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

Windows Server 2008 (x64), Windows Server 2008 R2 (x64)

6.0.1

September 2012

Symantec

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

Product version: 6.0.1

Document version: 6.0.1 Rev 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 support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Documentation

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:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Contents

Chapter 1

Preinstallation and planning

This chapter includes the following topics:

About the preinstallation and planning tasks

Before installing SFW or SFW HA, you must perform the following tasks, as a part of product installation planning.

- Review the release notes for your product
- Review the product installation requirements
- Review the supported hardware and software list
- Review the licensing details
- Review the specific requirements for your configuration
- Perform the applicable pre-requisite tasks
- For latest updates refer to the Late Breaking News (LBN)

http://www.symantec.com/docs/TECH161556

- Exit all running applications

Installation requirements

Review the following product installation requirements for your systems.

For the latest information on requirements for this release, see the following Symantec Technical Support TechNote:

http://www.symantec.com/docs/TECH152806

Operating system requirements

The server and client components of the software run on specific Windows operating systems. For information about the supported Windows operating systems, refer to the following:

- Supported operating systems for SFW and SFW HA servers
  See "Supported operating systems for server components" on page 12.
- Supported operating systems for SFW and SFW HA clients
  See "Supported operating systems for client components" on page 13.

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

http://www.symantec.com/docs/TECH153742

Supported operating systems for server components

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

Note: SFW software for servers supports Hyper-V and parent partitions.

However, SFW HA software for servers does not support Hyper-V and parent partitions.

Table 1-1 Supported operating systems for servers

Windows Server	Platform	Edition	Version
Windows 2008 Server Core	x64		RTM or SP2
Windows 2008 R2 Server Core	x64		RTM or SP1

Table 1-1 Supported operating systems for servers *(continued)*

Windows Server	Platform	Edition	Version
Windows Server 2008	x64	Standard, Enterprise, Datacenter	RTM or SP2
Windows Web Server 2008	x64		RTM or SP2
Windows Server 2008 R2	x64	Standard, Enterprise, Datacenter	RTM or SP1
Windows Web Server 2008 R2	x64		RTM or SP1
Windows Storage Server 2008	x64		
Windows Storage Server 2008 R2	x64		
Windows Small Business Server 2008	x64	Standard, Premium	
Windows Small Business Server 2011	x64	Standard, Premium	

Note: Installation of SFW HA server components in VMWare environment is supported only on Windows Server 2008 (x64), Windows Server 2008 R2 (x64), Windows 2008 Server Core (x64), and Windows 2008 R2 Server Core (x64).

Supported operating systems for client components

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

- Any one of the operating system versions, editions, and architectures that the Server Components are supported on except Server Core:
  See "Supported operating systems for server components" on page 12.
- Windows XP x86 (SP3 required), x64 (SP2 required)
- Windows Vista x86, x64: Ultimate Edition, Business Edition, Premium Edition (SP1 or SP2 required)
- Windows 7 x86, x64: Professional Edition, Ultimate Edition (RTM or SP1 required)

Supported VMware versions

The following VMware Servers and management clients are currently supported:

- VMware ESX Support

In this release, VMware ESX 3.0 or higher is required for installing and configuring SFW or SFW HA on VMware virtual machines.

- VMware Workstation support
  In this release, VMware Workstation 6.5 is required for running SFW or SFW HA on VMware virtual machines.

Disk space requirements

For installation, space required is calculated regardless of selected options or components.

Table 1-2 summarizes approximate disk space requirements for SFW and SFW HA systems.

Table 1-2 Disk space requirements

Installation options	Required disk space
SFW + all options	1124 MB
SFW Client components	632 MB
SFW HA + all options	1589 MB
SFW HA Client components	916 MB

Hardware requirements

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

http://www.symantec.com/docs/TECH152806

Table 1-3 displays the required hardware requirements.

Table 1-3 Hardware requirements

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

Table 1-3 Hardware requirements *(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
Display	Minimum resolution: 1024 X 768 pixels or higher VCS Cluster Manager (Java Console) requires an 8-bit (256 colors) display and a graphics card that can render 2D images
System requirements	If you are installing DMP as an option, ensure that you have at least two IO paths from the server to the storage array for load balancing to happen.

Firewall port settings and anti-spyware

Before installing the product software, disable spyware monitoring and removal software. This must be done only as pre-installation requirement and should be re-enabled immediately after installation.

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

See "About SFW HA services and ports" on page 149.

General requirements

The following are additional requirements that apply for SFW and SFW HA installation.

Table 1-4 lists the additional requirements for installing SFW and SFW HA.

Table 1-4 General requirements for SFW and SFW HA

Requirement	Description
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://www.symantec.com/docs/TECH152806 **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*.
Static IP address	VVR requires a static IP for replication and clustering. If you are installing the VVR option, make sure the system has at least one IP address configured that is not assigned by Dynamic Host Configuration Protocol (DHCP).

Permission requirements for SFW

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

Note: Ensure that local administrative privileges are granted to you or to the group to which you directly belong.

SFW HA requirements

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

Before you install SFW HA, 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://www.symantec.com/docs/TECH152806
- For the Software Compatibility List:
  http://www.symantec.com/docs/TECH153742

System requirements for SFW HA

The following system requirements must be met:

- 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*.

- 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. Use the second NIC exclusively for private network communication between the nodes of the cluster.
  Route each private NIC through a separate hub or switch to avoid single points of failure.
- For installing SFW HA, 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.

Network requirements for SFW HA

SFW HA has the following network requirements:

- Do not install SFW HA on servers that are assigned the role of a Domain Controller. Configuring a cluster on a domain controller is not supported.
- Ensure that your firewall settings allow access to ports used by SFW HA wizards and services. For a detailed list of services and ports used by SFW HA:

See "About SFW HA services and ports" on page 149.

- Static IP addresses are required for certain purposes when configuring high availability or disaster recovery solutions. For IPv4 networks, ensure that you have the addresses available to enter. For IPv6 networks, ensure that the network advertises the prefix so that addresses are autogenerated. Static IP addresses are required for the following purposes:
  - A minimum of one static IP address for each physical node in the cluster.
  - One static IP address per site for each application virtual server.
  - One static IP address per cluster used when configuring the Notification or Global Cluster option. The same IP address may be used for all options.
  - VVR requires a static IP for replication and clustering. If you are installing the VVR option, make sure the system has at least one IP address configured that is not assigned by Dynamic Host Configuration Protocol (DHCP).
  - 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.
- For IPv6 networks, SFW HA supports the following:

IP address configuration	Global unicast addresses are supported. Global unicast addresses are equivalent to public IPv4 addresses. Unique local unicast addresses are supported. Multicast and anycast addresses are not supported. Link local and site local addresses are not supported.
IP address configuration	Only stateless automatic configuration is supported. In stateless mode, the IP address is configured automatically based on router advertisements. The prefix must be advertised. Mixed mode configuration with stateful and stateless configurations are not allowed. DHCPv6 is not used for assignment of IP addresses. Manual configuration is not supported.

Transition technologies	The other types of automatic configuration (stateful or "both") are not supported. DHCPv6 is not used for assignment of IP addresses. Manual configuration is not supported.
LLT over UDP	LLT over UDP is supported on both IPv4 and IPv6.
VCS agents, wizards, and other components	VCS agents that require an IP address attribute and wizards that configure or discover IP addresses now support IPv6 addresses (of the type described above).

- In an IPv6 environment, the Lanman agent relies on the DNS records to validate the virtual server name on the network. If the virtual servers configured in the cluster use IPv6 addresses, you must specify the DNS server IP, either in the network adapter settings or in the Lanman agent's AdditionalDNSServers attribute.
- Verify that you have set the Dynamic Update option for the DNS server to Secure Only.
- 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*.
- If Network Basic Input/Output System (NetBIOS) is disabled over the TCP/IP, then you must set the Lanman agent's DNSUpdateRequired attribute to 1 (True).
- 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.

Permission requirements for SFW HA

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.

DMP DSM requirements

Review the following requirements if you plan to install DMP DSM as an option while installing SFW or SFW HA.

- Ensure 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.
- Install the correct hardware drivers for the DMP DSMs.
  Refer to your hardware documentation for detailed information about hardware drivers.
- 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.
- Ensure that no other third-party DSMs are installed for the same array you want to use.
  A DMP DSM cannot be installed together with a third-party DSM for the same array. Only one DSM at a time can claim the LUNs in an array. According to Microsoft Multipath I/O (MPIO) documentation, if multiple DSMs are installed, the Microsoft MPIO framework contacts each DSM to determine which is appropriate to handle a device. There is no particular order in which the MPIO framework contacts the DSMs. The first DSM to claim ownership of the device

is associated with that device. Other DSMs cannot claim an already claimed device. Therefore, to ensure that the DMP DSM claims the LUNs of an array, no other DSM should be installed for that same array.

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.

Setting up access rights

This task is applicable if you plan to install DMPW as an option.

DMPW uses the standard Microsoft Windows administrative privileges which govern the access rights of users to the DMPW servers and services.

The following services are associated with the product:

- Veritas Enterprise Administrator service (vxsvc)
- Veritas Installer Service (vxinstaller) used during installation
- Windows Management Instrumentation (WMI) service for DMPW functionality

By default, administrators have the right to load and unload device drivers and install and uninstall the Veritas Dynamic Multi-Pathing for Windows. For accessing and using the program you must have administrative rights.

As an administrator, you need to grant these same administrative privileges to other users. For example, you can grant these rights in the Local Users and Groups function under Windows Server 2008 Administrative Tools.

For details refer to the Microsoft Windows Server documentation.

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

Choosing the load balancing settings

For environments where DMP DSMs are used, 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 settings, 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*.

Supported applications

This section provides the details on the supported applications and their versions.

Supported Exchange Server 2007 versions

Table 1-5 lists the Microsoft Exchange 2007 versions supported in this release of SFW HA.

Table 1-5 Microsoft Exchange Server 2007 supported environments

Microsoft Exchange Server 2007	Windows Servers
Microsoft Exchange Server 2007 SP1, SP2, or SP3 Standard or Enterprise Edition (Mailbox server role required)	■ Windows Server 2008 x64 Editions (for AMD64 or Intel EM64T): Standard, Enterprise, or Datacenter Edition ■ Windows Server 2008 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 Web Edition ■ Windows Server 2008 x64 on all current editions and architectures Symantec currently supports (SP2 required)

Supported Exchange Server 2010 versions

Table 1-6 lists the Microsoft Exchange Server 2010 versions supported in this release of SFW HA.

Table 1-6 Microsoft Exchange Server 2010 supported environments

Microsoft Exchange Server 2010	Windows Servers
Microsoft Exchange Server 2010 RTM, SP1, or SP2 Standard or Enterprise Edition (Mailbox server role required)	■ Windows Server 2008 x64 with SP2: Standard or Enterprise Edition ■ Windows Server 2008 R2 on Standard or Enterprise Edition

Supported SQL Server 2005 versions

Table 1-7 lists the Microsoft SQL Server 2005 versions supported with this release of SFW HA.

Table 1-7 Microsoft SQL Server 2005 supported environments

SQL Server 2005	Windows Servers
Microsoft SQL Server 2005 SP2, SP3, or SP4 32-bit Standard or Enterprise Edition	■ Windows Server 2008 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 Web Edition ■ Windows Server 2008 x64 on all current editions Symantec currently supports (SP2 required)
Microsoft SQL Server 2005 SP1, SP2, SP3, or SP4 64-bit Standard or Enterprise Edition	■ Windows Server 2008 x64 (for AMD64 or Intel EM64T): Standard, Enterprise, or Datacenter Edition ■ Windows Server 2008 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 Web Edition ■ Windows Server 2008 x64 on all current editions Symantec currently supports (SP2 required) ■ Windows Storage Server 2008

Supported SQL Server 2008 and 2008 R2 versions

Table 1-8 lists the Microsoft SQL Server 2008 versions supported with this release of SFW HA.

