after upgrading to SFW HA 5.1 SP1" on page 246. **Note:** This procedure includes migrating the applications back to the original primary site.

Preparing VVR on the secondary (DR) site for upgrade

When preparing VVR for upgrade from SFW HA 5.0.x or 5.1.x to SFW HA 5.1 SP1, you begin by preparing the secondary site.

To prepare the secondary (DR) site for upgrade

1. Take the RVG resource offline, by performing one of the following procedures:
   - From the Cluster Manager console, right-click the RVG resource and click **Offline**.
   - From the command line, type the following command:

     ```
     hares -offline resource_name -sys system_name
     ```

2. If the existing replication settings are configured to use TCP, change the settings to use UDP.

   After both the primary and DR sites are upgraded to 5.1 SP1, you can switch the replication settings back to TCP.

3. Offline the Disk Group and IP resources, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and click **Offline**.
- From the command line, type the following command:

  ```
  hares -offline resource_name -sys system_name
  ```

  Repeat the above step to offline the IP resource.

Warning: Taking the DG (Disk Group) resource offline pauses replication, and if applications continue to run on the primary for too long, this may cause a possible replicator log overflow.

After you have completed these secondary (DR) site preparation steps, continue with the VVR upgrade preparation steps in sequence as described in Table 9-3.

These steps include:

- Prepare the VCS cluster on the secondary site for upgrade.
- Upgrade the secondary site nodes to SFW HA 5.1 SP1
- Re-enable VVR on the secondary site
- Prepare the primary site for upgrade

Preparing the primary site for upgrade

After upgrading the secondary (DR) site to SFW HA 5.1 SP1 and re-enabling VVR on that site, you prepare the primary site for upgrade. The procedure steps first use the remote switch operation to migrate the applications to the current secondary site, thus switching the roles so that the primary site becomes the secondary. You then prepare VVR for upgrade.

To prepare the primary site for upgrade

1. In the Service Groups tab of the Cluster Manager, right-click the application service group that is online at the primary site.
2. Click **Switch To**, and click **Remote switch**.
3. In the Switch global group dialog box, click the cluster of the secondary site to switch the group.
4. Click the specific system where you want to bring the global application service group online. Then click **OK**.

5 If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on the options available in your environment, these tasks may include mounting the databases or manually starting the application.

Once the applications are online, the sites have now switched roles, so that the former secondary site is now the primary site, and the old primary has the role of the secondary.

Therefore, on the old primary (now the secondary) complete the following steps, which are the same as when preparing the original secondary site for the upgrade.

6 Take the RVG resource offline, by performing one of the following procedures:

- From the Cluster Manager console, right-click the RVG resource and click **Offline**.
- From the command line, type the following command:

```
hares -offline resource_name -sys system_name
```

7 Offline the Disk Group and IP resources, by performing one of the following procedures:

- From the Cluster Manager console, right-click the Disk Group resource and click **Offline**.
- From the command line, type the following command:

```
hares -offline resource_name -sys system_name
```

Repeat the above step to offline the IP resource.

Warning: Taking the DG (Disk Group) resource offline pauses replication, and if applications continue to run on the primary for too long, this may cause a possible replicator log overflow.

After you have completed these primary site preparation steps, continue with the VVR upgrade preparation steps in sequence as described in Table 9-3.

These steps include:

- Preparing the cluster for upgrade
- Upgrading the cluster nodes to SFW HA 5.1 SP1
- Re-enabling VVR
- Migrating the applications back to the original primary site

Preparing to upgrade for a DMP environment

When preparing to upgrade for a DMP environment, perform one of the following procedures suitable to your environment:

- Prepare to add DMP DSMs to the upgraded environment:
  See "Preparing to add DMP DSMs to the upgraded environment" on page 211.
- Prepare your existing DMP DSM environment for upgrade:
  See "DMP DSM environment" on page 211.
- Prepare your existing DMP ASL environment for upgrade:
  See "DMP ASL environment" on page 212.

Preparing to add DMP DSMs to the upgraded environment

If you do not have DMP DSMs in your existing environment, but plan to add this feature while upgrading to SFW HA 5.1 SP1, add the HBA (host bus adapter) hardware before upgrading the SFW HA 5.1 SP1 software.

To determine the approved SFWHA hardware, refer to the Hardware Compliance List on the Symantec Support web site at:

http://entsupport.symantec.com/docs/302144

For more information on the hardware and software prerequisites for DMP DSM installation, see the following:

- Installing and uninstalling Veritas Dynamic Multi-pathing
- *Veritas Storage Foundation Administrator's Guide*

Do not connect paths from the new HBA to the storage array before upgrading to SFW HA 5.1 SP1 and installing DMP. Select the DMP option in the Options screen while running the installer.

Preparing an existing DMP environment for upgrading

Previous DMP environments are either DMP DSM or DMP ASL. The preparations for upgrade are different for each.

DMP DSM environment

If you are preparing to upgrade an existing DMP DSM environment, it is recommended to physically disconnect all but one path of the multipath storage to shorten upgrade time.

No other DMP preparation is required except as follows.

In upgrading from 4.3.x, in the following cases only, you must uninstall DMP DSM before the upgrade (and reinstall it during the upgrade):

- SFW 4.3 with DMP option installed and no SFW4.3 DDI-x has ever been applied
- SFW 4.3 DMP with DDI-1, DDI-3, DDI-4, DDI-5, or DDI-6 installed

Before uninstalling DMP DSM from a node in a cluster environment, the cluster resources should be moved to another node.

To uninstall the DMP or the DDI package

1. Make sure that only one path is attached for each array managed by DMP DSM.
2. Open the Windows Add/Remove Programs to uninstall the DDI. Select the Symantec support for DMP DSM entry and click **Remove** to begin the uninstallation.
3. Reboot the system when the uninstall process completes.

DMP ASL environment

DMP ASLs are no longer supported on SFW HA 5.1 SP1. Therefore, you must uninstall DMP ASLs before the upgrade to SFW HA 5.1 SP1.

It is important that you detach all but one path to the storage array before you uninstall.

Warning: Failure to limit DMP ASLs to a single path before uninstalling can lead to data corruption.

Warning: Always back up your data before upgrading.

To prepare an existing DMP ASL environment for upgrade

1. Physically remove all but one path from each multiple-path array.
2. In the VEA, exclude each multiple-path array from DMP ASLs management.
3. Display the Array Settings screen for the array you are excluding.
4. In the tree view under the Disks folder, select a disk from the storage array that you are excluding.
5. In the right pane, click the Paths tab for the disk.
6. Right-click a path and select Array Settings from the path context menu that appears.

7 In the Array Settings screen, check the **Exclude** check box.

8 Click **OK**. The array is now excluded from DMP control.

9 Select **Actions**>**Rescan** from the VEA menu bar. Veritas Storage Foundation for Windows rescans the array and updates the display.

10 Uninstall the DMP ASLs using the Add or Remove function through the installer.

See "Adding or removing features" on page 82.

11 After the uninstall process is complete, reboot the system.

12 If you want to install DMP DSMs during the upgrade, review the following information for more information on prerequisites for DMP DSMs:

- to See "Installing and uninstalling Veritas Dynamic Multi-pathing" on page 70.
- *Veritas Storage Foundation Administrator's Guide*

Preparing the VCS cluster for upgrade

This section covers the procedures to prepare the VCS cluster for the upgrade.

If your configuration uses a VCS cluster, then follow the procedures in this section to prepare the VCS cluster for upgrade:

- Removing VCS Management Console 5.1:
  See "Removing VCS Management Console 5.1" on page 214.
- Saving and closing the cluster configuration:
  See "Saving and closing the cluster configuration" on page 214.
- Taking the service groups offline:
  See "Taking the service groups offline" on page 214.
- Closing SFW HA clients:
  See "Closing SFW HA clients" on page 215.
- Stopping VCS services:
  See "Stopping VCS services" on page 215.
- Backing up customized type definitions:
  See "Backing up customized type definitions" on page 216.

Removing VCS Management Console 5.1

If one or more nodes in the VCS cluster have Veritas Cluster Server Management Console 5.1 installed, you must remove the management console before upgrading SFW HA. You can reinstall the management console after the upgrade.

See "Reinstalling VCS Management Console 5.1" on page 237.

To remove VCS Management Console 5.1

1. Stop the VCS Management Console. If the management console is clustered, take the CMC_MS service group offline.
2. Back up the console's data directory and datadir.conf files. Typically, the files are located at one of the following paths:
   - `C:\Program Files\Symantec\VRTScmcm`
   - `C:\Program Files (x86)\Symantec\VRTScmcm`
3. Remove VCS Management Console 5.1 from all nodes in the cluster using Windows Add/Remove Programs.

Saving and closing the cluster configuration

Before starting the upgrade process, use the VCS Java Console to "save and close" the VCS configuration. This operation involves saving the latest configuration to disk and changing the configuration state to read-only mode. You must also stop VCS before attempting the upgrade process.

In a VVR environment, perform these steps on both the VVR primary and secondary clusters.

To save and close the cluster configuration

- Perform one of the following tasks:

  From the VCS Java Console, click **Save and Close Configuration** on the Cluster Explorer toolbar.

  From the command prompt, type the following command.

  ```
  C:\>haconf -dump -makero
  ```

Taking the service groups offline

Take all service groups offline before the upgrade.

To take the service groups offline

1 From the command prompt, type:

```
C:\>hagrp -offline group_name -sys system_name
```

where group_name is the name of the service group and system_name is the node on which the group is online.

2 Repeat this command for all service groups that are online.

Closing SFW HA clients

Exit all instances of the Veritas Enterprise Administrator (VEA), Cluster Manager (Java Console), and Cluster Management Console (Single Cluster Mode) before the upgrade.

To close SFW HA clients

1 From the VEA, click **File**>**Exit** and then click Yes on the confirmation dialog box.

2 From the Cluster Manager (Java Console), click **File** > **Logout** on the Cluster Explorer window and then click **File** > **Exit** on the Cluster Monitor window.

3 If CMC was not uninstalled in the earlier procedure and resides on a server outside of the VCS cluster, then click **Logout** on the title bar of the Cluster Management Console.

Stopping VCS services

Stop the VCS services before the upgrade.

To stop VCS services

1 Stop HAD on all the cluster nodes. Type the following on the command prompt:

```
C:\>hastop -all -force
```

2 Stop the Veritas VCSComm Startup service on all the cluster nodes. Type the following on the command prompt:

```
C:\>net stop vcscomm
```

3 Stop the Veritas Command Server service on all the cluster nodes. Type the following on the command prompt:

```
C:\>net stop cmdserver
```

4 Stop GAB and LLT on all the cluster nodes. Type the following on the command prompt:

```
C:\>net stop gab
C:\>net stop llt
```

5 Stop the Veritas Enterprise Administrator Service on all the cluster nodes. Type the following on the command prompt:

```
C:\>net stop vxob
```

6 If the Windows Indexing Service is installed, then type the following on the command prompt to stop this service:

```
C:\>net stop cisvc
```

7 If upgrading from SFW HA 5.0.x, stop the Symantec Private Branch Exchange service, Veritas Storage Agent, Veritas GridNode, and the Veritas Action Agent services on all the cluster nodes.

Type the following commands on the command prompt:

```
C:\>net stop VRTSpbx
C:\>net stop vxvm
C:\>net stop vxgn
C:\>net stop actionagent
```

Backing up customized type definitions

The cluster type definitions are reset to their default values after the upgrade. If you have modified the values of type definitions in the cluster, make a backup copy of the types.cf file before the upgrade.

The types.cf file is typically located at %VCS_HOME%\conf\config. The variable %VCS_HOME%is the default installation directory for VCS, typically C:\Program Files\VERITAS\Cluster Server.

After you complete the upgrade, refer to the backup copy of the types.cf file and use the Cluster Manager (Java Console) to change the type definition default values with the values you had originally set in the cluster.

Note: After the upgrade, do not replace the types.cf file with the backup copy. Use the backup copy only as a reference for the customized type definition values in the cluster.

Upgrading to SFW HA 5.1 SP1

This section describes the upgrade procedures from SFW HA 4.3 MP2, 5.0.x, or 5.1.x to SFW HA 5.1 SP1 using the product installer. For information about supported minimum product versions:

See "Checking the supported minimum product versions" on page 96.

Note: If the cluster has VCS enterprise agents and options, make sure to select the same enterprise agents and options while upgrading to SFW HA 5.1 SP1. If you do not want to include the enterprise agents and options in the upgraded cluster, uninstall the agents from the cluster before proceeding.

In a SQL configuration, You can upgrade SFW HA on servers in a Windows Server 2003 domain.

This procedure consists of the following tasks:

- Changing the driver signing options:
  See "Changing driver signing options" on page 217.
- Upgrading to SFW HA 5.1 SP1 using the product installer:
  See "Upgrading using the product installer" on page 217.
- Resetting the driver signing options:
  See "Resetting the driver signing options" on page 225.

Changing driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

For information on how to change the driver signing options on each system:

See "Changing the driver signing options" on page 98.

Upgrading using the product installer

Follow the appropriate product installer procedures for your upgrade:

- Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 (Major Upgrade) using the product installer:
  See "Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer" on page 218.

- Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 (Minor Upgrade) using the product installer:
  See "Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer" on page 222.

Upgrading from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer

The following section describes how to upgrade from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer. This procedure is called a Major Upgrade.

To upgrade from SFW HA 4.3 MP2 or 5.0.x to SFW HA 5.1 SP1 using the product installer

1. Insert the DVD containing the Major Upgrade software into your system's disc drive or download the Major Upgrade software from the Symantec website.
2. Allow the autorun feature to start the upgrade or double-click **Setup.exe**.

   The Select Product screen appears.

3 Review the links on the Select Product screen. Links on this screen access Late Breaking News, the Configuration Checker, as well begin the process to install Storage Foundation 5.1 SP1 for Windows or Storage Foundation HA 5.1 SP1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide, Installation and Upgrade Guide, and Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Storage Foundation HA 5.1 SP1 for Windows**.

5 Click **Complete/Custom** to begin installation. The **Administrative Console** link lets you install only the Client components.

6 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

7 Read the License Agreement by using the scroll arrows in the view window.If you agree to the terms of the license agreement, click **I AGREE TO the terms of the license agreement**, and then click **Next**.

8 Enter the license key for each Symantec product option that you are upgrading or installing in the top field.

9 To add a key, click **Add**.

To remove a key, click the key to select it, and click **Remove**.

10 Repeat the above license key steps for each Symantec product and feature that you want to install.

Click a key to see its details.

11 Click **Next**.

12 Select the appropriate Storage Foundation HA options and click **Next**.

If any previous VCS agents and options are installed on the node, make sure you select the same agents and options while upgrading. If you do not want to include the agents and options in the upgraded cluster, uninstall them from the cluster before proceeding.

When upgrading multiple computers in a single installation using the product installer, all selected options for the multiple computers should be the same. This is only an issue if you are trying to upgrade on more than one computer at once, and these computers have different options installed. However, if a superset of options is selected for the computers during the upgrade, then the upgrade proceeds as normal and all selected options (superset of options) will be installed on all the computers.

13 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows Server 2003 and Windows Server 2008.
Install path	The install path cannot be changed for the upgrade.

14 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

15 Depending upon your earlier product installer selections and operating system, you may receive one or more of the following messages.

If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning stating the following:	The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system. If you are upgrading in a cluster environment, you must configure the Veritas Scheduler Service on all nodes to allow the automatic transfer of Capacity Monitoring and Automatic Volume Growth settings. Refer to the Capacity Monitoring and Automatic Volume Growth sections of the SFW Administrator's Guide for more information. If applicable to your installation, perform the above procedures.
On a Windows Server 2008 machine, you receive an additional warning:	On Windows Server 2008, the Microsoft Multipath input/output (Microsoft MPIO) feature must be enabled before installing DMP Device Specific Modules (DSMs). If applicable to your installation, perform the above procedure.

Click **OK**.

16 Review the pre-upgrade summary.

Click **Back** to make changes if necessary. Click **Install**.

17 If the installation is successful on all nodes, the installer automatically proceeds to the summary page.

Click **Next** after the progress indicator shows the installation is complete to proceed to the summary report to review the details of the failed installation.

Note: If a security alert asks you to accept the Symantec driver software, click **Yes**.

---

18 Review the installation report, taking action where necessary, and click **Next**.

19 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Select the upgraded remote computers and click **Reboot**. Wait for the remote computer to come back online.

Click **Next**.

20 Click **Finish**.

21 Click **Yes** to reboot the local node.

Upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer

The following section describes how to upgrade from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer. This procedure is called a Minor Upgrade.

Note: When upgrading from SFW HA 5.1.x to SFW HA 5.1 SP1, the product installer replaces the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator (VEA) GUI for Windows Server 2008. To change this default, access the VEA GUI after the upgrade completes and proceed to restore the Disk Management Snap-in. For information about using the VEA GUI, see *Veritas Storage Foundation™ Administrator's Guide*.

To upgrade from SFW HA 5.1.x to SFW HA 5.1 SP1 using the product installer

1 Insert the DVD containing the Minor Upgrade software into your system's disc drive or download the Minor Upgrade software from the Symantec website.

2 Allow the autorun feature to start the upgrade or double-click **Setup.exe**.

The Select Product screen appears.

3 Review the links on the Select Product screen.

There are links on this screen to access Late Breaking News, Configuration Checker, and to begin the process to install Service Pack 1 for SFW 5.1, SFW HA 5.1, and VCS 5.1 for Windows.

Click on **Read Late Breaking News** for the latest information on updates, patches, and software issues regarding this release.

The Select Product screen also contains the following links:

Product Installation	Click this link to return to this Product Installation screen.
Documentation	Click this link to see links for the Getting Started Guide and the Release Notes.
Technical Support	Click this link to see information about Symantec technical support.
Browse CD	Click this link to see the contents of the CD.
Symantec Home	Click this link to go to: http://www.symantec.com
Copyright	Click this link to see copyright information.
Exit	Click this link to exit the product installer.

4 Click **Service Pack 1 for SFW 5.1, SFW HA5.1, and VCS 5.1 for Windows**

5 Review the Welcome message and the listed prerequisites. Ensure that any of the listed prerequisites applicable to your installation are met before proceeding.

Click **Next**.

6 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description. When upgrading on multiple computers in a single installation, all the computers must have the same platform type (x86 or x64). However, the computers can have different Windows operating systems. For example, you can upgrade multiple computers at once running Windows Server 2003 and Windows Server 2008.
Install Path	The install path cannot be changed for the upgrade.

7 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

8 If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning stating the following:

- The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system.
  If you are upgrading in a cluster environment, you must configure the Veritas Scheduler Service on all nodes to allow the automatic transfer of Capacity Monitoring and Automatic Volume Growth settings. Refer to the Capacity Monitoring and Automatic Volume Growth sections of the SFW Administrator's Guide for more information.

If applicable to your installation, perform the above procedures.

Click **OK**.

9 Review the pre-upgrade summary. Click **Back** to make changes if necessary.

Click **Install**.

10 If the installation is successful on all nodes, the installer automatically proceeds to the summary page.

Click **Next** after the progress indicator shows the installation is complete to proceed to the summary report to review the details of the failed installation. Note that if a security alert asks you to accept the Symantec driver software, click **Yes**.

11 Review the installation report, taking action where necessary, and click **Next**.

12 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Select the upgraded remote computers and click **Reboot**.

Wait for the remote computer to come back online. Click **Next**.

13 Click **Finish**.

14 Click **Yes** to reboot the local node.

Resetting the driver signing options

After completing the installation sequence, reset the driver signing option (set before upgrade) on each computer running Windows 2003.

To reset the driver signing options

1 Open the Control Panel, and click **System**.

2 Click the Hardware tab and click **Driver Signing**.

3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat for each computer.

Performing tasks required after the upgrade

Perform the tasks required for your Microsoft SQL cluster configuration after upgrading to SFW HA 5.1 SP1.

For information about the tasks required after an upgrade:

See "About tasks after the SFW HA 5.1 SP1 upgrade" on page 235.

Upgrading your Microsoft SQL Server

This section describes the following Microsoft SQL Server upgrade procedures:

- Upgrading from Microsoft SQL Server 2000 to SQL Server 2005
- Upgrading from Microsoft SQL Server 2000/2005 to Microsoft SQL Server 2008

Upgrading from Microsoft SQL Server 2000 to SQL Server 2005

If you are upgrading Microsoft SQL Server as well as upgrading SFW HA, use the following sequence of procedures:

- Upgrade SQL Server on the primary node
- Upgrade SQL Server on each additional node
- Create the SQL Server 2005 service group
- Upgrade SFW HA 4.3 MP2, 5.0.x, or 5.1.x to SFW HA 5.1 SP1

If the SQL 2005 services are running under an account which is not a member of either the domain admins group, the local administrators group on the cluster nodes, or a group with equivalent access rights on the nodes, the SQL services will only start on the last node installed.

For a workaround, see the following:

http://seer.entsupport.symantec.com/docs/281828.htm

For instructions on setting up SQL Server 2005 for high availability in a new deployment, see *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL*.

To upgrade SQL Server 2000 SP4 to SQL Server 2005, complete the following steps. Start with the primary node in the cluster; you will have to follow the steps for each node in the cluster.

To upgrade SQL Server on the primary node

1. Bring online the SQL 2000 service group resources up to the SQL Server 2000 resource. Right-click each resource and select **Online**. Click **Yes** in the confirmation pop-up to bring the resource online.

   This action brings online the disks, volumes, and IP address associated with SQL Server.

2. Right-click the SQL Server service group in tree view and click **Freeze > Persistent**.

3 Back up the SQL Server 2000 (MSSQL) and Registry (RegRep) folders on the shared disk by making a copy of each.

4 Start SQL Server 2000 under a local node context. Click **Start > Run** and type **services.msc**.

5 In the Services panel, find **MSSQLServer**, right-click it, and select **Start**.

6 Launch the Microsoft SQL Server 2005 installer and proceed through the installation process.

Make sure that you select the option to upgrade the existing instance(s) when prompted to do so. This action automatically places the data files in the proper location.

Note: Depending on the circumstances, an in-place upgrade may not be suitable for your environment. Refer to Microsoft documentation before beginning any SQL Server upgrade.

Refer to your Microsoft SQL Server 2005 documentation for more detailed instructions on installing Microsoft SQL Server.

7 Reboot the node if requested to do so when the installation completes.

8 Unfreeze and bring offline the service group on the primary node if you did not reboot. (Rebooting automatically brings the service group offline.)