Table 1-8 Supported Microsoft SQL Server 2008 versions

SQL Server 2008	Windows Servers
Microsoft SQL Server 2008 SP1, SP2, and SP3 32-bit Standard , Enterprise, or Web Edition	■ Windows Server 2008 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 Web Edition ■ Windows Server 2008 x64 on all current editions Symantec currently supports (SP2 required)
Microsoft SQL Server 2008 SP1, SP2, and SP3 64-bit Standard, Enterprise, Enterprise Web Edition	■ Windows Server 2008 x64 Editions (for AMD64 or Intel EM64T): Standard, Enterprise, or Datacenter Edition ■ Windows Server 2008 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 Web Edition ■ Windows Server 2008 x64 on all current editions Symantec currently supports (SP2 required)

Table 1-9 lists the Microsoft SQL Server 2008 R2 versions supported with this release of SFW HA.

Table 1-9 Supported Microsoft SQL Server 2008 R2 versions

SQL Server 2008 R2	Windows Servers
Microsoft SQL Server 2008 R2 RTM and SP1 32-bit Standard, Enterprise, or Datacenter Edition	■ Windows Server 2008 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 Web Edition ■ Windows Server 2008 x64 on all current editions Symantec currently supports (SP2 required)

Table 1-9 Supported Microsoft SQL Server 2008 R2 versions *(continued)*

SQL Server 2008 R2	Windows Servers
Microsoft SQL Server 2008 R2 RTM and SP1 64-bit Standard, Enterprise, Datacenter Edition	■ Windows Server 2008 x64 (for AMD64 or Intel EM64T): Standard, Enterprise, or Datacenter Edition ■ Windows Server 2008 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 Web Edition ■ Windows Server 2008 x64 on all current editions Symantec currently supports (SP2 required)

Supported SQL Server 2012 versions

Table 1-10 lists the Microsoft SQL Server 2012 versions supported with this release of SFW HA

Table 1-10 Supported Microsoft SQL Server 2012 versions

SQL Server 2012	Windows Servers
Microsoft SQL Server 2012 32-bit / 64-bit Standard, Business Intelligence, Enterprise, or Web Edition	■ Windows Server 2008 x64 (for AMD64 or Intel EM64T): Standard, Enterprise, or Datacenter Edition ■ Windows Server 2008 R2 SP1 without Hyper-V on Standard, Enterprise, Datacenter editions ■ Windows Server 2008 R2 SP1 on Standard, Enterprise, Datacenter editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 SP1 Web Edition ■ Windows Server 2008 x64 on all current editions and architectures Symantec currently supports (SP2 required)

Table 1-10 Supported Microsoft SQL Server 2012 versions *(continued)*

SQL Server 2012	Windows Servers
Microsoft SQL Server 2012 64-bit Standard, Business Intelligence, Enterprise, or Enterprise Web Edition	■ Windows Server 2008 R2 SP1 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 SP1 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 SP1 Web Edition ■ Windows Server 2008 x64 on all current editions and architectures Symantec currently supports (SP2 required)

Supported Oracle versions

Table 1-11 lists the Oracle versions supported with this release of SFW HA.

Table 1-11 Supported Oracle environments

Oracle versions	Windows Servers
Oracle 10g Release 2 (10.2.0.4) Standard Edition, Enterprise Edition	■ Windows Server 2008 (64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)
Oracle 11g, Release 1 (11.1.0.7.0)	■ Windows Server 2008 (64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)
Oracle 11g R2	■ Windows Server 2008 (64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2008 R2 (64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition

Supported SharePoint Server versions

Table 1-12 lists the SharePoint versions supported with this release of SFW HA.

Table 1-12 Supported SharePoint versions

SharePoint versions	Windows Servers
Microsoft SharePoint Server 2007 (SP1 required) (x64) bit Standard Edition or Enterprise Edition	Windows Server 2008 (x64) Standard, Enterprise, Data Center, or Web Server with Service Pack 2 or later Windows Server 2008 R2 (x64) Standard, Enterprise, Data Center, or Web Server with SP1
Microsoft SharePoint Server 2010 (x64) bit Standard Edition or Enterprise Edition	Windows Server 2008 (x64) Standard, Enterprise, Data Center, or Web Server with Service Pack 2 or later Windows Server 2008 R2 (x64) Standard, Enterprise, Data Center, or Web Server with SP1

Supported Enterprise Vault and Blackberry Enterprise Server versions

This section lists the Enterprise Vault and Blackberry Enterprise Server versions supported with this release of SFW HA.

- Enterprise Vault 8.0 SP1, SP2, and SP3
- Enterprise Vault 9.0
- BlackBerry Enterprise Server (BES) 4.1.5

Verifying the system configuration using the Windows Data Collector

It is recommended to verify your system configuration before you begin to install the product. The Windows data collector enables you to gather information about the systems in your network. It thus helps you verify your system configuration before you begin with the product installation.

Installing the Windows Data Collector

To install and run the Windows data collector, your PC must be running at a minimum Windows 2000 SP4.

You can download the data collector using the product software disc or from the Symantec Operations Readiness Tools (SORT) Web site.

- To download the data collector using the product software disc, insert the product software disc into your system drive and double-click **setup.exe**.

This launches the CD Browser.
Click **Windows Data Collector** and extract all the files on to your system.

- To download the Windows data collector from the SORT Web site,
  - Go to the Symantec Operations Readiness Tools (SORT) Web site: https://sort.symantec.com
  - Under the SORT tab, select **My SORT**.
  - On the Custom Reports widget, follow the instructions to download the data collector.

Running the verification reports

The data collector uses the gathered information to generate the reports that enable you to perform the following:

- Determine whether a system is ready to install or upgrade to this release of SFW or SFW HA.
- Analyze the configuration of your current Symantec products and make recommendations about availability, use, performance, and best practices.
- Get detailed information about your installed Symantec products, versions, and licenses.

The report contains a list of passed and failed checks and details about each of them. After the Windows data collector completes the check, you can save a summary report as an HTML file and an XML file.

For more details on running a verification report, refer to the platform-specific README file located on the Custom Reports widget on the SORT Web site.

Licensing

SFW and SFW HA are available in the following editions:

- Standard
- Enterprise
- HA DR Standard
- HA DR Enterprise

The available product options are based on the edition you choose.

Table 1-13 provides the product options available per SFW or SFW HA license edition.

Table 1-13 License edition and available product options

Product	License edition	Features available			
		FlashSnap	Microsoft Failover Cluster	Fast Failover	GCO
SFW	Enterprise	✓	✓	Not applicable	Not applicable
SFW	Standard	Not available	Not available	Not applicable	Not applicable
SFW HA	Enterprise	✓	Not applicable	✓	Not available
SFW HA	Standard	Not available	Not applicable	Not available	Not available
SFW HA	HA DR Enterprise	✓	Not applicable	✓	✓
SFW HA	HA DR Standard	Not available	Not applicable	Not available	✓

Note: VVR is available as a separate licensed feature. To avail the VVR functionality, you must purchase the license separately.

Each of the license edition is further categorized based on the operating system edition. Depending on the operating system edition in use, you can choose a compatible product license edition.

Table 1-14 provides the compatibility matrix for the product license edition and the Windows operating system in use.

Table 1-14 Compatibility matrix with the Windows operating system

Windows operating system edition	Compatible SFW or SFW HA edition	SFW or SFW HA licensing terms
■ Server Edition ■ Standard Edition ■ Web Edition	■ Standard edition for standard, enterprise, and datacenter operating system ■ Enterprise edition for standard, enterprise, and datacenter operating system ■ HA DR standard for standard, enterprise, and datacenter operating system ■ HA DR enterprise for standard, enterprise, and datacenter operating system	A separate license is required for each virtual or physical server, where the software is installed.
■ Advanced Edition ■ Enterprise Edition	■ Standard edition for enterprise, and datacenter operating system ■ Enterprise edition for enterprise, and datacenter operating system ■ HA DR standard for enterprise, and datacenter operating system ■ HA DR enterprise for enterprise, and datacenter operating system	For each license, you may run one instance on a physical server and up to four simultaneous instances on virtual servers located on that physical server.

Table 1-14 Compatibility matrix with the Windows operating system *(continued)*

Windows operating system edition	Compatible SFW or SFW HA edition	SFW or SFW HA licensing terms
Datacenter Edition	■ Standard edition for datacenter operating system ■ Enterprise edition for datacenter operating system ■ HA DR standard for datacenter operating system ■ HA DR enterprise datacenter operating system	For each license, you may run one instance on one physical server and an unlimited instances on virtual servers located on that physical server.

During installation, the product installer provides the following options to specify the license details.

- Keyless
- User Entered Key

Note: Evaluation licenses are now deprecated.

A keyless license installs the embedded keys and allows you to use all the available product options listed in Table 1-13.

You can use the keyless license for 60 days. If you install the product using the keyless option, a message is logged everyday in the Event Viewer indicating that you must perform any one of the following tasks, within 60 days of product installation. Failing this, a non-compliance error is logged every four hours.

- Add the system as a managed host to a Veritas Operations Manager (VOM) Management Server.
  For more details, refer to the VOM documentation.
- Add an appropriate and valid license key on this system using the Symantec product installer from Windows Add/Remove Programs.

In case of an User Entered Key license, you must procure an appropriate license key from the Symantec license certificate and portal. The user entered license allows you to use the product options based on the license key you enter.

https://licensing.symantec.com/

The product installer enables you to switch from a keyless license to a user entered license and vice-a-versa. It thus helps you to overcome the issues faced while removing the left-over temporary keys.

Licensing notes

Review the following licensing notes before you install or upgrade the product.

- If you are installing the product for the first time, the "Keyless" option is available by default.
- If you are upgrading the product, the "User Entered Key" option is available by default. The wizard retrieves all the license keys installed earlier. If you choose to use the 5.x license keys, only the product options available for the entered keys are selected and allowed for installation.

  For example, you cannot install Fast Failover and Hyper-V DR options using the 5.x license keys. To install these options you must specify a 6.0 base license key.
- During the product upgrade, you can choose to change the license option to keyless. After changing the license option to keyless, you can install all the available product options.
- You cannot install the 6.0 base license key over the 5.x base license key. However, you can install the 6.0 feature key over the 5.x base key.
- You can perform the following cross product upgrades. During upgrade, the wizard provides the Keyless option by default.
  - SFW 6.0.1 to SFW HA 6.0.1
  - DMP 6.0.1 to SFW or SFW HA 6.0.1
  - VCS 6.0.1 to SFW HA 6.0.1
- While repairing the product installation, licenses can be managed only if "Keyless" license option was selected during the installation. You cannot manage the licenses, if the license option selected was "User Entered Key".

  To manage the licenses in case of "User Entered Key" option, you must use the Windows Add/Remove Programs.

  While managing the licenses, you can change the license option from Keyless to User Entered or vice a versa.
- If you are installing SFW Basic, a basic license key is installed by default. Keyless option is not available in case of SFW Basic installation. Using the Windows Add/Remove Programs you can change the option to Keyless or User Entered Key. If you choose the Keyless option, the product installation changes

to SFW. After selecting the Keyless option, you cannot revert back to SFW Basic.

- You must configure Veritas Operations Manager (VOM) within two months of product installation. Failing this, a warning message for non compliance is displayed periodically.
  For more details on configuring VOM, refer to VOM product documentation.
- You can install new licenses or remove the existing licenses using the product installer.
  If you remove all the licenses, the vxsvc service fails to start and the service recovery options are changed to “Take No Action”. To start the service you must enter the licenses and then manually start the service or change the service recovery option to “Restart the Service”.