9 Once you have completed the upgrade procedure on the primary node, you must perform the following steps on each additional node in the cluster.

To upgrade SQL Server on each additional node

1 Bring online the SQL 2000 service group resources up to the SQL Server 2000 resource, but do not online the regrep resources. Right-click each resource and select **Online**. Click **Yes** in the confirmation pop-up to bring the resource online.

2 Restore the copies of the SQL Server 2000 (MSSQL) and Registry (RegRep) folders on the shared disk. Delete the original MSSQL and RegRep folders.

3 Bring online the regrep resources (right-click and select **Online**).

4 In the tree view, freeze the service group (right-click and select **Freeze > Persistent**).

5 Start SQL Server 2000 under a local node context. Click **Start > Run** and type **services.msc**.

6 In the Services panel, find **MSSQLServer**, right-click it, and select **Start**.

7 Launch the Microsoft SQL Server 2005 installer and proceed through the installation process.

Make sure that you select the option to upgrade the existing instance(s) when prompted to do so. This action automatically places the data files in the proper location.

Refer to your Microsoft SQL Server 2005 documentation for more detailed instructions on installing Microsoft SQL Server.

8 Reboot the node if requested to do so when the installation completes.

9 Unfreeze and bring offline the service group on the secondary or additional node if you did not reboot. (Rebooting automatically brings the service group offline.)

10 Once you have completed upgrading all of the nodes in the SQL Server cluster, continue with creating the service group.

To create the SQL Server 2005 service group

1 On the primary node, bring online the VMdg and MountV resources from the SQL2000 service group. Right-click the resource, select Online, and select the primary node.

2 Delete the existing SQL2000 service group (in tree view). Right-click the service group and select **Delete**. Click **Yes** when asked to confirm if you want to delete the service group.

3 Create the SQL2005 service group using the SQL Server Configuration Wizard. Click **Start > All Programs > Symantec > SQL Server Configuration Wizard**.

For instructions on how to use the wizard, see the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL*.

4 Test switch the service group to the secondary node (or any additional node in the cluster). Right-click the service group in tree view, select **Switch To**, and select any additional node in the cluster.

5 Proceed with upgrading SFW HA.

Upgrading from Microsoft SQL Server 2000/2005 to Microsoft SQL Server 2008

The following steps describe how to upgrade your existing clustered SQL Server 2000 or SQL Server 2005 setup to SQL Server 2008. Complete these steps on all the cluster nodes that are part of the SQL service group, one node at a time.

At a high level, upgrading to SQL Server 2008 involves the following tasks:

- Upgrade SQL Server on the first cluster node
- Upgrade SQL Server on each additional failover node
- In case of a Disaster Recovery configuration, repeat the SQL upgrade procedures on the nodes at the secondary site. First upgrade the first cluster node at the DR site and then the additional failover nodes.
- Delete the existing SQL 2000 or 2005 service group, including the service group at the DR site, if applicable.
- Create a SQL Server 2008 service group using the SQL Server 2008 Configuration Wizard.
  In case of a DR setup, create a service group at the DR site

---

Note: In case of a Disaster Recovery setup, you must first upgrade SQL on the cluster nodes at the primary site and then proceed with the nodes at the secondary site. You must follow the same upgrade sequence at both sites, upgrade first node and then the additional nodes, as described in the procedures in this section.

These steps are applicable only if you already have SQL 2000 or SQL 2005 set up in an SFW HA cluster environment.

To configure a new HA and DR environment for SQL Server 2000 or SQL Server 2005, refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL*.

To configure a new HA and DR environment for SQL Server 2008, refer to the*Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008*.

Ensure that you do the following before proceeding with the upgrade tasks:

- Take a backup of the SQL databases.
- In case of a Disaster Recovery environment, ensure that the databases at the primary and secondary sites are synchronized.
- Ensure that you have installed SFW HA 5.1 Application Pack 1 for Windows and the VCS database agents for SQL 2008, on all the SQL service group cluster nodes that you want to upgrade.
- Make a note of the SQL virtual server name and all the IP addresses configured at both the primary and the secondary site, for the SQL setup in the DR environment. This includes the IP addresses used for the replication service group. You will need these details later

Upgrading SQL on the first cluster node

These steps assume a single SQL Server instance configured in a two-node cluster configuration.

To upgrade SQL Server on the first cluster node

1. On the node on which the SQL service group is online, take all the resources up to but excluding the MountV resource, offline. Keep the MountV resource online.
2. From the VCS Cluster Manager (Java Console), right-click the resource and select **Offline**. Click **Yes** in the confirmation pop-up box to take the resource offline.
3. Bring the registry replication (RegRep) resource online.
4. Make a backup copy of the SQL Server 2000 or SQL Server 2005, and the Registry (RegRep) directories from the shared disk and store them in a temporary location.

   You will need the backed-up directories while upgrading SQL on the additional failover nodes, later.
5. Freeze the SQL Server service group.

   From the Cluster Manager (Java Console), right-click the SQL Server service group in tree view on the left pane, and click **Freeze > Persistent**.
6. Launch the Microsoft SQL Server 2008 installer and install SQL Server 2008 on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so. The SQL Server 2008 installer then automatically places the SQL data files in the appropriate location.

   Refer to the Microsoft SQL Server 2008 documentation for instructions.
7. From the VCS Cluster Manager (Java Console), right-click the SQL Server service group in tree view on the left pane and click **Unfreeze**, and then take the entire service group offline on the node.

This completes the upgrade steps on the first cluster node. Proceed to upgrading SQL on the additional failover nodes.

Upgrading SQL on the additional failover node

Perform the following steps on each additional failover node that is part of the SQL service group.

To upgrade SQL Server on the additional failover node

1. Bring the SQL service group resources up to and including the MountV resource, online.

   From the VCS Cluster Manager (Java Console), right-click the resource and click **Online**. Click **Yes** in the confirmation pop-up box to bring the resource online.

2. Rename the SQL Server and the Registry (RegRep) directories on the shared disks. These directories were updated after the SQL 2008 install on the first node. You can also delete these directories, if desired.

3. Copy the backed-up SQL Server 2000 or SQL Server 2005, and the Registry (RegRep) directories from the temporary location to the shared disks. The backup directories are the same that you had backed up earlier while upgrading SQL on the first cluster node

4. Bring the RegRep resource online.

   From the VCS Cluster Manager (Java Console), right-click the resource and select **Online**. Click **Yes** in the confirmation pop-up box to bring the resource online.

5. Freeze the SQL Server service group.

   From the Cluster Manager (Java Console), right-click the SQL Server service group in tree view on the left pane and click **Freeze > Persistent.**

6. Launch the Microsoft SQL Server 2008 installer and install SQL Server 2008 on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so. The SQL Server 2008 installer automatically places the SQL data files in the appropriate location.

   Refer to the Microsoft SQL Server 2008 documentation for instructions.

7. Unfreeze and then take the SQL Server service group offline. From the VCS Cluster Manager (Java Console), right-click the SQL Server service group in tree view on the left pane and click **Unfreeze**, and then take the entire service group offline on the node.

This completes the upgrade steps on an additional failover node. Proceed to configuring the SQL Server 2008 service group in the cluster.

Configuring SQL service group

Perform the following steps on one of the cluster nodes at the primary site.

Note: This procedure requires you to run the SQL Server 2008 Configuration Wizard to configure the SQL 2008 service group. The SQL 2008 service group configuration steps are not described here. Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Guide for Microsoft SQL 2008* for instructions.

To configure SQL service group

1. Rename the Registry (RegRep) directory on the shared disk.
2. On one of the cluster node, bring the VMDg and MountV resources of the SQL service group, online.
3. If you have configured a VVR-based replication for SQL, delete the replication service group created for the SQL Server service group. From the Cluster Manager (Java Console), right-click the replication service group in tree view and click **Delete**. Click **Yes** when prompted to confirm if you want to delete the service group.
4. Delete the existing SQL Server 2000 or 2005 service group from the VCS Cluster Manager (Java Console).
5. In case of a DR configuration, repeat steps 1 to 4 on a node at the secondary site. Then perform the next steps on a node at the primary site.
6. Create the SQL Server 2008 service group using the SQL Server 2008 Configuration Wizard.

   Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Guide for Microsoft SQL 2008* for detailed instructions on how to create the service group using the SQL Server 2008 Configuration Wizard.
7. In case of a DR configuration, complete the required procedures for setting up the Global Cluster Option (GCO) and the replication components. Note that you must use the same SQL virtual server name, IP addresses and other details, that were used by the SQL 2000 or 2005 setup earlier.

   Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Guide for Microsoft SQL Server 2008* for instructions.

8 In case of a DR configuration, after completing the service group and replication components at the primary site, run the Disaster Recovery Wizard to set up the DR configuration between the primary and secondary sites.

   Note that you must use the same SQL virtual server name, IP addresses and other details, that were used by the SQL 2000 or 2005 setup earlier. Refer to the DR workflow in the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Guide for Microsoft SQL Server 2008* for instructions.

9 After creating the SQL service group, verify the configuration by switching the service group to another node in the cluster.

10 Delete the RegRep directory that you renamed in the first step. Repeat this at the DR site, if applicable.

11 If you had configured an MSDTC service group on Windows 2008 systems in your cluster, then after upgrading to SQL 2008 you have to reconfigure the MSDTC server using the SQL Server Configuration Wizard (not the SQL Server 2008 Configuration Wizard) and the MSDTC client manually.

   You do not have to reconfigure MSDTC if it is configured on Windows 2003 systems.

   Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Guide for Microsoft SQL Server 2008* for instructions.

Chapter 10

Tasks after SFW HA 5.1 SP1 Upgrade

This chapter includes the following topics:

About tasks after the SFW HA 5.1 SP1 upgrade

Table 10-1 displays tasks that may be performed after an SFW HA 5.1 SP1 upgrade.

Note: Whether a task is considered optional or not is dependent upon the steps performed for your SFW HA 5.1 SP1 upgrade. For example, if you uninstalled the VCS Management Console 5.1 during your upgrade process, then follow the instructions in this chapter to reinstall this application.

Table 10-1 SFW HA 5.1 SP1 post-upgrade tasks

Task	Description
1	Reinstall the VCS Management Console 5.1: See Reinstalling VCS Management Console 5.1
2	Include custom resources in the upgraded cluster: See Including custom resources in the upgraded cluster
3	Add a GCO resource to the ClusterService group: See Adding a GCO resource to the ClusterService group
4	Establish secure communication within the global cluster: See Establishing secure communication within the global cluster
5	Re-enabling VVR after the upgrade: See Re-enabling VVR after upgrading to SFW HA 5.1 SP1
6	Reconnect DMP DSM paths after the upgrade: See Reconnecting DMP DSM paths after the upgrade
7	Bring the print share service group online after the upgrade: See Bringing the print share service group online after the upgrade
8	Upgrade dynamic disk groups: See Upgrading dynamic disk groups

Table 10-2 displays the optional tasks that may be performed after an SFW HA 5.1 upgrade for an Exchange or SQL Server cluster.

Note: Whether a task is considered optional depends upon the steps performed for your SFW HA 5.1 SP1 upgrade for an Exchange or SQL Server cluster. For example, if you uninstalled the VCS Management Console 5.1 during your upgrade process, then follow the instructions in this chapter to reinstall this application.