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

Planning an SFW basic or SFW installation

Review the following recommendations if you plan to set up a Microsoft cluster (MSCS) or Microsoft failover cluster with SFW or SFW Basic.

- Microsoft clustering is configured on all the systems where you want to install SFW or SFW Basic. This enables SFW to install Microsoft cluster resources such as Volume Manager disk groups and various other shared resources.
- Since SFW or SFW Basic installation requires a reboot, install the product on the inactive nodes of the cluster first, then use the Move Group command in Microsoft clustering to move the active node. Subsequently, install the product on the remaining nodes.

  For additional information about planning an SFW or SFW Basic installation with a Microsoft cluster, refer to the *Veritas Storage Foundation Administrator's Guide*.

Planning a SFW HA installation

Review the following pre-installation tasks that you must perform, if you plan to set up a SFW HA cluster.

Unconfiguring the MSCS or Microsoft Failover Cluster

Verify if MSCS or Microsoft Failover Cluster is configured on the systems where you want to install SFW HA. If MSCS or Microsoft Failover Cluster is configured, you must unconfigure the same before you proceed to install SFW HA.

Refer to Microsoft documentation for details on unconfiguring the MSCS or Microsoft Failover Cluster.

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 installation.

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

Enable the Computer Browser Service on your Windows Server 2008 (x64) systems before installing SFW HA.

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 your product installation, on a Windows Server 2008 server.

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

Upgrading the Microsoft Windows operating system

While you plan to install the product, you may want to upgrade your Windows operating system to one of the supported operating system. Symantec recommends performing the Windows upgrade before installing SFW HA.

See "Operating system requirements" on page 12.

In some circumstances though, you may need to install SFW HA before upgrading your Windows operating system.

If you install SFW or SFW HA before upgrading your Windows Server 2008 operating system, you must run the SFW utility called FixVDSKey.bat and then repair your installation, after you complete the Windows Server 2008 R2 or SP2 upgrade. The SFW utility restarts the Storage Agent (VxVM) and VDSservices.

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

See "Repairing the SFW HA installation" on page 70.

Chapter 2

Installing SFW or SFW HA

This chapter includes the following topics:

About installing SFW Basic

To install SFW Basic you must download the installation package from the following location:

https://fileconnect.symantec.com

SFW Basic follows the install and uninstall process similar to that of SFW HA.

- For information about installing SFW Basic
  See "About installing SFW or SFW HA" on page 37.
- For information about uninstalling SFW Basic
  See "About uninstalling SFW or SFW HA" on page 73.

About installing SFW or SFW HA

This section describes the process for a new installation of SFW or SFW HA.

You can perform the installation using either the product installer wizard or the command line interface (CLI).

Note: If you are installing SFW HA in a VMware environment, it is recommended to first install the Symantec High Availability Console and then install VCS.

As part of the Console installation, the installer registers the Symantec High Availability plugin for VMware vCenter Server. This plugin enables integration of Symantec High Availability with VMware vSphere Client and adds the following options to the VMware vSphere Client:

- Menu to install the Symantec High Availability guest components

- Symantec High Availability home page

- Symantec High Availability tab

- Symantec High Availability dashboard

For details, refer to the *Symantec High Availability Solution for VMware* Guide.

Before you begin to install the product, ensure that you have reviewed and performed the required preinstallation and planning tasks.

Note: If the VOM Managed Host components of any version earlier to 5.0 are installed in your environment, then the guest components installer upgrades these components to its latest version.

During the installation you can choose to separately install the server components or the client components.

If you choose to install the server components, the following options are installed by default:

Client components	In case of SFW this installs the VEA Java GUI on the same nodes where the server components are installed. In case of SFW HA this installs the VCS Java Console on the same nodes where the server components are installed.

High Availability Hardware Replication Agents (Applicable in case of SFW HA)	■ Veritas Cluster Server Hardware Replication Agent for EMC MirrorView Enables VCS to manage MirrorView replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for EMC SRDF Enables VCS to manage SRDF replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for EMC SRDFSTAR Enables VCS to manage SRDFSTAR replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for Hitachi TrueCopy Enables VCS to manage TrueCopy replicated devices.
High Availability Application Agents (Applicable in case of SFW HA)	■ Veritas Cluster Server Application Agent for Exchange 2007 ■ Veritas Cluster Server Database Agent for Exchange 2010 ■ Veritas Cluster Server Application Agent for SharePoint Server 2010
High Availability Database Agents (Applicable in case of SFW HA)	■ Veritas Cluster Server Database Agent for SQL This installs the VCS agent for both, SQL Server 2005 and SQL Server 2008 ■ Veritas Cluster Server Database Agent for Oracle
VRTSvbs package	Enables you to add the system as a managed host to the Virtual Business Services. For more details about configuring Virtual Business Services, refer to *Virtual Business Services User's Guide*

Note: The high availability agents that get installed with the product software are also available in the form of an agent pack. The agent pack is released on a quarterly basis. The agent pack includes support for new applications as well as fixes and enhancements to existing agents. You can install the agent pack on an existing SFW HA installation.

Refer to the Symantec Operations Readiness Tools (SORT) Web site for information on the latest agent pack availability.

https://sort.symantec.com

Refer to the agent-specific configuration guide for more details about the application agents.

To install the server or client components, using the product installer,

See "Installing the SFW HA server components using the product installer" on page 40.

See "Installing the SFW HA client components using the product installer" on page 53.

To install the server or client components, using the CLI,

See "Installing SFW HA server or client components using CLI" on page 57.

Installing the SFW HA server components using the product installer

The Symantec product installer enables you to install the server components for the following products:

- Veritas Storage Foundation for Windows (SFW)
- Veritas Storage Foundation and High Availability Solutions for Windows (SFW HA)
- Dynamic Multi-Pathing (DMP) for Windows
- Veritas Cluster Server for Windows

Note: To install SFW Basic you must download the installation package from the following location:

https://fileconnect.symantec.com

For installing DMP or Veritas Cluster Server for Windows refer to the respective installation guide.

The steps in this section are based on SFW HA installation. The steps for an SFW installation are similar.

Perform the following steps to install SFW HA server components

1. Insert the software disc containing the installation package into your system's disc drive or download the installation package from the following location:

   https://fileconnect.symantec.com

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

   The CD browser appears.

Note: If you are installing the software using the product software disc, the CD browser displays the installation options for all the products specified earlier. However, if you are downloading the installation package from the Symantec website, the CD browser displays the installation options only for the product to be installed.

---

3 Click to download the required contents.

Note: The client components are installed by default along with the server components. However, on a server core machine, the client components will not be installed.

Veritas Storage Foundation and High Availability Solutions 6.0.1	Click to install the server components for Storage Foundation and High Availability Solution for Windows.
Veritas Storage Foundation 6.0.1	Click to install the server components for Storage Foundation for Windows.
Late Breaking News	Click to access the latest information about updates, patches, and software issues regarding this release.
Windows Data Collector	Click to verify that your configuration meets all pertinent software and hardware requirements.
SORT	Click to access the Symantec Operations Readiness Tools site. In addition to the product download you can also download the custom reports about your computer and Symantec enterprise products, a checklist providing configuration recommendations, and system and patch requirements to install or upgrade your software.
Browse Contents	Click to view the software disc contents.
Technical Support	Click to contact Symantec Technical Support.

4 On the Welcome panel, review the list of prerequisites and click **Next**.

Note that the **Check for product updates** check box is selected by default. The product installer searches for the available product updates on the SORT website. You can then download and apply the available updates. If you do not want to apply the available patches, clear the selection of **Check for product updates** check box.

5 On the License panel, read the license terms, select **I accept the terms of License Agreement**, and then click **Next**.

The **Participate in the Symantec Product Improvement Program by submitting system and usage information anonymously** check box is selected by default. The Product Improvement Program allows the product installer to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, clear the selection of the check box.

6 On the Product Updates panel, review the list of available product updates.

This panel appears only if you have selected the **Check for product updates** check box on the Welcome panel.

The product updates comprise of the pre-installation patches, post-installation patches, High Availability Agents, and Array-Specific Modules. The panel lists the available pre-installation patches and the post-installation patches. Download and apply the pre-installation patches in the sequence shown in the table and rerun the wizard. After the successful installation of the product, apply the post-installation patches. Also download and install the High Availability Agents and Array-Specific Modules from the SORT website.

7 On the System Selection panel, select the systems and the desired Installation and Product options:

You can select the systems in one of the following ways:

- In the System Name or IP text box, manually type the system name or its IP address and click **Add**.

  Note: The wizard does not support the internet protocol version 6. To add the systems having internet protocol version 6, you must type the system name.

  The local host is populated by default.

- Alternatively, browse to select the systems.
  The systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click **OK**.

Once you add or select a system, the wizard performs certain validation checks and notes the details in the Verification Details box. To review the details, select the desired system.

To select the installation and product options, perform the following tasks on each of the selected system.

Note: To apply the selection to multiple systems, select the system for which you have selected the installation and product options and then click **Apply to multiple systems**.

See "Applying the selected installation and product options to multiple systems" on page 52.

- By default the wizard uses %ProgramFiles%\Veritas as the installation directory. To customize the installation directory, click **Browse** and select the desired location. Click **OK**.
  Install the product at the same location on all the cluster nodes.
  The installation directory is selected by default on the systems where the product is being upgraded.

  Note: If you plan to configure the cluster for single sign-on authentication, the installation directory must contain only English characters.

  In case your system runs a non-English locale operating system, ensure that the installation directory contains only English characters.

- Select the required license type from the **License key** drop-down list.

  Note: The default license type is "Keyless".

  If you select the "Keyless" license type, all the available product options are displayed and are selected by default.
  If you select "User entered license key" as your license type, the License Details panel appears by default. On the License Details panel, enter the license key and then click **Add**. You can add multiple licenses for the various product options you want to use.
  The wizard validates the entered license keys and displays the relevant error if the validation fails. After the validation is complete, click **OK**.

- From the list of product options, select the options to be installed.
  While you select the options, note the following points:

  - The client components, high availability hardware replication agents, high availability application agents, and the high availability database agents are installed by default.
    For details, See "About installing SFW or SFW HA" on page 37.

- During the upgrade, do not choose to clear the selection for the DSMs you want to remove. Clearing the default selection does not remove the installed DSMs.
  To remove the DSMs, perform any one of the following:
  - Before you begin to upgrade the cluster, remove the required DSM, using the Windows Add Remove Program. Reboot the node and then perform the upgrade.
  - Upgrade the cluster and then use the Add Remove Program to remove the DSM.
  - Upgrade the cluster and then navigate to %ALLUSERSPROFILE%\Veritas\MPIO\. From the command prompt, run the following command:
    `instdsm.exe –u DSMName.inf`

Note: If you clear the default selection during the upgrade, you cannot remove the DSM using the Add Remove Program. To remove the DSM in this case, you must run the command mentioned earlier.

The options differ depending on your product and environment.
The following product options are available for SFW:

Storage Foundation Options	■ Veritas Volume Replicator (VVR) Veritas 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 and application components. FlashSnap supports VSS based snapshots to provide application data in a consistent state after the application is restored. ■ Microsoft Failover Cluster Provides support for Microsoft Failover Cluster. You can select this option even if Microsoft clustering is not currently configured. If you choose to select this option even if Microsoft clustering is not currently configured, you must manually register the VMDg and RVG resource after configuring Microsoft Failover Cluster. ■ Replace Disk Management Snap-in with SFW VEA GUI Replaces 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.