Table 10-2 SFW HA 5.1 SP1 post-upgrade tasks for an Exchange or SQL Server cluster

Task	Description
1	Reinstall the VCS Management Console 5.1: See Reinstalling VCS Management Console 5.1
2	Include custom resources in the upgraded cluster: See Including custom resources in the upgraded cluster
3	Configure a secure cluster: See Configuring a secure cluster
4	Add a GCO resource to the ClusterService group: See Adding a GCO resource to the ClusterService group
5	Establish secure communication within the global cluster: See Establishing secure communication within the global cluster
6	Configure the VxSAS service (VVR only): See Configuring the VxSAS service (VVR only)
7	Re-enable VVR after the upgrade: See Re-enabling VVR after upgrading to SFW HA 5.1 SP1
8	Reconnect DMP DSM paths after the upgrade: See Reconnecting DMP DSM paths after the upgrade
9	Upgrade dynamic disk groups: See Upgrading dynamic disk groups

In addition, you may want to upgrade the Exchange or SQL Server service pack.

For information about upgrading Microsoft Exchange service packs:

See "Upgrading the Microsoft Exchange Service Pack" on page 253.

For information about upgrading Microsoft SQL service packs:

See "Upgrading the Microsoft SQL Service Pack" on page 258.

Reinstalling VCS Management Console 5.1

If you uninstalled VCS Management Console earlier according to the procedures for preparing for the upgrade, you can now reinstall it.

To re-install VCS Management Console 5.1

1. Install VCS Management Console 5.1.

   For information about installing VCS Management Console 5.1, see the *Veritas Cluster Server Management Console Implementation Guide*.

2. Restore the backed up VCS Management Console 5.1 data files.

3. Start the VCS Management Console. If the management console is clustered, bring the CMC_MS service group online.

Including custom resources in the upgraded cluster

The VCS Configuration Wizard does not upgrade custom resources. If a service group in the previous configuration contains custom resources, the wizard does not include the service group in the upgraded cluster.

To include a service group with custom resources in the upgraded cluster

1. Make sure that the agent binaries for the custom agent are available under `%VCS_HOME%\bin` where the variable *%VCS_HOME%* represents the VCS installation directory, typically `C:\Program Files\Veritas\cluster server`.

2. Stop the VCS engine (HAD) on all the nodes in the cluster.

   From the command prompt, type:

   ```
   C:\> hastop -all -force
   ```

3. During installation of the SFW HA 5.1 software, the installer copies previous configuration files to a backup location. Locate the backed up types.cf and main.cf files: `C:\Documents and Settings\All Users\Application Data\Veritas\cluster server\vpibackup`.

4. Copy the resource type definition for the custom resource from the backed up types.cf and add it to the types.cf file for the VCS 5.1 cluster.

5. Copy the service group configuration containing the custom resource from the backed up main.cf and add it to the main.cf file for the VCS 5.1 cluster.

6 If resources for a custom resource type are dependent on resources for agents bundled with VCS 5.1, you must update the resource definition of the VCS bundled agent to include the new attributes or remove the deprecated attributes.

For information on new and deprecated attributes, see the *Veritas Storage Foundation and High Availability Solutions 5.1 Release Notes*.

For information on the attribute values and descriptions, see the *Veritas Cluster Server 5.1 Bundled Agents Reference Guide*.

7 Verify the configuration.

From the command prompt, type:

```
C:\> hacf -verify config_directory
```

The variable *config_directory* refers to the path of the directory containing the main.cf and types.cf.

8 Start the VCS engine (HAD) on the node where you changed the configuration. Type the following at the command prompt:

```
C:\> hastart
```

9 Start the VCS engine (HAD) on all the other cluster nodes.

Configuring a secure cluster

If you want to configure a secure cluster, you must reconfigure the cluster using the VCS Configuration Wizard.

Note: The following procedure for configuring a secure cluster is not a required post-upgrade procedure. Performing the tasks in this procedure is dependent upon your configuration.

To configure a secure cluster

1 Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Cluster Configuration Wizard**.

2 The VCS Configuration Wizard Welcome screen appears.

Click **Next**.

3 The Configuration Options screen appears. Select **Cluster Operations** and then click **Next**.

4 The Domain Selection screen appears. Enter a domain name or select one from the list and then click **Next**.

5 The System Selection screen appears. Enter a system name and click **Add** or select a system from the list and click the arrow button to add it to the Selected System list.

Click **Next**.

6 The Cluster Configurations Options screen appears. Select **Edit Existing Cluster** and then click **Next**.

7 The Cluster Selection screen appears. Select the cluster name from the displayed list of clusters and then click **Next**.

8 The Edit Cluster Options screen appears. Select **Reconfigure** and then click **Next**.

9 Enter the username and password for the cluster in the Cluster User Information Dialog.

10 Select **Configure/Change Veritas Security Services (Single Sign-On)**.

Click **Next**.

11 Select Change Symantec Product Authentication Service Configuration (Change Root Broker).

12 Next, perform one of the following procedures:

- Select **Specify Symantec Product Authentication Service Root broker system** and enter a system name and click **Next**
- Select **Discover the Symantec Product Authentication Service Root broker system in the domain** and click **Scope**.

13 Select the Entire Domain or Specify Scope and select an organizational unit.

If needed, select a property, such as a system name to use as a filter in the Filter Criteria field and click **OK**.

Click **Next**.

For additional information, see the *Veritas Cluster Server 5.1 Administrator's Guide*.

Adding a GCO resource to the ClusterService group

VCS 5.1 provides the Global Cluster Option to enable a collection of VCS clusters to work together for wide-area disaster recovery.

Note: The procedure for adding a GCO resource to the ClusterService group is not a required post-upgrade procedure. Performing the tasks in this procedure is dependent upon your configuration.

For additional information, see the *Veritas Cluster Server 5.1 Administrator's Guide*.

Establishing secure communication within the global cluster

A global cluster is created in non-secure mode by default. You may continue to allow the global cluster to run in non-secure mode or choose to establish secure communication between clusters.

Note: The procedure for establishing secure communications within the global cluster is not a required post-upgrade procedure. Performing the tasks in this procedure is dependent upon your configuration.

The following prerequisites are required for establishing secure communication within a global cluster:

- The clusters within the global cluster must be running in secure mode.
- You must have Administrator privileges for the domain.

The following information is required for adding secure communication to a global cluster:

- The active host name or IP address of each cluster in the global configuration.
- The user name and password of the administrator for each cluster in the configuration.
- If the local clusters do not point to the same root broker, the host name and port address of each root broker.

Adding secure communication involves the following tasks:

- Taking the ClusterService-Proc (wac) resource in the ClusterService group offline on the clusters in the global environment
- Adding the -secure option to the StartProgram attribute on each node.
- Establishing trust between root brokers if the local clusters do not point to the same root broker.

- Bringing the ClusterService-Proc (wac) resource online on the clusters in the global cluster.

To take the ClusterService-Proc (wac) resource offline on all clusters

1. From Cluster Monitor, log on to a cluster in the global cluster.
2. In the **Service Groups** tab of the Cluster Explorer configuration tree, expand the **ClusterService** group and the Process agent.
3. Right-click the **ClusterService-Proc** resource, click **Offline**, and click the appropriate system from the menu.
4. Repeat the above steps for any additional clusters in the global cluster.

To add the -secure option to the StartProgram resource

1. In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the **ClusterService-Proc** resource under the **Process** type in the **ClusterService** group.
2. Click **View**, and then **Properties** view.
3. Click the Edit icon to edit the **StartProgram** attribute.
4. In the Edit Attribute dialog box, add `-secure` switch to the path of the executable Scalar Value.

   For example:

   ```
   "C:\Program Files\Veritas\Cluster Server\bin\wac.exe"-secure
   ```

5. Repeat 4 for each system in the cluster.
6. Click **OK** to close the Edit Attribute dialog box.
7. Click the **Save and Close Configuration** icon in the tool bar.
8. Repeat the above steps for each cluster in the global cluster.

To establish trust between root brokers if there is more than one root broker

- Establishing trust between root brokers is only required if the local clusters do not point to the same root broker.

  Log on to the root broker for each cluster and set up trust to the other root brokers in the global cluster. The complete syntax of the command is:

  ```
  vssat setuptrust --broker host:port
  --securitylevel low|medium|high [--hashfile filename
  | --hash roothash in hex]
  ```

  For example, to establish trust with a low security level in a global cluster comprised of Cluster1 pointing to RB1 and Cluster2 pointing to RB2:

  from RB1, type:

  ```
  vssat setuptrust --broker RB2:14141 --securitylevel low
  ```

  from RB2, type:

  ```
  vssat setuptrust --broker RB1:14141 --securitylevel low
  ```

To bring the ClusterService-Proc (wac) resource online on all clusters

1. In the **Service Groups** tab of the Cluster Explorer configuration tree, expand the **ClusterService** group and the Process agent.
2. Right-click the **ClusterService-Proc** resource, click **Online**, and click the appropriate system from the menu.
3. Repeat the above steps for any additional clusters in the global cluster.

Configuring the VxSAS service (VVR only)

If you upgraded or installed the Volume Replicator (VVR) option, you can launch the wizard for Veritas Volume Replicator Security Service (VxSAS) after the SFW HA installation to configure security services for all nodes. This step is required for VVR if you are upgrading from the SFW HA 4.3 MP2 version. If you are upgrading from SFW HA 5.0.x or 5.1.x to 5.1 SP1 and VxSAS was already configured for 5.0.x or 5.1.x, you do not need to configure it again.

Complete the following procedure to configure the VxSAS service for VVR.

The procedure has the following prerequisites:

- You must be logged on with administrative privileges on the server for the wizard to be launched.

- The account you specify must have administrative and log-on as service privileges on all the specified hosts.
- Avoid specifying blank passwords.
  In a Windows Server environment, accounts with blank passwords are not supported for log-on service privileges.
- Make sure that the hosts on which you want to configure the VxSAS service are accessible from the local host.

Note: The VxSAS wizard does not automatically launch after installing SFW or SFW HA. You must launch this wizard manually to complete the VVR security service configuration.

For details on this required service, see the *Veritas Storage Foundation Veritas Volume Replicator Administrator's Guide*.

To configure the VxSAS service

1. To launch the wizard, select **Start > All Programs > Symantec > Veritas Storage Foundation > Configuration Wizards > VVR Security Service Configuration Wizard** or run `vxsascfg.exe` from the command prompt of the required machine.

   Read the information on the Welcome page and click **Next**.

2. Complete the Account Information panel as follows:

Account name (domain\account)	Enter the administrative account name.
Password	Specify a password.

   If you have already configured the VxSAS service for one host that is intended to be a part of the RDS, make sure that you specify the same username and password when configuring the VxSAS service on the other hosts.

   Click **Next**.

3 On the Domain Selection panel, select the domain to which the hosts that you want to configure belong:

Selecting domains	The Available domains pane lists all the domains that are present in the Windows network neighborhood. Move the appropriate name from the Available domains list to the Selected domains list, either by double-clicking it or using the arrow button.
Adding a domain	If the domain name that you require is not displayed, click **Add domain** This displays a dialog that lets you specify the domain name. Click **Add** to add the name to the Selected domains list.

Click **Next**.

4 On the Host Selection panel, select the required hosts:

Selecting hosts	The Available hosts pane lists the hosts that are present in the specified domain. Move the appropriate host from the Available hosts list to the Selected hosts list, either by double-clicking it or using the arrow button. Use the Shift key with the up or down arrow keys to select multiple hosts.
Adding a host	If the host name you require is not displayed, click **Add host**. In the Add Host dialog specify the required host name or IP in the **Host Name** field. Click **Add** to add the name to the Selected hosts list.