DMP Device Specific Modules (DSMs)	■ 3PARDATA (V3PARAA) ■ Compellent array (VCOMPLNT) ■ Dell EqualLogic array (VEQLOGIC) ■ EMC Clarion (VEMCCLAR) ■ EMC Symmetrix/DMX (VEMCSYMM) ■ EMC VPLEX array (VEMCVPLX) ■ FUJITSU ETERNUS 2000 array (VFUJITSUAA) ■ Hitachi 95xx-AMS-WM (VHDSAP) ■ Hitachi TagmaStore/HP XP (VHDSAA) ■ HP 2000 array (VHPMSA2) ■ HP EVA-MSA (VHPEVA) ■ HUAWEI S5300/S2300 array (VHUAWEIAP) ■ IBM DS AP (VIBMAPDS) ■ IBM DS6000 (VIBMAP) ■ IBM DS4000/SUN 6000 (VENGAP) ■ IBM DS8000/ESS (VIBMAADS) ■ IBM XiV Storage System (VXIV) ■ NETAPP (VNETAPP) ■ NEXSAN SATA/SAS Beast, E60/E18 array (VNEXSAN) ■ PILLAR (VPILLAR) ■ Promise Array (VPROMISE) ■ SUN Array - (VSUN) ■ XioTech Array (VXIOTECH)

Symantec maintains a Hardware Compatibility List (HCL) for Veritas Storage Foundation and High Availability Solutions 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://www.symantec.com/docs/TECH152806

Note: Do not use a DMP DSM together with a third-party DSM for the same array. Only one DSM at a time can claim the LUNs in an array. According to Microsoft Multipath I/O (MPIO) documentation, if multiple DSMs are installed, the Microsoft MPIO framework contacts each DSM to determine which is appropriate to handle a device. There is no particular order in which the MPIO framework contacts the DSMs. The first DSM to claim ownership of the device is associated with that device. Other DSMs cannot claim an already claimed device. Therefore, to ensure that the DMP DSM claims the LUNs of an array, no other DSM should be installed for that same array.

The following are the available options for SFW HA:

Storage Foundation Options

- Veritas Volume Replicator (VVR)
  Veritas 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 and application components. FlashSnap supports VSS based snapshots to provide application data in a consistent state after the application is restored.
- Replace Disk Management Snap-in with SFW VEA GUI
  Replaces 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.

DMP Device Specific Modules (DSMs)	■ 3PARDATA (V3PARAA) ■ Compellent array (VCOMPLNT) ■ Dell EqualLogic array (VEQLOGIC) ■ EMC Clarion (VEMCCLAR) ■ EMC Symmetrix/DMX (VEMCSYMM) ■ EMC VPLEX array (VEMCVPLX) ■ FUJITSU ETERNUS 2000 array (VFUJITSUAA) ■ Hitachi 95xx-AMS-WM (VHDSAP) ■ Hitachi TagmaStore/HP XP (VHDSAA) ■ HP 2000 array (VHPMSA2) ■ HP EVA-MSA (VHPEVA) ■ HUAWEI S5300/S2300 array (VHUAWEIAP) ■ IBM DS AP (VIBMAPDS) ■ IBM DS6000 (VIBMAP) ■ IBM DS4000/SUN 6000 (VENGAP) ■ IBM DS8000/ESS (VIBMAADS) ■ IBM XiV Storage System (VXIV) ■ NETAPP (VNETAPP) ■ NEXSAN SATA/SAS Beast, E60/E18 array (VNEXSAN) ■ PILLAR (VPILLAR) ■ Promise Array (VPROMISE) ■ SUN Array - (VSUN) ■ XioTech Array (VXIOTECH)

Symantec maintains a Hardware Compatibility List (HCL) for Veritas Storage Foundation and High Availability Solutions 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.

http://www.symantec.com/docs/TECH152806

Note: Do not use a DMP DSM together with a third-party DSM for the same array. Only one DSM at a time can claim the LUNs in an array. According to Microsoft Multipath I/O (MPIO) documentation, if multiple DSMs are installed, the Microsoft MPIO framework contacts each DSM to determine which is appropriate to handle a device. There is no particular order in which the MPIO framework contacts the DSMs. The first DSM to claim ownership of the device is associated with that device. Other DSMs cannot claim an already claimed device. Therefore, to ensure that the DMP DSM claims the LUNs of an array, no other DSM should be installed for that same array.

Veritas Cluster Server Options

- Global Cluster Option
  Global Cluster Option (GCO) enables you to link the clusters located in different geographies.
  This provides wide-area failover and disaster recovery.
- Fast Failover
  Fast failover improves the failover time taken by storage resources during the service group failovers, in a clustered environment. Fast failover is particularly noticeable in clusters having multiple storage stacks configured, typically over 20 disk groups and over 150 volumes.

8 On the System Selection panel, click **Next**.

Note that the wizard fails to proceed with the installation, unless all the selected systems have passed the validation checks and are ready for installation. In case the validation checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the installation, select the system and click **Re-verify** to re-initiate the validation checks for this system.

9 On the Pre-install Summary panel, review the summary and click **Next**.

Note that the **Automatically reboot systems after installer completes operation** check box is selected by default. This will reboot all the selected remote systems immediately after the installation is complete on the respective system. If you do not want the wizard to initiate this auto reboot, clear the selection of **Automatically reboot systems after installer completes operation** check box.

10 On the Installation panel, review the progress of installation and click **Next** after the installation is complete.

If an installation is not successful on any of the systems, the status screen shows a failed installation.

Note: During the upgrade, the Installation panel displays a list of services and processes running on the systems. Select a system to view the services and processes running on it and review the list.

The wizard stops the product-specific services and discovers the processes running, if any, on the systems. These processes need to be stopped to proceed with the operation. Click **Next** to forcefully stop the processes and proceed with the operation. Alternatively, you can manually stop the processes. If the services or processes cannot be stopped, the operation fails. Rectify the error and then click **Retry** to validate the affected system again. Click **Retry All** to validate all the systems again.

In case you wish to proceed with the upgrade without stopping a particular process, contact Symantec Technical Support.

---

11 On the Post-install Summary panel, review the installation result and click **Next**.

If the installation has failed on any of the system, refer to the log file for details. You may have to re-install the software.

12 On the Finish panel, click **Finish**.

If you had chosen to initiate the auto reboot, a confirmation message to reboot the local system appears. Click **Yes** to reboot immediately or **No** to reboot later.

In case you had not selected to initiate the auto reboot, ensure that you manually reboot these systems.

This completes the product installation.

If you have installed SFW with Microsoft Failover Cluster, but if Microsoft Failover Cluster is not yet configured, you must register the Volume Manager Disk Group resource after configuring the Microsoft clustering software.

If you have installed VVR, you must also configure the MSCSVVRrvgresource.

See "Registering the resource DLLs" on page 52.

For configuring application service groups refer to the application specific solutions guide. For any administrative tasks to be performed, refer to the *Veritas Storage Foundation Administrator's Guide*.

Applying the selected installation and product options to multiple systems

To apply the selected installation and product options to multiple systems, perform the following steps:

1. Click on any one of the selected system and select the desired installation and product options.
2. Click **Apply to multiple systems**.
3. On the Apply Installation Options panel, select the installation options to be applied and then select the desired systems. Click **OK**.

Note: The installation directory is selected by default on the systems where the product is being upgraded. The selected **Install Directory** option does not apply to these systems.

Registering the resource DLLs

You must perform this task only if you have installed SFW with Microsoft Failover Cluster option, but Microsoft Failover Cluster is not yet configured in your environment.

You must register the following resource DLLs after configuring the Microsoft clustering software.

- Volume Manager Disk Group resource
- MSCSVVRrvgresource resource
  This resource must be added only if you have installed VVR during the SFW installation.

To register the resource DLLs

1. Navigate to c:\windows\cluster folder.
2. From the command prompt run the following command.

   For Volume Manager Disk Group resource:

   ```
   cluster RESTYPE "Volume Manager Disk Group" /CREATE /DLL:vxres.dll
   /TYPE:"Volume Manager Disk Group"
   ```

   For MSCSVVRrvgresource resource

   ```
   Cluster RESTYPE "Replicated Volume Group" /CREATE
   /DLL:mscsrvgresource.dll /TYPE:"Replicated Volume Group"
   ```

Restarting the vxsvc service

If you are installing the Microsoft Failover Clustering feature on a server on which Veritas Storage Foundation for Windows is already installed, then restart Veritas Enterprise Administrator Service (vxsvc) manually.

Issue the following CLI commands to restart the vxsvc service:

- `net stop vxsvc`
- `net start vxsvc`

Installing the SFW HA client components using the product installer

The Symantec product installer enables you to install the client components for the following products:

- Veritas Storage Foundation for Windows (SFW)
- Veritas Storage Foundation and High Availability Solutions for Windows (SFW HA)
- Dynamic Multi-Pathing (DMP) for Windows
- Veritas Cluster Server for Windows

For installing DMP or VCS for Windows refer to the respective installation guide.

Note: Client components cannot be installed on server core systems.

Before you begin with the installation, ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress on the systems where you want to install the client components.

Perform the following steps to install SFW HA client components

1 Insert the software disk containing the installation package into your system's disc drive or download the installation package from the following location:

https://fileconnect.symantec.com

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

The CD browser appears.

3 Click to download the required contents.

Veritas Storage Foundation and High Availability Solutions 6.0.1	Click to install the server or client components for Storage Foundation and High Availability Solution for Windows.
Veritas Storage Foundation 6.0.1	Click to install the server or client components for Storage Foundation for Windows.
Late Breaking News	Click to access the latest information about updates, patches, and software issues regarding this release.
Windows Data Collector	Click to verify that your configuration meets all pertinent software and hardware requirements.
SORT	Click to access the Symantec Operations Readiness Tools site. In addition to the product download you can also download the custom reports about your computer and Symantec enterprise products, a checklist providing configuration recommendations, and system and patch requirements to install or upgrade your software.
Browse Contents	Click to view the software disc contents.
Technical Support	Click to contact Symantec Technical Support.

4 On the Welcome panel, review the list of prerequisites and click **Next**.

Note that the **Check for product updates** check box is selected by default. The wizard searches for the available product updates on the SORT website. You can then download and apply the available updates. If you do not want to apply the available patches, clear the selection of **Check for product updates** check box.

5 On the License Agreement panel, read the license terms, select **I accept the terms of License Agreement**, and then click **Next**.

The **Participate in the Symantec Product Improvement Program by submitting system and usage information anonymously** check box is selected by default. The Product Improvement Program allows the product installer to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, clear the selection of the check box.

6 On the Product Updates panel, review the list of available product updates.

This panel appears only if you have selected the **Check for product updates** check box on the Welcome panel.

The product updates comprise of the pre-installation patches, post-installation patches, High Availability Agents, and Array-Specific Modules. The panel lists the available pre-installation patches and the post-installation patches. Download and apply the pre-installation patches in the sequence shown in the table and rerun the wizard. After the successful installation of the product, apply the post-installation patches. Also download and install the High Availability Agents and Array-Specific Modules from the SORT website.

7 On the System Selection panel, select the systems and the installation directory.

You can select the systems in one of the following ways:

- In the System Name or IP text box, manually type the system name or its IP address and click **Add**.

  Note: The wizard does not support the internet protocol version 6. To add the systems having internet protocol version 6, you must type the system name.

  Local host is populated by default.

- Alternatively, browse to select the systems.
  The systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click **OK**.

Once you add or select a system, the wizard performs certain validation checks and notes the details in the Verification Details box. To review the details, select the desired system.

By default the wizard uses %ProgramFiles%\Veritas as the installation directory. To customize the installation directory, click **Browse** and select the desired location. Click **OK**.