After you have selected a host name, the **Configure** button is enabled. Click **Configure** to proceed with configuring the VxSAS service.

5 After the configuration completes, the Configuration Results page displays whether or not the operation was successful. If the operation was not successful, the page displays the details on why the account update failed. The page also displays possible reasons for failure and recommendations on getting over the failure.

6 Click **Back** to change any information you had provided earlier.

Click **Finish** to exit the wizard.

Re-enabling VVR after upgrading to SFW HA 5.1 SP1

After upgrading an environment where VVR replicates data from a primary site to a secondary site, use the appropriate procedures to re-enable VVR replication:

- Re-enabling VVR after the upgrading from 4.3 MP2 versions to 5.1 SP1
- Re-enabling VVR after upgrading from 5.0.x or 5.1.x to 5.1 SP1

Re-enabling VVR after the upgrading from 4.3 MP2 versions to 5.1 SP1

This section describes the process to re-enable VVR after upgrading from SFW HA 4.3 MP2 to SFW HA 5.1 SP1.

Re-enabling from 4.3MP2 versions to 5.1 SP1

Follow the procedures in the order given while re-enabling from SFW HA 4.3MP2 to SFW HA 5.1 SP1.

Warning: A full autosynchronization is required if the procedures listed below are not performed in the given order.

To enable the updated objects

1. Bring the Disk Group Resource online, by performing one of the following procedures:
   - From the Cluster Manager (Java Console), right-click the Disk Group Resource and click **Online**.
   - From the command line, type:

     ```
     hares -online resource_name -sys system_name
     ```

2. Bring the VVR IP Resource online, by performing one of the following procedures:
   - From the Cluster Manager (Java Console), right-click the VVR IP Resource and click Online.
   - From the command line, type:

     ```
     hares -online resource_name -sys system_name
     ```

3. Re-associate the Replicator Log volume, by performing one of the following procedures:

- From the VEA console and on the primary site, expand the RDS to which you want to associate the Replicator Log volume. Right-click the primary RVG, and click the **Associate Replicator Log** option. Select the correct Replicator Log volume from the dialog box and click **OK**.
- From the command line, type:

  ```
  vxrvg [-g diskgroup_name] aslog rvg_name volume_name
  ```

4. To attach the RLINK, open a command prompt and run the following command:

   ```
   vxrlink -f att RLINK
   ```

5. Repeat steps 1-3 on the secondary site.
6. On both the primary and the secondary site, bring the RVG service group online, by performing one of the following procedures:
   - From the Cluster Manager (Java Console), right-click the RVG service group and click **Online**.
   - From the command line, type:

     ```
     hagrp -online group_name -sys system_name
     ```

7. On the primary site, bring the application service group online by performing one of the following procedures:
   - From the Cluster Manager (Java Console), right-click the application service group and click **Online**.
   - From the command line, type:

     ```
     hagrp -online group_name -sys system_name
     ```

8. If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on options in your environment, these tasks may include mounting databases or manually starting the application.

Re-enabling VVR after upgrading from 5.0.x or 5.1.x to 5.1 SP1

After upgrading the cluster nodes from SFW HA 5.0.x or 5.1.x versions to SFW HA 5.1, re-enable VVR on the upgraded site. The site is in the secondary role during the upgrade and when re-enabling VVR.

To re-enable VVR after upgrading from SFW HA 5.0.x or 5.1.x to SFW HA 5.1 SP1, you must perform the following procedures:

- Enabling the updated objects on the secondary site
- Preparing the primary site for upgrade
- Migrating the applications back to the original primary site

Enabling the updated objects on the secondary site

Follow the procedure below to enable the updated objects on the secondary site.

To enable the updated objects on the secondary site

1. Bring the Disk Group Resource online on the secondary site, by performing one of the following procedures:
   - From the Cluster Manager (Java console), right-click the Disk Group Resource and click **Online**.
   - From the command line, type:

     ```
     hares -online resource_name -sys system_name
     ```

2. Bring the RVG service group online, by performing one of the following procedures:
   - From the Cluster Manager (Java Console), right-click the RVG service group and click **Online**.
   - From the command line, type:

     ```
     hagrp -online group_name -sys system_name
     ```

   For VVR environments with multiple secondary sites, any operations that need to be performed on a secondary site should be repeated on all secondary sites.

Preparing the primary site for upgrade

For an SFW HA 5.1 SP1 upgrade, if you are performing this procedure on the original secondary site, go to the procedure to prepare the primary site for upgrade.

See "Preparing the primary site for upgrade" on page 158.

For an SFW HA 5.1 SP1 upgrade on an Exchange or SQL Server cluster, if you are performing this procedure on the original secondary site, go to the procedure to prepare the primary site for upgrade.

- For an SFW HA 5.1 SP1 upgrade on an Exchange cluster:

See "Preparing the primary site for upgrade" on page 183.

- For an SFW HA 5.1 SP1 upgrade on an SQL server cluster:
  See "Preparing the primary site for upgrade" on page 209.

If you have completed the upgrades on both the primary and secondary sites, you can now migrate the applications back to the original primary.

See "Migrating the applications back to the original primary site" on page 249.

Migrating the applications back to the original primary site

This section discusses the process of migrating the applications back to the original primary site.

Migrate the applications back to the original primary site

Once you have upgraded both the primary and the secondary sites, you may want to switch back the applications to the site that was primary before the upgrade.

To migrate the applications back to the original primary

1. In the Service Groups tab of the Cluster Manager, right-click the Application service group that is online at the current primary site.
2. Click **Switch To**, and click **Remote switch**.
3. In the Switch global group dialog box, click the cluster of the original primary to switch the group.
4. Click the specific system where you want to bring the global application service group online, and then click **OK.**

Reconnecting DMP DSM paths after the upgrade

After you complete the upgrade for an existing DMP DSM environment, or if you have added DMP DSMs during the upgrade perform the following tasks.

To reconnect DMP DSM paths after the upgrade

1. Physically connect any additional paths to the DMP DSM array that were disconnected before the upgrade.
2. In the VEA, rescan the disks.

Bringing the print share service group online after the upgrade

For SFW HA 5.1 SP1, the PrintSpool agent (for VCS) has been enhanced to meet scalability and performance requirements. The PrintSpool agent no longer depends on the RegRep agent for operation. The dependency between the PrintSpool and the RegRep resource in a print share service group has been eliminated.

This affects print share service groups configured in earlier versions of VCS. If you have configured a print share and you upgrade VCS, then the existing print share service group will fail to come online, after the upgrade.

After the upgrade is complete, you must run the Print Share Configuration Wizard to modify the print share service group. This will allow the wizard to make the required changes to the service group configuration.

Note: In case of an upgrade, do not add or remove any resources, or modify any other attributes in the print share service group for the first time you run the Print Share Configuration Wizard to modify the service group.

Before you modify the existing print share service group:

- Make sure that the VCS engine (HAD) is running on the cluster node.
- Mount the drives or LUNs that contain the spooler and the registry replication directories on the system on which you will run the wizard.

To modify the print share service group after an upgrade

1. Start the Print Share Configuration Wizard. **(Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Print Share Configuration Wizard)**
2. Read the information on the Welcome panel and click **Next**.
3. On the Wizard Options panel, click **Modify service group**, select your existing print share service group, and then click **Next**.
4. On the Service Group Configuration panel, click **Next**.

5 On the Configure Data Path panel, complete the following and then click **Next.**

Spooler Directory	Leave this field as it is. Do not make any changes to the spooler directory path.
Replication Directory	Type the path or click ... (ellipsis button) to browse for the directory. All changes related to the printer registry keys will be logged at this location. The selected directory must reside on a shared, non-system drive.

6 Click **Next** on the subsequent wizard panels and complete the wizard steps. You can now bring the printshare service group online.

Upgrading dynamic disk groups

If your previous installation included Volume Manager 4.x, upgrade the disk group types to make use of the current program features.

For additional information, see the *Veritas Storage Foundation 5.1 Administrator's Guide*.

Note: If you upgrade a disk group to SFW HA 5.1, you cannot import it to another server that is running an earlier version of Volume Manager or Disk Management. After upgrading a disk group, the group cannot revert to an earlier version.

To upgrade a dynamic disk group version

1 Open up the VEA.

In the tree view, right-click the disk group you want to upgrade and select **Upgrade Dynamic Disk Group Version**.

2 Click **Yes** to upgrade the dynamic disk group.

Chapter 11

Microsoft Service Pack upgrades

This chapter includes the following topics:

Upgrading the Microsoft Exchange Service Pack

This section discusses the following Microsoft Exchange service pack (SP) upgrades:

- Upgrading Microsoft Exchange 2003 SP2 in a VCS environment:
  See "Upgrading to Microsoft Exchange 2003 SP2 in a VCS environment" on page 253.
- Upgrading Microsoft Exchange 2007 SP1 or SP2 in a VCS environment:
  See "Upgrading to Microsoft Exchange 2007 SP1 or SP2 in a VCS environment" on page 255.

Upgrading to Microsoft Exchange 2003 SP2 in a VCS environment

This section describes the procedure for upgrading to Microsoft Exchange 2003 SP2 in a VCS environment, if you already have Microsoft Exchange 2003 installed and you want to apply Exchange 2003 SP2.

For information on upgrading an Exchange cluster to SFW HA 5.1:

See "About upgrading an Exchange Server cluster" on page 175.

Before upgrading to Microsoft Exchange 2003 SP2, make sure to set the "DetailMonitor" attribute of all "ExchService" type resources to zero.

Perform the following steps to upgrade an Exchange 2003 installation on a node that is part of the Exchange service group. Make sure that all the nodes which are part of the Exchange service group have the same version and service pack level of Microsoft Exchange.

To upgrade to Microsoft Exchange 2003 SP2

1. Make sure that you do not mount the Exchange databases on the failover nodes. Bring the Exchange service group online on the node where you are upgrading the Exchange installation.
2. Stop HAD on the node where the service group was brought online. At the command prompt, type:

   ```
   C:\> hastop -local -force
   ```

3. Install Microsoft Exchange 2003 SP2 on the node where the service group was brought online.
4. Start HAD on the node. At the command prompt, type:

   ```
   C:\> hastart
   ```

5. After the Exchange 2003 SP2 installation is complete, take the Exchange service group offline.
6. Restart the Windows Management Instrumentation (WMI) service from the Services snap-in.
7. Repeat step 1 through step 6 on all remaining nodes that are part of the Exchange service group.
8. Update the ExchConfig registry information on every system where Exchange is upgraded.
9. To update the registry on the local system, navigate to `%vcs_home%\bin\ExchSetup` folder and type the following at the command prompt:

   ```
   Setup.exe /UpdateExchVersion
   ```

10. To update the registry on more than one node simultaneously, navigate to `%vcs_home%\bin\ExchSetup` folder and type the following at the command prompt:

    ```
    Setup.exe /UpdateExchVersion system_name1 system_name2...
    ```

    Here, system_name1, system_name2 are the cluster node names.

11 This completes the upgrade. You can now bring the Exchange service group online in the cluster.

12 For a disaster recovery environment, repeat this procedure at the secondary (DR) site.

Upgrading to Microsoft Exchange 2007 SP1 or SP2 in a VCS environment

This section describes how to upgrade Exchange 2007 to Exchange 2007 SP1 or SP2 using the Exchange 2007 Upgrade Wizard. It is applicable only if you already have Exchange 2007 set up in a VCS cluster environment.