To apply the customized directory to multiple systems, click **Apply to multiple systems**. On the Apply Installation Options panel, select the systems to apply the customized directory. Click **OK**.

The installation directory is selected by default on the systems where the product is being upgraded. The selected **Install Directory** option does not apply to these systems.

Note: If you plan to configure the cluster for single sign-on authentication, the installation directory must contain only English characters. In case your system runs a non-English locale operating system, ensure that the installation directory contains only English characters.

---

8 On the System Selection panel, click **Next**.

Note that the wizard fails to proceed with the installation, unless all the selected systems have passed the validation checks and are ready for installation. In case the validation checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the installation, select the system and click **Re-verify** to re-initiate the validation checks for this system.

9 On the Pre-install Summary panel, review the summary and click **Next**.

10 On the Installation panel, review the progress of installation and click **Next** after the installation is complete.

If an installation is not successful on any of the systems, the status screen shows a failed installation.

Note: During the upgrade, the Installation panel displays a list of services and processes running on the systems. Select a system to view the services and processes running on it and review the list.

The wizard stops the product-specific services and discovers the processes running, if any, on the systems. These processes need to be stopped to proceed with the operation. Click **Next** to forcefully stop the processes and proceed with the operation. Alternatively, you can manually stop the processes. If the services or processes cannot be stopped, the operation fails. Rectify the error and then click **Retry** to validate the affected system again. Click **Retry All** to validate all the systems again.

In case you wish to proceed with the upgrade without stopping a particular process, contact Symantec Technical Support.

---

11 On the Post-install Summary panel, review the installation result and click **Next**.

If the installation has failed on any of the system, refer to the log file for details. You may have to re-install the software.

12 On the Finish panel, click **Finish**.

This completes the installation of the client components.

Installing SFW HA server or client components using CLI

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

During the installation ensure that you verify the following points:

- There are no parallel installations, live updates, or Microsoft Windows updates in progress.
- A third-party DSM is not installed for the array you want to use.
  DMP DSM is not used together with a third-party DSM for the same array. Only one DSM at a time can claim the LUNs in an array. According to Microsoft

Multipath I/O (MPIO) documentation, if multiple DSMs are installed, the Microsoft MPIO framework contacts each DSM to determine which is appropriate to handle a device. There is no particular order in which the MPIO framework contacts the DSMs. The first DSM to claim ownership of the device is associated with that device. Other DSMs cannot claim an already claimed device. Therefore, to ensure that the DMP DSM claims the LUNs of an array, no other DSM should be installed for that same array.

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

To install from the command line

1. If you are installing the package from the software disc, insert the product software disc into your system's drive.
2. Log into a console session.
3. Open a command window by clicking **Start** > **Run**.
4. Enter `cmd` in the Open field and click **OK**.
5. Navigate to the root directory of your software disc.

   If you are downloading the installation software from the Symantec web site, then navigate to the download path where the setup.exe is located.
6. Use the following command syntax to install the product software.

   For example,

```
Setup.exe /s SOLUTIONS="1" INSTALL_MODE=InstallMode
Telemetry=Telemetry
[INSTALLDIR="InstallDirPath"] [REBOOT=RebootMode] [NODE="SysA"]
[LICENSEKEY="LicenseKey"] [OPTIONS="a,b,c,..."]
NoOptionDiscovery= NoOptionDiscovery
GetPatchInfo=GetPatchInfo
```

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

Note: The "Licensekey" parameter is applicable only if you plan to use the "User entered license key" as your license type. You need not specify this parameter for "Keyless" license type.

Parameters for setup.exe

Table 2-1 contains information about the possible parameter values.

Table 2-1 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 Basic or SFW Server Components (includes client components) 2 = SFW HA Server Components (includes client components) 3 = SFW Client Components only 4 = SFW HA Client Components only Example: SOLUTIONS=1
Telemetry	Set this parameter to participate in the Symantec Product Improvement Program by submitting system and usage information anonymously. The Product Improvement Program allows the product installer to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, set this parameter to 0.

Table 2-1 Parameters for setup.exe *(continued)*

Parameter	Use
Install_dir	Set the installation directory path. The path must start and end with a quotation mark. The default setting is SystemDrive: \Program files\Veritas Example: INSTALLDIR="C:\InstallationDirectory" This is an optional parameter. **Note:** If you plan to configure the cluster for single sign-on authentication and your system runs a non-English locale operating system, ensure that the installation directory contains only English characters.
Reboot	Set 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:** This is an optional parameter.
Node	Set the node name. Specify 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="PC177VM-3"
LICENSEKEY	Set the license key for the installation. Enter multiple keys by separating them with a comma (e.g. 123-345-567-789-123, 321-543-765-789-321, etc.) The license key must start and end with a quotation mark ("). LicenseKey has no default setting. Example: LICENSEKEY="123-234-123-234-345" **Note:** This parameter is applicable only if you plan to use the "User entered license key" as your license type. You need not specify this parameter for "Keyless" license type.

Table 2-1 Parameters for setup.exe *(continued)*

Parameter	Use
Options	Set the desired options, if any. The option must start and end with a quotation mark ("). Multiple options can be entered, using a comma as a separator. Options differ depending on your product and environment. There are no default settings. Refer to Table 2-2 for the list of available options. **Note:** During an upgrade, you must specify the previously installed options in the OPTIONS parameter, else they will be uninstalled. To include the previously installed options in this parameter, either specify these options individually in the OPTIONS parameter or specify “Installed” in the OPTIONS parameter to upgrade all options (example: options=”Installed,flashsnap”).
NoOptionDiscovery	Set this parameter to uninstall the previously installed options during an upgrade. Default value is 0. If this parameter is set to 0, the setup discovers the previously installed options which are not specified in the OPTIONS parameter, and the setup exits. Rerun the setup and either include the previously installed options individually in the OPTIONS parameter or specify "Installed" in the OPTIONS parameter. If you set this parameter to 1 during an upgrade, the setup uninstalls the previously installed options which are not specified in the OPTIONS parameter.

Table 2-1 Parameters for setup.exe *(continued)*

Parameter	Use
GetPatchInfo	Set this parameter to search for available product updates. 1 = Lists available updates 0 = Does not list available updates Default value is 1. The product updates comprise of the pre-installation patches, post-installation patches, High Availability Agents, and Array-Specific Modules. If you set this parameter to 1, then the available pre-installation patches and post-installation patches are listed. If any pre-installation patches are available, then the setup exits to let you download and apply the pre-installation patches. Apply the pre-installation patches in the sequence displayed and rerun the setup with GetPatchInfo = 0. After the successful installation of the product, apply the post-installation patches. Also download and install the High-Availability Agents and Array-Specific Modules from the SORT website.

Table 2-2 shows the available options.

Table 2-2 Available options

Option	Description	SFW	SFW HA
Installed	During an upgrade, you can use this option if you do not want to uninstall the previously installed options.	✓	✓
All	You can use this option to install all the available options.	✓	✓
vvr	Volume Replicator (VVR) replicates data across multiple sites for disaster recovery	✓	✓
flashsnap	FlashSnap lets you create and maintain split-mirror, persistent snapshots of volumes	✓	✓

Table 2-2 Available options *(continued)*

Option	Description	SFW	SFW HA
MSCS	Cluster option for Microsoft Failover Cluster You can install this option even if Microsoft clustering is not currently configured. If you choose to install this option even if Microsoft clustering is not currently configured, you must manually register the VMDg resource after configuring Microsoft Failover Cluster. Additionally, if you choose to install VVR, you must also register the RVG resource after configuring Microsoft Failover Cluster. See "Registering the resource DLLs" on page 52.	✓	NA
DISKMGMT	Cluster option for Disk Management Snap-in	✓	✓
V3PARAA	3PARDATA DSM	✓	✓
VCOMPLNT	Compellent array	✓	✓
VEQLOGIC	Dell EqualLogic	✓	✓
VEMCCLAR	EMC Clarion	✓	✓
VEMCSYMM	EMC Symmetrix/DMX	✓	✓
VEMCVPLX	EMC VPLEX array	✓	✓
VFUJITSUAA	FUJITSU ETERNUS 2000 array	✓	✓
VHDSAP	Hitachi 95xx-AMS-WM	✓	✓
VHDSAA	Hitachi TagmaStore/HP XP	✓	✓
VHPMSA2	HP 2000 array	✓	✓
VHPEVA	HP EVA-MSA	✓	✓
VHUAWEIAP	HUAWEI S5300/S2300 array	✓	✓
VIBMAPDS	IBM DS AP	✓	✓
VIBMAP	IBM DS6000	✓	✓
VENGAP	IBM DS4000/Sun 6000	✓	✓
VIBMAADS	IBM DS8000/ESS	✓	✓

Table 2-2 Available options *(continued)*

Option	Description	SFW	SFW HA
VXIV	IBM XiV Storage System	✓	✓
VNETAPP	NETAPP DSM	✓	✓
VNEXSAN	NEXSAN SATA/SAS Beast, E60/E18 array	✓	✓
VPILLAR	PILLAR	✓	✓
VSUN	SUN Array	✓	✓
VXIOTECH	XioTech	✓	✓
GCO	Global Cluster Option (GCO) enables you to link clusters to provide wide-area failover and disaster recovery.	NA	✓
Fast Failover	Fast failover improves the failover time taken by storage resources during the service group failovers, in a clustered environment. Fast failover is particularly noticeable in clusters having multiple storage stacks configured, typically over 20 disk groups and over 150 volumes.	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 TELEMETRY=1
INSTALLDIR="C:\InstallationDirectory" REBOOT=0
```

Silent installation example: SFW server and client

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 TELEMETRY=1
LICENSEKEY="123-234-123-234-345,321-543-765-789-321,321-543-765-789-789"
OPTIONS="MSCS",VVR,DISKMGMT"
INSTALLDIR="C:\InstallationDirectory" REBOOT=1
```

Chapter 3

Administering SFW or SFW HA installation

This chapter includes the following topics:

Adding or removing product options

After installing SFW or SFW HA, you may need to add or remove the product options.

Note the following points before you begin to add or remove the product options:

- You cannot add or remove the product options on a system that runs Server Core operating system. To add or remove the product options on these systems you must uninstall the product and then install it again using the new licenses.
- You can add or remove the product options on the local system only.
- You can add or remove the product options only if you have installed the server components.

Before you choose to add any product option, ensure that you have reviewed and performed the required pre-installation and planning tasks, if any, for the option you want to install.

If you are adding the DMP DSMs to an existing SFW HA or Windows Server Failover Cluster, ensure that you move the resources to another node or take the resource

offline, install the required hardware drivers and then perform the following steps.

To add or remove features

1. Open the Windows Control Panel and click **Programs and Features**.
2. Select the option for the Veritas Storage Foundation.

   For example, for SFW HA select **Veritas Storage Foundation HA 6.0.1 for Windows** and click **Change**.
3. On the **Mode Selection** panel, select **Add or Remove** and then click **Next**.
4. On the System Selection panel, the wizard performs the verification checks and displays the applicable installation and product options. In case the verification checks have failed, review the details and rectify the issue. Before you choose to proceed with the installation click **Re-verify** to re-initiate the verification checks.

   Note that the wizard enables you to proceed only if the verification checks are passed.

   To add or remove the options, select or clear the product option check boxes to add or remove the respective component.

   Note: You can add or remove the features only if you have selected **User entered license key** as your license type. Also, only the options included in your product license, will be enabled for selection. To select any other option, you must first enter the required license details.

   For details on managing your licenses See "Managing SFW HA licenses" on page 67.

   ---

5. On the System Selection panel, click **Next**.

   The wizard performs the verification checks and proceeds to the Pre-install Summary panel.

   Note that the wizard proceeds only if the verification checks are passed.
6. On the Pre-install Summary panel, review the summary and click **Next**.