For information on upgrading an Exchange cluster to SFW HA 5.1:

See "About upgrading an Exchange Server cluster" on page 175.

To configure a new HA and DR environment for Exchange 2007, refer to the following manual:

See the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007*.

Before you proceed with the Exchange 2007 upgrade to SP1 or SP2, note the following:

- Ensure that the Exchange 2007 service group is offline in the cluster.
- While performing the upgrade the Exchange 2007 Upgrade Wizard renames and then restarts the cluster node. Exit all the other programs before you run the wizard on a cluster node.

Note: The following procedure describes how to upgrade Exchange 2007 to Exchange 2007 SP1, this procedure can also be used to upgrade Exchange 2007 to Exchange 2007 SP2.

Complete the following steps on all cluster nodes that are part of the Exchange 2007 service group, one node at a time.

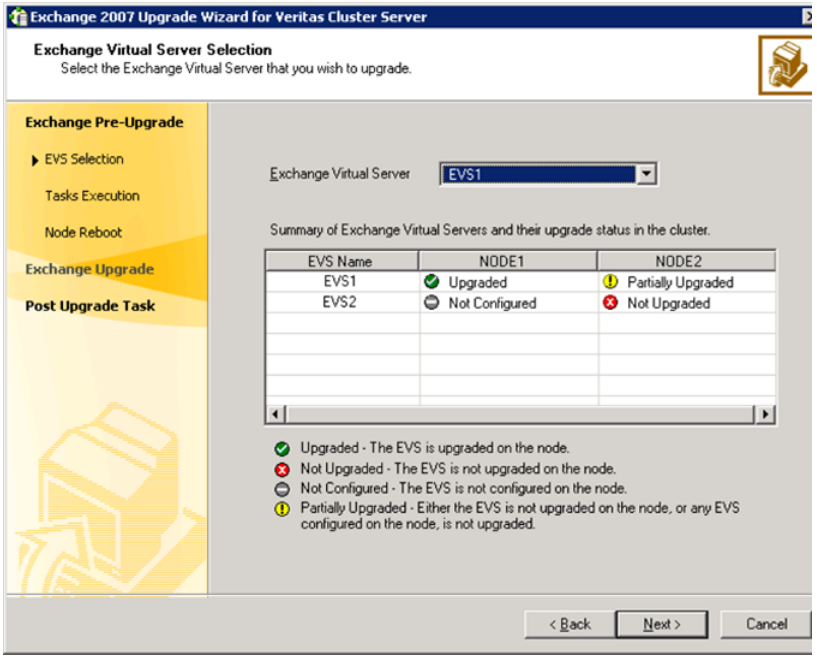
To upgrade Exchange 2007 to Exchange 2007 SP1

1 On one of the cluster nodes, click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange 2007 Upgrade Wizard** to start the Exchange 2007 Upgrade wizard.

2 Review the information on the Welcome panel and click **Next**.

3 On the Exchange Virtual Server Selection panel, select the Exchange virtual server that you want to upgrade and then click **Next**.

The Summary table provides the details of the Exchange virtual servers in the cluster and their upgrade status on each cluster node.



4 The wizard performs the tasks required to set up the VCS environment for the Exchange upgrade. The Tasks table displays the progress of the various tasks. After all the tasks are completed, click **Next**.

5 Review the information on the Cluster Node Reboot panel and then click **Reboot**. The wizard prompts you to reboot the node. Click **Yes** to reboot the node.

The Exchange virtual server name is temporarily assigned to the cluster node. On rebooting the node, the Exchange 2007 Upgrade Wizard is launched automatically with a message that the Exchange pre-upgrade tasks are complete. Do not click **Continue** at this time. Wait until after the Exchange upgrade is complete.

6 Run the Exchange 2007 SP1 installer to upgrade Exchange 2007 on the node. Type the following at the command prompt:

```
<drive letter>:\setup.com /mode:Upgrade
```

Here `<drive letter>` is the drive where the Exchange SP1 installer is located.

Note: You can also run Setup.exe to launch the installer GUI for upgrading Exchange. If using the installer GUI, ensure that you do not select any other Exchange 2007 server role. Only the Mailbox server role must be upgraded.

Verify that the upgrade has completed successfully. In case there are errors or if the upgrade has partially succeeded or has failed, resolve the errors and ensure that the upgrade is successful.

Refer to the Microsoft Exchange documentation for more information.

7 Return to the Exchange 2007 Upgrade Wizard and click **Continue**.

If the wizard is not running, click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange 2007 Upgrade Wizard** to start the wizard and then click **Next**.

8 The wizard performs the tasks required to set up the VCS environment after the Exchange upgrade. The Tasks table displays the progress of the various tasks. After all the tasks are completed, click **Next**.

9 Review the information on the completion panel and then click **Finish**.

The wizard displays the status of the Exchange virtual server upgrade. The Summary table provides the details of the Exchange virtual servers in the cluster and their upgrade status on each cluster node.

10 Repeat these steps on the remaining cluster nodes. After you have upgraded all the cluster nodes that are configured to host the Exchange virtual server, bring the Exchange 2007 service group online in the cluster.

Note: Do not bring the Exchange 2007 service group online until you have completed the upgrade on all the cluster nodes that are part of the service group.

---

11 For a disaster recovery environment, repeat this procedure at the secondary (DR) site.

Upgrade considerations in case of multiple Exchange virtual servers

Consider the scenario where there are multiple Exchange virtual server instances in the cluster (an any-to-any configuration).

Table 11-1 describes the configuration objects.

Table 11-1 Exchange 2007 SP1 upgrade configuration objects

Object	Description
Node1, Node2, Node3	Physical node names
EVS1, EVS2	Exchange virtual servers

The configuration is such that:

- EVS1 can fail over on Node1 and Node2.
- EVS2 can fail over on Node3 and Node2.

So, Node2 is the common failover node for EVS1 and EVS2.

In this case, upgrade the Exchange virtual servers as follows:

- Upgrade EVS1 on Node1.
- Upgrade EVS2 on Node3.
- And then upgrade either EVS1 or EVS2 on Node2.
  You must upgrade Node2 (common failover node) only once; the Exchange virtual server (whether EVS1 or EVS2) does not matter.

In general, for multiple Exchange virtual servers, upgrade each Exchange virtual server on one cluster node first, and then upgrade any one of the Exchange virtual servers on the common failover nodes.

Upgrading the Microsoft SQL Service Pack

This section discusses the following Microsoft SQL Server service pack (SP) upgrades:

- Upgrading Microsoft SQL 2000 to SP4 in a VCS environment:
  See "Upgrading Microsoft SQL 2000 to SP4 in a VCS environment" on page 259.
- Upgrading Microsoft SQL 2005 to SP1 in a VCS environment:
  See "Upgrading Microsoft SQL 2005 to SP1 in a VCS environment" on page 261.
- Upgrading Microsoft SQL 2005 to SP2 or later version in a VCS environment:

See "Upgrading Microsoft SQL 2005 to 2005 SP2 or later in a VCS environment" on page 262.

- Upgrading Microsoft SQL 2008 to 2008 SP1 in a VCS environment:
  See "Upgrading Microsoft SQL 2008 to 2008 SP1 in a VCS environment" on page 266.

Upgrading Microsoft SQL 2000 to SP4 in a VCS environment

This section outlines the procedure required to install Microsoft SQL 2000 Server SP4 on a computer running Veritas Storage Foundation HA for Windows 5.1.

For information on upgrading a SQL Server cluster to SFW HA 5.1.

See "About upgrading a SQL Server cluster" on page 201.

Consider the following points before applying Microsoft SQL 2000 SP4 to a production server:

- Review your Microsoft documentation for the requirements for a Microsoft SQL 2000 Server SP4 installation.
  Make sure that your system meets these requirements.
- Make sure that you have a recent backup of your system and user databases.
- Server down time is required for this procedure.

To install Microsoft SQL 2000 Server SP4

1. From the Cluster Explorer, right-click the SQL Server service group and select **Offline** on all nodes.
2. On the node where the SQL Server service group was taken offline, online the MountV resource for the shared drive containing the SQL databases (for example, S:\MSSQL$SQL2000).
3. On the shared disk, make a copy of your recent MSSQL data files directory (S:\MSSQL$SQL2000) and rename it, for example to S:\MSSQL$2000.SP3A.
4. From the Cluster Explorer, right-click the SQL Server service group which is now partially online, and select **Freeze >Persistent**.
5. Install Microsoft SQL 2000 Service Pack 4 on the active node (where the SQL Server service group is online), using the instructions provided by Microsoft.
6. Repeat step 5 for each additional SQL instance in this service group, if you have more than one instance in this service group.
7. From the Cluster Explorer, right-click the SQL Server service group which is still online and select **Unfreeze**.

8 From the Cluster Explorer, right-click the SQL Server service group and select **Offline** on the node where it was online.

9 In a Disaster Recovery environment, switch the Replication service group to one of the other additional or failover nodes in this cluster.

10 On the failover node, online the MountV resource for the shared drive containing the SQL databases (for example, S:\MSSQL$SQL2000).

11 On the shared disk, rename the S:\MSSQL$SQL2000 directory to S:\MSSQL$SQL2000.SP4. If S:\MSSQL$SQL2000.SP4 already exists on the shared disk, then delete it before renaming the S:\MSSQL$SQL2000 directory.

12 On the shared disk, rename the S:\MSSQL$SQL2000.SP3A directory to S:\MSSQL$SQL2000. If there are additional nodes in this cluster to be updated, copy the S:\MSSQL$SQL2000.SP3A directory to S:\MSSQL$SQL2000 instead of renaming the directory.

13 From the Cluster Explorer, right-click the SQL Server service group which is now partially online and select **Freeze >Persistent**.

14 Install Microsoft SQL 2000 Service Pack 4 on the active node (where the SQL Server service group is online), using the instructions provided by Microsoft.

15 Repeat step 14 for each additional SQL instance in this service group, if you have more than one instance in this service group.

16 From the Cluster Explorer, right-click the SQL Server service group which is still online and select **Unfreeze**.

17 From the Cluster Explorer, right-click the SQL Server service group and select **Offline** on the node where it was online.

18 Repeat step 9 through step 17 on each additional node if more than two SQL 2000 nodes are in use.

19 For a Disaster Recovery environment, repeat this procedure at the secondary site.

20 When Microsoft SQL 2000 Server Service Pack 4 has been completely installed on all nodes, test user connectivity to the instances.

21 Test the SQL Server service group by bringing it online and failing it over from node to node. When testing is complete, the upgrade is complete.

22 If more than one SQL Server service group is present, repeat this entire procedure for each SQL Server service group.

Upgrading Microsoft SQL 2005 to SP1 in a VCS environment

This section outlines the procedure needed to install Microsoft SQL 2005 Server SP1 on a computer running Veritas Storage Foundation HA for Windows 5.1.

Consider the following points before applying Microsoft SQL 2005 Server SP1 to a production server:

- Review your Microsoft documentation for the requirements for a Microsoft SQL 2005 Server SP1 installation.
  Make sure that your system meets these requirements.
- Make sure that you have a recent backup of your system and user databases.
- Server down time is required for this procedure.