   Note that the **Automatically reboot systems after installer completes operation** check box is selected by default. This will reboot all the selected remote systems immediately after the installation is complete on the respective system. If you do not want the wizard to initiate this auto reboot, clear the selection of **Automatically reboot systems after installer completes operation** check box.

7 On the Installation panel, review the progress of installation and click **Next** after the installation is complete.

If an installation is not successful, the status screen shows a failed installation. Refer to the Post-install summary for more details. Rectify the issue and then proceed to re-install the component.

8 On the Post-install Summary panel, review the installation result and click **Next**.

If the installation has failed, refer to the log file for details.

9 On the Finish panel, click **Finish**.

If you had chosen to initiate the auto reboot, a confirmation message to reboot the local system appears. Click **Yes** to reboot immediately or **No** to reboot later.

In case you had not selected to initiate the auto reboot, ensure that you manually reboot these systems.

For adding the DMP DSMs, if you had disconnected all but one path, you must reconnect the additional physical path now.

You can now proceed to configure the service groups for the newly added options.

For details, refer to *Veritas Storage Foundation Administrator's Guide*.

Managing SFW HA licenses

After you have installed SFW or SFW HA, you may need to manage the product licenses to add or remove the product options.

You can manage your licenses by performing any of the following tasks:

- Changing the license type that you had selected during the installation.
  You can change the type of license you had selected during the installation.
  For the **Keyless** license type, all the product options are enabled by default. You can choose to clear the options that you do not intend to use.
  For the **User entered license key**, the product options available are based on the licenses you enter.
- Adding or removing the license keys.
  You can add or remove the license keys only if the license type selected is "User entered license key".

Note the following points before you begin to manage the licenses:

- You cannot manage licenses on a system that runs Server Core operating system. To manage licenses on these systems you must uninstall the product and then install it again using the new licenses.
- You can manage the licenses on the local system only.
- You can manage the licenses only if you have installed the server components.

To manage licenses

1. Open the Windows Control Panel and click **Programs and Features**.
2. Select the option for Veritas Storage Foundation.

   For example, for SFW HA select **Veritas Storage Foundation HA 6.0.1 for Windows** and the click **Change**.
3. On the Mode Selection panel, select **Add or Remove** and then click **Next**.
4. On the System Selection panel, the wizard performs the verification checks and displays the applicable installation and product options. In case the verification checks have failed, review the details and rectify the issue. Before you choose to proceed with the installation click **Re-verify** to re-initiate the verification checks.

   Note that the wizard enables you to proceed only if the verification checks are passed.

   To manage the licenses, perform any of the following applicable task:

   - To change the license type, select the required license type from the **License key** drop-down list.
     If you change your license type to "Keyless", all the available product options appear and are selected by default. Clear the selection for the product options that you do not intend to use and then proceed through step 7.
     If you change your license type to "User entered license key", the License Details panel appears by default. Proceed through step 5 to add the license keys.
   - To add or remove the licenses, click **Edit**.
5. On the License Details panel, enter the license key and then click **Add**.

   Repeat the step to add multiple licenses for the various product options you want to use.

   The wizard validates the entered license keys and displays the relevant error if the validation fails.

6 On the License Details panel, click **OK**.

The wizard displays the applicable installation and product options on the System Selection panel.

7 On the System Selection panel, select or clear the required product options and then click **Next**.

The wizard performs the verification checks and proceeds to the Pre-install Summary panel. In case the verification checks have failed, review the details and rectify the issue. Before you choose to proceed with the installation click **Re-verify** to re-initiate the verification checks.

Note that the wizard proceeds only if the verification checks are passed.

8 On the Pre-install Summary panel, review the summary and click **Next**.

Note that the **Automatically reboot systems after installer completes operation** check box is selected by default. This will reboot all the selected remote systems immediately after the installation is complete on the respective system. If you do not want the wizard to initiate this auto reboot, clear the selection of **Automatically reboot systems after installer completes operation** check box.

9 On the Installation panel, review the progress of installation and click **Next** after the installation is complete.

If an installation is not successful, the status screen shows a failed installation. Refer to the Post-install summary for more details. Rectify the issue and then proceed to re-install the component.

10 On the Post-install Summary panel, review the installation result and click **Next**.

If the installation has failed, refer to the log file for details.

11 On the Finish panel, click **Finish**.

If you had chosen to initiate the auto reboot, a confirmation message to reboot the local system appears. Click **Yes** to reboot immediately or **No** to reboot later.

In case you had not selected to initiate the auto reboot, ensure that you manually reboot these systems.

Note: If you make any changes to the licenses, the changes take effect when the vxsvc service starts again. If remove all the licenses, the vxsvc service fails to start and the service recovery options are changed to “Take No Action”. To start the service you must enter the licenses and then manually start the service and change the service recovery option to “Restart the Service”.

Repairing the SFW HA installation

The product installer can repair an existing installation of the SFW and SFW HA 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.

You can repair the installation only on the local system.

Note: Before you proceed to repair the installation, you must save your configuration to another system and failover the service groups for your applications to another node.

To repair the installation

1. Open the Windows Control Panel and click **Programs and Features**.
2. Select **Veritas Storage Foundation HA 6.0.1 for Windows**.

   If you have installed the client components, select **Veritas Storage Foundation HA 6.0.1 for Windows (Client Components)**.
3. Click **Change**.
4. On the Mode Selection panel, select **Repair**. Click **Next**.
5. On the System Selection panel, installer performs the verification checks. Click **Next** once the status is "Ready for repair".

   In case the verification checks have failed, review the details and rectify the issue. Before you choose to proceed with the installation, click **Re-verify** to re-initiate the verification checks.

   Note: You cannot select the installation and product options.

   ---
6. On the Pre-install Summary panel, review the information and click **Next** to begin the repair process.

   Note that if you are repairing the server installation, the **Automatically reboot systems after installer completes operation** check box is selected by default. This will reboot the node immediately after the repair operation is complete. If you do not want the wizard to initiate this auto reboot, clear the selection of **Automatically reboot systems after installer completes operation** check box.

7 On the Installation panel, review the list of services and processes running on the systems. Select a system to view the services and processes running on it.

The wizard stops the product-specific services and discovers the processes running, if any, on the systems. These processes need to be stopped to proceed with the operation. Click **Next** to forcefully stop the processes and proceed with the operation. Alternatively, you can manually stop the processes.

If the services or processes cannot be stopped, the operation fails. Rectify the error and then click **Retry** to validate the affected system again. Click **Retry All** to validate all the systems again.

8 On the Post-install Summary panel, review the summary and click **Next**.

9 On the Finish panel, click **Finish**.

In case you had not selected to initiate the auto reboot, ensure that you manually reboot the node.

About reinstalling SFW HA

If your product installation has failed due to some reason, you can choose to reinstall it without uninstalling the components that were installed during the failed attempt.

Note: You must reboot your system before you begin to reinstall the product.

To reinstall the product, rectify the cause of failure and then procced with the installation.

See "Installing the SFW HA server components using the product installer" on page 40.

See "Installing the SFW HA client components using the product installer" on page 53.

See "Installing SFW HA server or client components using CLI" on page 57.

If you choose to install the product using the product installer wizard, during the installation a confirmation message is displayed on the System Selection panel. Click **Yes** to proceed with the installation.

Chapter 4

Uninstalling SFW or SFW HA

This chapter includes the following topics:

About uninstalling SFW or SFW HA

You can completely uninstall the product using the product installer wizard or through CLI. However, if you want to uninstall any of the installed product options, you must choose the Add or Remove feature.

Before you uninstall SFW or SFW HA, you must perform the following tasks:

- Verify if the system is a part of a VCS cluster or a SFW configuration for Hyper-V Live Migration support.
  - In case of a SFW configuration, you must launch the SFW Configuration for Hyper-V Live Migration Utility from the Solutions Configuration Center (SCC) and remove the configuration from the system.
  - In case of a VCS cluster, run the VCS Cluster Configuration Wizard (VCW) and remove the node from the cluster.
- If you are running Veritas NetBackup, you must stop the Symantec Private Branch Exchange (PBX) service.

Uninstalling SFW HA using the product installer

The Symantec Product Installer wizard enables you to uninstall the product software. You can simultaneously uninstall the product from multiple remote nodes. To uninstall the product from remote nodes, ensure that the product is installed on the local node.

Uninstalling the Server components, uninstalls the client components and the high availability, replication and the database agents.

The steps in this section are based on a SFW HA uninstallation. The steps for an SFW uninstallation are similar.

To uninstall using the product installer

1. In the Windows Control Panel, select **Programs and Features**.
2. Click **Veritas Storage Foundation HA 6.0.1 for Windows**.

   If you had installed the client components, click **Veritas Storage Foundation HA 6.0.1 for Windows (Client Components)**.
3. Click **Uninstall**.
4. Review the information on the Welcome panel and then click **Next**.
5. On the System Selection panel, add the nodes from which you want to uninstall the product software.

   Note: By default the local system is selected for uninstallation. In case you are performing a remote uninstallation and do not want to uninstall the software from the local system, you must remove the node from the list.

   You can add the nodes in one of the following ways:

   - In the System Name or IP text box, manually type the node name and click **Add**.

     Note: The wizard does not support the internet protocol version 6. To add the systems having internet protocol version 6, you must type the system name.

   - Alternatively, browse to select the nodes.
     The nodes that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more nodes and click the right arrow to move them to the Selected Systems list. Click **OK**. Once you add

or select a node, wizard performs the verification checks and notes the verification details.

6 Click **Next**.

Note that the wizard fails to proceed with the uninstallation, unless all the selected nodes have passed the verification checks and are ready for uninstallation. In case the verification checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the uninstallation click **Re-verify** to re-initiate the verification checks for this node.

7 On the Pre-install Summary panel, review the summary and click **Next**.

Note that the **Automatically reboot systems after installer completes operation** check box is selected by default. This will reboot the remote systems immediately after the installation is complete on the respective system. If you do not want the wizard to initiate this auto reboot, clear the selection of **Automatically reboot systems after installer completes operation** check box.

8 On the Uninstallation panel, review the list of services and processes running on the systems. Select a system to view the services and processes running on it.

The wizard stops the product-specific services and discovers the processes running, if any, on the systems. These processes need to be stopped to proceed with the operation. Click **Next** to forcefully stop the processes and proceed with the operation. Alternatively, you can manually stop the processes.

If the services or processes cannot be stopped, the operation fails. Rectify the error and then click **Retry** to validate the affected system again. Click **Retry All** to validate all the systems again.

9 On the Post-uninstall Summary panel, review the uninstallation results and click **Next**.

If the uninstallation has failed on any of the system, review its summary report and check the log file for details.

10 On the Finish panel, click **Finish**.

In case you had not selected to initiate the auto reboot for the remote nodes, ensure that you manually reboot these nodes.

Uninstalling SFW HA using the command line

You can silently uninstall the product software through the command prompt, using the `VPI.exe` command.

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

```
%Installation Directory%\Veritas Shared\VPI\
{F834E070-8D71-4c4b-B688-06964B88F3E8}\{6.0.1.xxx}\VPI.exe install_mode=5
solutions=1 telemetry=1 reboot=1
```

Table 4-1 displays information about the possible parameter values for uninstalling the 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`
`SOLUTIONS`	Set to the type of uninstallation. *1* = SFW Server (includes client components) *2* = SFW HA Server (includes client components) *3* = SFW Client only *4* = SFW HA Client only The default setting is *1* for SFW Server. Example: `SOLUTIONS=1` Example: SOLUTIONS=1
`TELEMETRY`	Set this parameter to participate in the Symantec Product Improvement Program by submitting system and usage information anonymously. The Product Improvement Program allows the product installer to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, set this parameter to 0.