To install Microsoft SQL 2005 Server SP1

1. From the Cluster Explorer, right-click the SQL Server service group and select **Offline** on all nodes.
2. On the node where the SQL Server service group was taken offline, online the SQL 2005 resource for the shared drive containing the SQL databases.
3. From the Cluster Explorer, right-click the SQL Server service group which is now partially online, and select **Freeze >Persistent**.
4. If a VVR RVG service group is present, verify that it is online on the node where Microsoft SQL 2005 Service Pack 1 is to be installed.
5. Install Microsoft SQL 2005 Service Pack 1 on the active node (where the SQL Server service group is online), using the instructions provided by Microsoft.
6. Repeat step 5 for each additional SQL instance in this service group, if you have more than one instance in this service group.
7. From the Cluster Explorer, right-click the SQL Server service group which is still online and select **Unfreeze**.
8. From the Cluster Explorer, right-click the SQL Server service group and select **Offline** on the node where it was online.
9. On the failover node, online the SQL 2005 resource for the shared drive containing the SQL databases.
10. From the Cluster Explorer, right-click the SQL Server service group which is now partially online and select **Freeze >Persistent**.
11. Install Microsoft SQL 2005 Service Pack 1 on the active node (where the SQL Server service group is online), using the instructions provided by Microsoft SQL Server 2005 Service Pack 1 Setup.

12 Repeat step 11 for each additional SQL instance in this service group, if you have more than one instance in this service group.

13 From the Cluster Explorer, right-click the SQL Server service group which is still online and select **Unfreeze**

14 From the Cluster Explorer, right-click the SQL Server service group and select **Offline** on the node where it was online

15 Optionally reboot and online each service group to verify the database connect for each node.

16 Repeat step 9 through step 17 on each additional node if more than two SQL 2005 nodes are in use.

17 For a Disaster Recovery environment, repeat this procedure at the secondary site.

18 When Microsoft SQL 2005 Server Service Pack 1 has been completely installed on all nodes, test user connectivity to the instances.

19 Test the SQL Server service group by bringing it online and failing it over from node to node. When testing is complete, the upgrade is complete.

20 If more than one SQL Server service group is present, repeat this entire procedure for each SQL Server service group.

Upgrading Microsoft SQL 2005 to 2005 SP2 or later in a VCS environment

This section describes how to upgrade SQL 2005 to SQL 2005 SP2 or later on a computer running Veritas Storage Foundation HA for Windows 5.1 SP1.

Note: Do not follow the installation steps provided in this section to install SQL Server 2005 Service Pack 1 and all other hotfixes released before Service Pack 2.

Prerequisites

Consider the following points before applying Microsoft SQL 2005 Server SP2 or later service pack version to a production server:

- You must be a domain user having administrative privileges to the cluster nodes.
- You must have administrative privileges to the SQL instance that you want to upgrade.
- You must back up the SQL Server 2005 databases.

- Refer to the Microsoft documentation for prerequisites related to SQL Server 2005 Service Pack installation.

Preliminary installation information

Typically, multiple SQL instances are configured in a VCS cluster. Each SQL service group is configured to fail over on one or more nodes in the cluster. The node on which the SQL service group is online is called as the Active node for that SQL instance. The node on which the SQL service group is offline is called as the Passive node for that SQL instance. The procedure for applying service packs, patches, or hotfixes for SQL instances varies depending on whether it is an active or a passive node. This document describes procedures for both the cases in detail.

Use the procedure that applies to the type of setup you have.

To provide context, the installation procedures described in this document assume two SQL Server 2005 instances configured in a three-node VCS cluster.

Table 11-2 lists the configuration objects referenced in the following procedures.

Table 11-2 SQL Server 2005 SP upgrade configuration objects

Object	Description
Node1, Node2, Node3	Cluster node names
SQLinst1, SQLinst2	SQL Server 2005 instance names
SQLServer2005SP2-KB921896-x86-ENU.exe	SQL Server 2005 SP2 installer for 32-bit

The configuration is as follows:

- SQLinst1 can fail over on Node1 and Node2, and SQLinst2 can fail over on Node3 and Node2.
  So, Node2 is the common failover node for SQLinst1 and SQLinst2.
- The SQL service group for SQLinst1 is online on Node1, and the SQL service group for SQLinst2 is online on Node3.
  So, Node1 and Node3 are the “active” nodes for SQLinst1 and SQLinst2 respectively. Node2 is the “passive” node for both SQL instances.
  You will first install the service pack on Node2 (passive node) and then proceed to install on Node1 and Node3.

Installing the Service Pack on “passive” cluster nodes

Perform these steps on all the nodes where the SQL service group is configured to fail over but is not online. You can either perform the installation at one time

for all the SQL instances that are configured to fail over on the node, or repeat the steps for each SQL instance separately.

Do not run these steps for SQL instances whose corresponding service groups are online on the nodes (active nodes). For installation on active nodes,

See "Installing the Service Pack on "active" cluster nodes" on page 265.

Note: You can install SQL Server 2005 Service Pack in an unattended mode from the command prompt using the /quiet switch to suppress the setup dialog boxes. Refer to the Microsoft documentation for more information.

To install the Service Pack on passive cluster nodes

1. Ensure that service groups for SQL instances SQLinst1 and SQLinst2 are offline on Node2.

   Note: This upgrade procedure will not upgrade the SQL instance whose corresponding service group is online on the node.

   ---

2. On Node2, copy the SQL Server 2005 Service Pack installer or map a drive to the directory where the installer is located.
3. From the command prompt on Node2, navigate to the directory where the installer is located.
4. From the command prompt, run the Service Pack installer command with the appropriate options.

   For example,

   The command format for running the installer is as follows:

   ```
   SQLServer2005SP2-KB921896-x86-ENU.exe [options] /passive=1
   ```

   You can use the following options for the command:

   - /allinstances
     This option upgrades all SQL Server 2005 instances and shared components to the desired SQL Server 2005 SP.
   - /instancename = "<instance1>, <instance2>, ..."
     This option upgrades only the specified SQL Server 2005 instances and shared components to the desired SQL Server 2005 SP.

   You can run any of the following commands on Node2:

   ```
   SQLServer2005SP2-KB921896-x86-ENU.exe /allinstances /passive=1
   ```

or

```
SQLServer2005SP2-KB921896-x86-ENU.exe /instancename = SQLinst1,
SQLinst2 /passive=1
```

Note that in case of multiple SQL instances, there should be no spaces between instance names in the command.

5 Follow the upgrade wizard to complete the installation.

Once the installation is complete on the passive nodes, proceed to install on the active nodes.

Installing the Service Pack on “active” cluster nodes

Perform these steps on all the nodes on which the SQL service group is online. You can either perform the installation at one time for all the SQL instances that are configured to fail over and are online on the node, or repeat the steps for each SQL instance separately.

Do not run these steps for SQL instances whose corresponding service groups are offline on the nodes (passive nodes). For installation on passive nodes,

See “Installing the Service Pack on “passive” cluster nodes” on page 263.

Referring to the configuration example described earlier, run these steps on Node1 and Node3 where the SQL service groups for SQLinst1 and SQLinst2 are online.

To install the Service Pack on active cluster nodes

1 Ensure that the SQL service group for SQLinst1 is online on Node1.

2 In the SQL service group for SQLinst1, take all resources of type SQLServer2005 offline on Node1.

If there are other SQL Server 2005 instances configured on the node that you want to upgrade, take SQLServer2005 resources of the respective service groups offline as well.

3 From the Services snap-in, stop the SQL server Full Text Search service and the Analysis service, if they are not configured as part of the SQL service groups.

4 Freeze the SQL service group for SQLinst1 on Node1.

From the Cluster Manager (Java Console), right-click the SQL service group, select **Freeze** and click **Temporary**.

or

Type the following on the command prompt: `hagrp -freeze service_group`

5 If the SQL Server Reporting Services is installed for a particular instance, start the SQL Server Database Service of the respective instance using the Services snap-in.

6 Run the SQL Server 2005 Service Pack installer.

Double-click **SQLServer2005SP2-KB921896-x86-ENU.exe** to launch the SP installation wizard.

7 Follow the upgrade wizard to complete the installation.

8 After the installation is complete, stop the SQL Server services, if started before applying the patch.

Note: SQLServer2005 resources may go in UNKNOWN state if we start the services outside the VCS cluster. Ignore this and probe the resources after installation is completed and all the services are stopped.

---

9 Unfreeze the SQL service group and probe the resources for SQLinst1 on Node1.

From the Cluster Manager (Java Console), right-click the SQL service group, select **Unfreeze**.

or

Type the following on the command prompt: `hagrp -unfreeze service_group`

10 From the Services snap-in, start the SQL server Full Text Search service and the Analysis service, if they are not configured as part of the SQL service groups.

11 Ensure that all the services related to the SQL Server 2005 instance are in stopped state

12 Apart from the SQL Browser service, set the startup type of all the SQL services to manual.

13 Bring the SQLServer2005 resources in the SQL service group for SQLinst1 online on Node1.

14 Repeat step 1 to step 13 for SQLinst2 on Node3.

Upgrading Microsoft SQL 2008 to 2008 SP1 in a VCS environment

This section discusses the procedure to upgrade Microsoft SQL 2008 to Microsoft SQL 2008 SP1 in a VCS 5.1 SP1 environment.

The procedure is applicable only if you already have SQL 2008 set up in a VCS cluster environment.

Prerequisites for upgrading to Microsoft SQL Server 2008 SP1

Consider the following points before proceeding with the upgrade:

- You must have administrative privileges to the SQL instance that you want to upgrade.
- Make sure that you have a recent backup of your system and user databases.
- Make sure that the VCS version installed is VCS 5.1 SP1.
- Refer to the Microsoft documentation for prerequisites related to SQL Server 2008 Service Pack 1 installation.

Upgrading to Microsoft SQL Server 2008 SP1

The following upgrade procedure considers a two node cluster, Node A and Node B.

The SQL service group is ONLINE on Node A, and Node B is the passive node.

Upgrading from Microsoft SQL 2008 to Microsoft SQL Server 2008 SP1

1. Change the RegRep resource Exclude Keys Attribute on any one of the cluster nodes, using HA commands or JavaGUI.

   Add the following key in Exclude Keys:

   ```
   HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\
   InstanceName\MSSQLServer\Filestream
   ```

2. Upgrade the SQL 2008 instance on Node B (passive node) and reboot Node B.

   Note: Upgrade to SQL 2008 SP1 requires a reboot if you are upgrading for first time.

3. Proceed to failover the Service Group from Node A to Node B.
4. Ensure that all services are coming online and working as expected.

   Check the SQL version.

5 Upgrade the SQL 2008 instance on Node A. After a reboot, failover the Service Group and repeat step 4 .

6 Remove the Exclude key from RegRep resource that was added in step 1.

Chapter 12

Upgrading an Oracle cluster

This chapter includes the following topics:

About upgrading an Oracle cluster

This chapter describes the steps for upgrading from SFW 4.3.MP2, 5.0.x, or 5.1.x to SFW HA 5.1 SP1 with different versions of Oracle.

Upgrade matrix for an Oracle cluster

Table 12-1 presents possible scenarios for upgrading to an SFW HA cluster with Oracle.