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

Parameter	Use
REBOOT	Set 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 all components are uninstalled correctly. You do not have to reboot after uninstalling the client.

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

To uninstall from the command prompt

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

```
VPI.exe /s INSTALL_MODE=InstallMode
 SOLUTIONS="1'
Telemetry=Telemetry
[REBOOT=RebootMode ] [NODE="SysA"]
```

Uninstall command examples

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

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

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

```
VPI.exe /s INSTALL_MODE=5 SOLUTIONS=1 TELEMETRY=1 REBOOT=1
```

Chapter 5

Upgrading SFW or SFW HA

This chapter includes the following topics:

Preparing the SFW HA cluster nodes for upgrade

Perform the following tasks before you begin to upgrade your cluster configuration:

Checking the supported minimum product versions

Before upgrading, you must ensure that your systems meets the minimum product version requirement.

Note: While you plan to install the product, you may have to upgrade your Windows operating system to the supported minimum level. Symantec recommends performing the Windows upgrade before upgrading the product.

See "Operating system requirements" on page 12.

Table 5-1 lists the supported upgrade paths.

Table 5-1 Supported upgrade paths

Upgrade from	Upgrade to
SFW 5.1 SFW 5.1 AP1 SFW 5.1 SP1 SFW 5.1 SP1 AP1 SFW 5.1 SP2 SFW 6.0 DMPW 6.0.1 SFW Basic 6.0.1	SFW 6.0.1
SFW HA 5.1 SFW HA 5.1 AP1 SFW HA 5.1 SP1 SFW HA 5.1 SP1 AP1 SFW HA 5.1 SP2 SFW HA 6.0 SFW Basic 6.0.1 SFW 6.0.1 DMPW 6.0.1 VCS for Windows 6.0.1	SFW HA 6.0.1

If your current installation does not meet this minimum required level, 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.

General preparations

Before you begin to upgrade the cluster, perform the following general tasks:

- Back up the configuration and application data.

- Review the licensing details
  See "Licensing" on page 28.
- Ensure that you have reviewed the list of installation requirements and the supported hardware and software details.
  See "Installation requirements" on page 12.
- Ensure that you have performed the applicable pre-installation and planning tasks.
  See "Planning an SFW basic or SFW installation" on page 33.
  See "Planning a SFW HA installation" on page 34.
- Ensure that there are no parallel scheduled snapshots in progress.
- Run the Windows Data Collector or access the SORT website to verify whether the systems in your environment meet the requirements to upgrade the cluster.
- Ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.
- If you are running Veritas NetBackup™ version 6.0 or 6.5 on systems where you are upgrading to SFW HA 6.0.1, then you must shut down the OpsCenterServer service prior to the upgrade. Both NetBackup and SFW HA share the same AT broker and client, and for this reason the OpsCenterServer service must by shut down prior to an upgrade.
- Note that if the VOM Managed Host components of any version earlier to 5.0 are installed in your environment, then the guest components installer upgrades these components to its latest version.

Saving and closing the cluster configuration

Before starting the upgrade process, use the Java Console to "save and close" your configuration. This operation involves saving the latest configuration to disk and changing the configuration state to read-only mode. You must also stop SFW HA before attempting the upgrade process.

To save the cluster configuration, perform one of the following tasks:

- From the 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 backup of custom agent binaries

During the product upgrade a backup of the main.cf and other configuration files is taken. However, it does not take the backup of any agent binaries.

During the upgrade the contents of %VCS_home% folder are removed. This removes the binaries of all the enterprise agents and custom agents that were installed. After the upgrade is complete, all the binaries of enterprise agents are installed again. However, the binaries of a custom agent are not installed again. The main.cf that is restored after the upgrade shows that the custom agent resources are configured, but since the binaries are not present in the %VCS_home% folder you must manually install the custom agents after the upgrade is complete.

Taking the service groups offline

This task is applicable only in case of parallel 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 client applications

If you are running any of the following client applications on the systems where you are upgrading the product, make sure you stop and exit all the application instances.

- Cluster Manager (Java Console)
- Solutions Configuration Center (SCC)
- Veritas Enterprise Administrator (VEA)

Deleting SharepointSearch service group

SFW HA 6.0.1 does not support the SharepointSearch application. If you have SFW HA 6.0 installed with Agent Pack 3 and have configured SharepointSearch application service group, then after upgrading to SFW HA 6.0.1, the SharepointSearch functionality will be lost. If you want to upgrade to SFW HA

6.0.1, manually delete the SharepointSearch service group and proceed with the upgrade.

Exporting the configured rules

If you have configured any rules for event notification messages and actions, you must export them into XML format before you begin with the upgrade.

To export the configured rules

1. From the VEA Control Panel perspective, select the actionagent node in the tree view.
2. Double-click Rule Manager in the right pane.
3. In the Rule Manager window select the rules you want to export.
4. Click **Export**.
5. Save the rules at any temporary location in the XML format.

SFW or SFW HA upgrade notes

Note the following points before you begin with the upgrade:

- During the upgrade, verify the selected installation and product options. All the installed options are selected by default.
  If you do not want to include any of the installed options in the upgraded environment, you must uninstall the same before you proceed with the upgrade. Use the Add Remove feature to uninstall the option.
  If you want to add any additional options, you must select the same.
- While upgrading, 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.
- If you are upgrading in a VVR environment, you must first perform the upgrade at the secondary site. After you have completed the upgrade and the post upgrade tasks at the secondary site, you must fail over the applications from the primary site to the secondary site and then proceed to upgrade the nodes at the primary site. Once the nodes at the primary site are upgraded, you must migrate the applications back.

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.

- If your configuration has DMP configured, then it is recommended to reduce the number of paths to each array to one, before you begin the upgrade.
  For more information about the hardware and software prerequisites for DMP DSM installation, refer to *Veritas™ Dynamic Multi-Pathing for Windows Installation and Upgrade Guide*.
  If you do not have DMP DSMs in your existing environment, but plan to add this feature during the upgrade, add the HBA(host bus adapter) hardware before performing the upgrade. Connect no more than one path from the new HBA to the storage array before the upgrade and DMP DSMs installation. Select the DMP DSM option or the appropriate DMP DSMs while running the installer.
- SFW and SFW HA 6.0 does not provide Dynamic Multi-Pathing support for PROMISE arrays. If currently installed, Dynamic Multi-Pathing support for PROMISE will be removed after the upgrade is complete.
- Upgrading from SFW Basic to SFW does not require any re-installation. Use the Windows Add/Remove Programs to specify a valid SFW license key or choose the keyless license option. In case of User-defined license key, the product options will be available based on the license key you enter.

SFW HA configuration upgrade notes

While upgrading SFW HA configuration, the product installer wizard performs the following tasks:

- Deletes the attributes that are no longer required by SFW HA 6.0.1. For example, the wizard removes the AgentDebug attribute.
- Updates user passwords. Using a different encryption mechanism, SFW HA 6.0.1 decrypts the passwords and re-encrypts them using the SFW HA 6.0.1 encryption mechanism.

Upgrading SFW or SFW Basic in a non-clustered environment

This section describes the tasks to be performed when upgrading SFW.

Table 5-2 lists the tasks to be performed for upgrading SFW in a non-clustered environment

Table 5-2 SFW upgrade tasks in a non-clustered environment

Step	Tasks
1	Review the pre-upgrade tasks to be performed See "Preparing the SFW HA cluster nodes for upgrade" on page 79.
2	Review the upgrade notes See "SFW or SFW HA upgrade notes" on page 83.
3	If your configuration has DMP configured, then it is recommended to reduce the number of paths to each array to one, before you begin the upgrade. For more information about the hardware and software prerequisites for DMP DSM installation, refer to *Veritas™ Dynamic Multi-Pathing for Windows Installation and Upgrade Guide*. If you do not have DMP DSMs in your existing environment, but plan to add this feature during the upgrade, add the HBA(host bus adapter) hardware before performing the upgrade. Connect no more than one path from the new HBA to the storage array before the upgrade and DMP DSMs installation. Select the DMP DSM option or the appropriate DMP DSMs while running the installer.
4	Perform the upgrade steps **Note:** After the upgrade is complete, the installer wizard performs certain cleanup tasks and a command prompt is displayed for certain time. Ignore the prompt and continue with the further tasks. The command prompt closes after the cleanup tasks are complete. Do not close the command prompt before the cleanup tasks are complete. The cleanup tasks are aborted if you close the prompt. In case of VVR environment, first perform the upgrade on the secondary site. No preparations are required on the secondary site. See "Installing SFW HA server or client components using CLI" on page 57.
5	In case of VVR environment, prepare the existing primary site for upgrade See "Preparing the primary site for upgrade- non-clustered SFW environment" on page 86.
6	Upgrade the nodes on the primary site
7	Move the applications back to the original primary site
8	Perform the post-upgrade tasks See "About the tasks after upgrading SFW" on page 103.

Preparing the primary site for upgrade- non-clustered SFW environment

The following procedure must be performed to prepare the nodes on the primary site for the SFW upgrade, in a VVR environment.

Note: Before you prepare the nodes on the primary site, ensure that you have upgraded SFW and performed the post-upgrade tasks, on the secondary site.

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, you can switch the replication settings back to TCP.

You can now proceed to upgrade the nodes.

Upgrading SFW or SFW Basic in a Windows Server Failover Cluster enviroment

This section describes the tasks to be performed to upgrade SFW in a Windows Server Failover Cluster.

You must reboot the system after you upgrade SFW. However, rebooting an active cluster node causes it to fail over. To avoid this, you must first upgrade SFW on an inactive cluster node, switch the active cluster node to a second node, and then upgrade the first node.

In the following example, 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 Failover Cluster console to make Node B the active cluster node after finishing the upgrade.

Table 5-3 lists the tasks to be performed to upgrade SFW in a Windows Server Failover Cluster

Table 5-3 SFW upgrade tasks in a Windows Server Failover Cluster cluster

Step	Tasks
1	Review the pre-upgrade tasks to be performed. See "Preparing the SFW HA cluster nodes for upgrade" on page 79.
2	Review the upgrade notes. See "SFW or SFW HA upgrade notes" on page 83.
3	Prepare the nodes on the existing secondary (DR) site for the upgrade See "Preparing the secondary site for SFW upgrade- Windows Server Failover Cluster environment" on page 89.

Table 5-3 SFW upgrade tasks in a Windows Server Failover Cluster cluster *(continued)*

Step	Tasks
4	If your configuration has DMP configured, then it is recommended to reduce the number of paths to each array to one, before you begin the upgrade. For more information about the hardware and software prerequisites for DMP DSM installation, refer to *Veritas™ Dynamic Multi-Pathing for Windows Installation and Upgrade Guide*. If you do not have DMP DSMs in your existing environment, but plan to add this feature during the upgrade, add the HBA(host bus adapter) hardware before performing the upgrade. Connect no more than one path from the new HBA to the storage array before the upgrade and DMP DSMs installation. Select the DMP DSM option or the appropriate DMP DSMs while running the installer.
5	Perform the upgrade steps on the inactive node (Node A) **Note:** After the upgrade is complete, the installer wizard performs certain cleanup tasks and a command prompt is displayed for certain time. Ignore the prompt and continue with the further tasks. The command prompt closes after the cleanup tasks are complete. Do not close the command prompt before the cleanup tasks are complete. The cleanup tasks are aborted if you close the prompt. See "Installing SFW HA server or client components using CLI" on page 57.
6	Re-enable DMP on Node A, if applicable See "Reconnecting DMP DSM paths after the upgrade" on page 114.
7	Prepare the nodes on the existing primary site for the upgrade See "Preparing the primary site for SFW upgrade- Windows Server Failover Cluster environment" on page 90.
8	Move the active node See "Making Node A the active node" on page 91.
9	Perform task number 4, if applicable
10	Upgrade SFW on Node B **Note:** After the upgrade is complete, the installer wizard performs certain cleanup tasks and a command prompt is displayed for certain time. You can ignore the prompt and continue with the further tasks. The command prompt closes after the cleanup tasks are complete.