Depending on your current configuration and upgrade scenario, the upgrade process involves one or both of the following procedures:

- VCS and the VCS database agent for Oracle upgrade
- Oracle upgrade

Table 12-1 Oracle cluster upgrade

Upgrade from this configuration ...	To this configuration ...
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, 5.1, and 5.1 AP1 ■ Windows Server 2003 SP1 ■ Oracle 9.0.1, 9.0.2, 9.1x	■ SFW HA 5.1 SP1 ■ Windows Server 2003 SP2 ■ Oracle 9.2x
■ SFW HA 4.3 MP2, 5.0, 5.0 RP1a, 5.0 RP2, 5.1, and 5.1 AP1 ■ Windows Server 2003 SP1 ■ Oracle 10.1, 10.2	■ SFW HA 5.1 SP1 ■ Windows Server 2003 SP2 ■ Oracle 10.1, 10.2

Upgrading to SFW HA 5.1 SP1

Perform the following tasks to upgrade to SFW HA 5.1 SP1:

- Prepare the VCS cluster for upgrade:
  See "Preparing the VCS cluster for upgrade" on page 161.
- Upgrade SFW HA and the database agent for Oracle from version 4.3 MP2, 5.0.x, or 5.1.x to version 5.1 SP1.
  See "Upgrading to SFW HA 5.1 SP1" on page 165.

Upgrading Oracle in a VCS cluster

This section describes the tasks necessary to upgrade Oracle in a VCS cluster.

Note: For information about supported Oracle upgrade paths, refer to your Oracle documentation.

Upgrading the Oracle application

Upgrading Oracle involves the following steps:

- Upgrading the Oracle binaries.
- Upgrading the Oracle database.

Perform the following tasks before upgrading the Oracle database:

- Bring the Oracle service group online.
- Stop HAD using the `hastop -local -force` command.

Additional tasks after upgrading Oracle

Perform the following tasks to configure Oracle in a VCS environment:

- Associate the updated database with the listener for Oracle 10g.
  See "Associating the updated database with the listener" on page 271.
- Configure the database and listener to use the virtual IP address.
  See "Configuring the database and listener to use the virtual IP address" on page 272.
- Configure Oracle and listener services.
  See "Configuring Oracle and listener services" on page 275.
- Modify the ServiceName attribute for the Netlsnr resource.
  See "Modifying the ServiceName attribute for the netlsnr resource" on page 276.

Associating the updated database with the listener

The following procedures describe how to associate databases with listeners.

Prerequisites to associate databases with listeners

Ensure that the initialization parameter file contains the following entries:

- SERVICE_NAMES (the name of the database service)
- INSTANCE_NAME (the name of the database instance)

These parameters are created during installation or database creation.

Associate the database with the listener

The following procedure associates the database with the listener.

To associate the database with the listener

1. Use one of the following procedures to configure the new attribute listener_alias:

   Run the following SQL command:

   ```
   SQL> ALTER SYSTEM SET LOCAL_LISTENER='<listener_alias>' scope=spfile;
   ```

   OR

   Add the following entry to the initialization parameter file (pfile or spfile):

   ```
   LOCAL_LISTENER = <listener_alias>
   ```

2. Define the parameter listener_alias. If your Oracle configuration uses the file tnsnames.ora, edit the file as instructed below. The default location of tnsnames.ora is `%ORACLE_HOME%\NETWORK\ADMIN`.

   Add the following to tnsnames.ora file:

   ```
   <listener_alias>=
   (DESCRIPTION =
   (ADDRESS=(Protocol=TCP)(HOST=virtual_IP_address)(Port=1521))
   )
   ```

3. Stop and restart the database.

   The listener_alias parameter gets appended by the default domain name that is specified in the file sqlnet.ora.

Configuring the database and listener to use the virtual IP address

All databases and listeners configured must use the same virtual IP. Update the Oracle files to set the virtual IP address.

Setting the virtual IP address involves the following tasks:

- Creating a virtual IP address.
- Verifying the initialization file settings.
- Updating the Oracle configuration files.
- Restarting the services.

Use the following procedures to configure the Oracle database and listener.

To create a virtual IP address

1. Open the **Network Connections (Start > Settings > Network Connections)**.
2. Right-click the public network connection to be used and click **Properties**.
3. Select **Internet Protocol (TCP/IP)** and click **Properties**.
4. Click **Advanced**.
5. In the **IP Settings** tab, click **Add** to add a virtual IP address and subnet mask.

To verify the initialization file settings, if a PFILE is used

1. Open the Registry Editor.

   From the **Start** menu, choose **Run**. In the **Open** field, enter `regedit` and click **OK**.
2. Double-click the ORA_*SID*_PFILE registry key at HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME_*ID*\.

   The variable *SID* represents the database instance.
3. Verify that the Value data field specifies the correct path at which the initialization file, `init.ora`, is located.

To verify the initialization file settings, if an SPFILE is used

1. Run sqlplus.exe.
2. Connect to the database.
3. Verify the following query returns the correct path of the SPFILE.

```
select value from v$parameter where name = 'spfile'
```

To update the Oracle configuration files

1. In the listener.ora and tnsnames.ora files, change the host name for all the TCP protocol address databases to the virtual IP address that you created.

   Replace

   ```
   HOSTNAME=machine_name
   ```

   with

   ```
   HOSTNAME=virtual_IP_address
   ```

2. In the initialization file, change the dispatchers parameter.

   Oracle requires an initialization file, a PFILE or an SPFILE, to start database instances. Choose the appropriate reference depending on the initialization file you use.

   See "Setting the dispatchers parameter in PFILE" on page 274.

   See "Setting the dispatchers parameter in SPFILE" on page 274.

3. Restart the Oracle and listener services.

Setting the dispatchers parameter in PFILE

In the PFILE, set the host name for all TCP protocol address dispatchers to the virtual IP address that you created.

Edit the dispatchers parameter only for the host name and leave the rest of the configuration as it is. Set the value as:

```
dispatchers = '(ADDRESS = (Protocol=TCP)(HOST=virtual_IP_address)
(any other previously existing entry))'
```

The variable *virtual_IP_address* represents the virtual IP address that you created.

For example:

```
dispatchers = '(ADDRESS = (Protocol=TCP)(HOST=10.210.100.110)(SERVICE=Data1XDB)'
```

Setting the dispatchers parameter in SPFILE

Use the following steps to set the dispatchers parameter in SPFILE.

To set the dispatchers parameter in SPFILE

1. Convert the SPFILE to PFILE.
2. Modify the PFILE.

   See "Setting the dispatchers parameter in PFILE" on page 274.
3. Convert the PFILE to SPFILE.
4. Save the SPFILE to the original location on the shared disk.

   Refer to the Oracle documentation for specific information on converting a PFILE or an SPFILE.

Configuring Oracle and listener services

Configuring the Oracle and Listener services involves the following tasks:

- Making the Oracle and Netlsnr services manual.
- Configuring log on properties for Oracle services.

Use the following procedures to configure Oracle and listener services.

To make services manual

1. Open the **Services** applet (**Start > Programs > Administrative Tools > Services**).
2. Double-click the service. In the SCM, the following appears:
   - Oracle services appear as OracleService*SID*, where *SID* represents the database instance.
   - Listener services appear as Oracle*Ora_Home*TNS*ListenerName*, where *Ora_Home* represents the Oracle home directory and *ListenerName* is the name of the listener set during the installation.
3. In the **Properties** window, click the **General** tab.
4. From the **Startup Type** drop-down list, select **Manual**.
5. Click **OK**.

To configure the log on properties for oracle services

1. Open the **Services** applet (**Start > Programs > Administrative Tools > Services**).
2. Double-click the Oracle service. In the SCM, the names of Oracle services appear as OracleService*SID*, where *SID* represents the database instance.
3. In the **General** tab of the **Properties** window, click **Stop** to stop the service.
4. Click the **Log On** tab.

5 Choose **This Account**.

6 Enter the credentials of the user in whose context Oracle was installed.

7 Click the **General** tab and click **Start** to start the service with the new Log On properties. Click **OK**.

Modifying the ServiceName attribute for the netlsnr resource

Perform the following steps to modify the ServiceName attribute for the Netlsnr resource.

To modify the ServiceName attribute

1 Start HAD. Type the following on the command prompt:

```
C:\> hastart
```

2 Offline the Netlsnr resource. Type the following on the command prompt:

```
C:\> hares -offline resource_name -sys system_name
```

3 Modify the ServiceName attribute for the Netlsnr resource. Type the following on the command prompt:

```
C:\> hares -modify resource_name attribute_name attribute_value
```

For example, to modify the ServiceName attribute of the Netlsnr resource, Netlsnr_res, type:

```
C:\> hares -modify Netlsnr_res ServiceName attribute_value
```

where, *attribute_value* is the name of the listener service in Oracle 9i or 10g versions.

4 Online the Netlsnr resource. Type the following on the command prompt:

```
C:\> hares -online resource_name -sys system_name
```

Appendix A

Services and ports used by SFW HA

This appendix includes the following topics:

- About SFW HA services and ports

About SFW HA services and ports

If you have configured the Windows firewall, then ensure that the firewall settings allow access to the services or ports used by SFW HA.

Table A-1 displays the services and ports used by SFW HA .

Note: The following port numbers that appear in bold are mandatory for configuring SFW HA: 2148, 14150, 14141, and 7419.

Table A-1 SFW HA services and ports

Port Number	Protocol	Description	Process
2148, 3207	TCP/UDP	Veritas Enterprise Administrator (VEA) Server 2148 (TCP) 3207 (UDP)	vxsvc.exe
14150	TCP	Veritas Command Server	cmdServer.exe

Table A-1 SFW HA services and ports *(continued)*

Port Number	Protocol	Description	Process
14141	TCP	Veritas High Availability Engine Veritas Cluster Manager (Java console) (ClusterManager.exe) VCS Agent driver (VCSAgDriver.exe)	had.exe
7419	TCP	Symantec Plugin Host Service Solutions Configuration Center (SFWConfigPanel.exe) CCF Engine (CEngineDriver.exe)	pluginHost.exe
1556	TCP/UDP	Symantec Private Branch Exchange	pbx_exchange.exe
2821	TCP/UDP	Symantec Product Authentication Service (VxSS)	vxatd.exe
8199	TCP	Volume Replicator Administrative Service	vras.dll
8989	TCP	VVR Resync Utility	vxreserver.exe
4145	UDP	VVR Connection Server VCS Cluster Heartbeats	vxio.sys
4888	TCP	Veritas Scheduler Service Use to launch the configured schedule.	VxSchedService.exe
49152-65535	TCP/UDP	Volume Replicator Packets	User configurable ports created at kernel level by vxio .sys file
8443	TCP	VCS Secure Web Server	vrtsweb.exe
14144	TCP/UDP	VCS Notification	Notifier.exe
14153, 15550 - 15558	TCP/UDP	VCS Cluster Simulator	hasim.exe
14155	TCP/UDP	VCS Global Cluster Option (GCO)	wac.exe
8181/ 8443/ 14151	TCP/UDP	VRTS Web Administration	vrtsweb.exe

Table A-1 SFW HA services and ports *(continued)*

Port Number	Protocol	Description	Process
5634	HTTPS	Veritas Storage Foundation Messaging Service	xprtld.exe
14145 14994 14443	TCP/UDP	Veritas Cluster Server Management Console Web Server MS port: 14145 Sybase ASA port: 14994 HTTPS Web Server: 14443 For information about the Veritas Cluster Server Management Console and ports, see the *Veritas™ Cluster Server Management Console Implementation Guide.*	cmcweb.exe

Index

V