Table 5-3 SFW upgrade tasks in a Windows Server Failover Cluster cluster *(continued)*

Step	Tasks
11	Re-enable DMP on Node B, if applicable
12	Re-enable VVR after upgrading all nodes See "Re-enabling VVR in a Windows Server Failover Cluster environment" on page 103.
13	Perform the remaining post-upgrade tasks See "About the tasks after upgrading SFW" on page 103.

Preparing the secondary site for SFW upgrade- Windows Server Failover Cluster environment

The following procedure must be performed to prepare the nodes on the secondary site for the SFW upgrade, in a Windows Server Failover clustered VVR environment.

To prepare the secondary (DR) site

1. Take the RVGresource 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, you can switch the replication settings back to TCP.

You can now proceed to upgrade SFW on all nodes of the secondary site.

Preparing the primary site for SFW upgrade- Windows Server Failover Cluster environment

Once the DR site is upgraded, 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 a Windows Server Failover clustered VVR environment.

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.

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 Failover Cluster 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.

Upgrading SFW HA

This section describes the tasks to be performed while upgrading SFW HA.

You can upgrade the cluster in any one of the following ways:

- Parallel upgrade
  See “About the parallel upgrade” on page 92.
- Rolling upgrade

See "About the rolling upgrades" on page 93.

Before upgrading the SFW HA cluster

Ensure that you perform the following tasks before you upgrade the cluster.

- Review the upgrade notes.
  See "SFW or SFW HA upgrade notes" on page 83.
- If you are upgrading the cluster in a disaster recovery environment, you must stop the replication before you begin to upgrade the cluster nodes.
  See "Preparing the primary and secondary sites for upgrading SFW HA in a VVR environment" on page 96.
- Perform the pre-upgrade tasks.
  See "Preparing the SFW HA cluster nodes for upgrade" on page 79.

About the parallel upgrade

To perform a parallel upgrade you must bring the application service groups offline on all the cluster nodes and then run the product installer to begin the upgrade. This requires a considerable amount of downtime for the clustered applications.

To perform the steps for a parallel upgrade,

See "Installing the SFW HA server components using the product installer" on page 40.

Note: If the cluster is configured for single sign-on authentication, the user account credentials used for authentication will be invalid after the upgrade. After all the nodes are upgraded you must re-configure the cluster for single sign-on authentication.

To re-configure the cluster for single sign-on authentication, run the following command from any one of the cluster nodes:

```
VCWSilent -upgrade
```

You need to run this command only when upgrading from release 5.x to 6.x. This is not required when upgrading from release 6.0 to 6.0.1.

After the upgrade is complete, the installer wizard performs certain cleanup tasks and a command prompt is displayed for certain time. Ignore the prompt and continue with the further tasks. The command prompt closes after the cleanup tasks are complete. Do not close the command prompt before the cleanup tasks are complete. The cleanup tasks are aborted if you close the prompt.

About the rolling upgrades

You can upgrade the server components using the rolling upgrade wizard. Rolling upgrade minimizes the cluster downtime as compared to the parallel upgrade.

Note: You cannot upgrade the client components using the Rolling Upgrade wizard. To upgrade the client components only, use the parallel upgrade method.

See "Installing the SFW HA client components using the product installer" on page 53.

During rolling upgrade, the wizard identifies the passive nodes and the application service group dependency. Depending on this information the wizard generates an upgrade plan, such that the passive nodes are upgraded first. After the passive nodes are upgraded, the service groups failover to these upgraded nodes. The passive nodes now become the active nodes and the active nodes are now the passive nodes. After the service groups failover the wizard upgrades the new passive nodes.

Note: If your cluster configuration has any parallel service groups, you must manually take these service groups offline, before you begin to upgrade the cluster nodes using the rolling upgrade wizard. After the upgrade is complete, you must bring these service groups online.

Upgrading SFW HA using the rolling upgrades

Perform the following steps to upgrade the server components, using the rolling upgrade wizard

1. On any of the system that does not belong to the cluster you want to upgrade, insert the product software disk containing the installation package into your system's disc drive.
2. Allow the autorun feature to start the installation or double-click **Setup.exe**.

   The CD browser appears.
3. Click **Veritas Storage Foundation and High Availability Solutions 6.0.1**.
4. Click **Upgrade Server Components (Rolling Upgrade)**.

5 On the Welcome panel, review the list of prerequisites and click **Next**.

Note that the **Check for product updates** check box is selected by default. The wizard searches for the available product updates on the SORT website. You can then download and apply the available updates. If you do not want to apply the available patches, clear the selection of **Check for product updates** check box.

6 On the License panel, read the license terms, select **I accept the terms of License Agreement**, and then click **Next**.

The **Participate in the Symantec Product Improvement Program by submitting system and usage information anonymously** check box is selected by default. The Product Improvement Program allows the product installer to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, clear the selection of the check box.

7 On the Product Updates panel, review the list of available product updates.

This panel appears only if you have selected the **Check for product updates** check box on the Welcome panel.

The product updates comprise of the pre-installation patches, post-installation patches, High Availability Agents, and Array-Specific Modules. The panel lists the available pre-installation patches and the post-installation patches. Download and apply the pre-installation patches in the sequence shown in the table and rerun the wizard. After the successful installation of the product, apply the post-installation patches. Also download and install the High Availability Agents and Array-Specific Modules from the SORT website

8 On the Cluster Details panel, perform the following tasks:

- In the **Cluster Node host name or IP** text box, specify the node name or IP address of a node that belongs to the cluster you want to upgrade.
- Enter the cluster user account details or select **log-on user credentials** to log-on with the user account credentials of the system on which you are running the wizard.

Note: The wizard ignores the specified details and uses the logged-on user credentials, if the cluster is configured using single sign-on authentication.

The user account must have local administrator privileges on all the cluster nodes. The wizard discovers only those nodes where the user has the required permissions.

Note: To perform a rolling upgrade, the cluster must be configured to use VCS authentication. After you enter the cluster details, the wizard identifies the cluster that you want to upgrade. If you have configured the cluster for single sign-on authentication, the wizard prompts for a confirmation to convert the cluster configuration to use VCS authentication.

After the upgrade is complete, the wizard re-configures the cluster for single sign-on authentication.

9 On the Upgrade Details panel, perform the following tasks:

Note: You must perform these tasks for each cluster node.

- Select the required license type from the **License key** drop-down list.
  If you select the "Keyless" license type, all the available product options are displayed and are selected by default.
  If you select "User entered license key" as your license type, the License Details panel appears by default. On the License Details panel, enter the license key and then click **Add**. You can add multiple licenses for the various product options you want to use.
  The wizard validates the entered license keys and displays the relevant error if the validation fails. After the validation is complete, click **OK**.
- The installed product options are selected by default. Select the additional options to be installed, if any. These options are available depending on your product license.
  You can also choose to clear the default selection for any of the installed option. If you clear the selection, the option is uninstalled.

10 On the Cluster Identification panel, enter a temporary cluster identification number in the **Temporary Cluster ID** text box. The cluster ID value can range in between 0 to 65535.

A virtual cluster is formed using this temporary ID while all the cluster nodes are upgraded.

The wizard restores the original identification number after all the cluster nodes are upgraded.

11 On the Upgrade Plan panel, review the cluster upgrade plan generated by the wizard and then click **Next**.

You can sort the nodes to customize the upgrade sequence. To sort the nodes, select the desired node and change the sequence using the Up and Down arrow and then click **Update Plan**.

Review the new upgrade plan and then click **Next**.

12 On the Installation panel, review the upgrade progress. After the upgrade is complete, click **Finish**.

The wizard displays the status of each upgrade task. If any of the tasks fail, you must rectify the cause and run the wizard again. If the upgrade was successful on any of the cluster node and you have now launched the wizard again to run the installation on the failed nodes, the wizard discovers only the nodes that were not upgraded earlier. It also populates the temporary cluster ID on the Cluster Identification panel. This is the same ID that you had specified during the earlier run.

Note: If your service groups belong to a cluster that is a part of a Virtual Business Service (VBS), the VBS dependencies get deleted during the rolling upgrade of SFW HA. You can recreate the VBS dependencies through the VOM console after the rolling upgrade is complete on all the nodes.

Preparing the primary and secondary sites for upgrading SFW HA in a VVR environment

To upgrade the SFW HA cluster in a VVR environment, you must first stop the replicated volume group (RVG) to detach the replication links and deassociate the replication logs between the primary and secondary site.

Perform the following steps from any one of the cluster node at the primary site

1 Using the Cluster Manager offline the application that uses VVR to replicate data between the sites.

2 From the command prompt run the `vxprint -lVP` command.

3 Verify that the data on the Replicator Log is written to the secondary site and the RLINKSs are up-to-date.

```
vxrlink [-gdiskgroup] status rlink_to_secondary
```

4 Using the Cluster Manager, take the VvrRvg resource offline in the VVR replication service group.

5 Detach the RLINK to prevent VVR from replicating data to the secondary site. From the Veritas Enterprise Administrator console, right-click the secondary RVG and select the **Stop Replication** option to stop VVR from replicating to the secondary site.

6 Disassociate the Replicator Log from the RVG. From the Veritas Enterprise Administrator console, right-click the Replicator Log and select **Dissociate Replicator Log** option from the menu that appears.

Perform the following steps from any one of the cluster node at the secondary site

1 Use Cluster Manager to take the VvrRvg resource offline in the VVR replication service group.

2 From the command prompt run the `vxprint -lVP` command.

3 Disassociate the Replicator Log from the RVG. From the Veritas Enterprise Administrator console, right-click the Replicator Log and select **Dissociate Replicator Log** option from the menu that appears.

Upgrading DMP to SFW or SFW HA

This section describes the tasks to upgrade Veritas Dynamic Multi-Pathing (DMP) to Veritas Storage Foundation for Windows (SFW) or Veritas Storage Foundation and High Availability Solutions for Windows (SFW HA).

You can perform this upgrade only if you have DMP 6.0.1 installed. If your current installation does not meet this minimum required level, you must manually apply the appropriate product upgrades to meet the minimum product level required before proceeding with the installer.

If you have Microsoft Failover Cluster configured, note the following points before you begin to upgrade the cluster nodes:

- To upgrade to SFW, you must first install SFW on the inactive nodes of the cluster. Use the Move Group command in Microsoft Failover Clustering to move the active node and then install SFW on the remaining cluster nodes.
- To upgrade to SFW HA, you must unconfigure the Microsoft cluster and then install SFW HA.

Table 5-4 lists the tasks to be performed for upgrading DMPW to SFW.

Table 5-4 DMPW to SFW upgrade tasks

Step	Tasks
1	Review the pre-upgrade tasks to be performed See "Preparing the SFW HA cluster nodes for upgrade" on page 79.
2	Review the upgrade notes See "SFW or SFW HA upgrade notes" on page 83.
3	Perform the upgrade Select the DMP DSM option or the appropriate DMP DSMs while running the installer.

Upgrading SFW to SFW HA

To upgrade SFW to SFW HA, your system must have SFW version 6.0.1 installed.

If your current installation does not meet this minimum required level, you must manually apply the appropriate product upgrades to meet the minimum product level required before proceeding with the installer.

Table 5-5 lists the tasks to be performed for upgrading SFW to SFW HA.

Table 5-5 SFW to SFW HA upgrade tasks

Step	Tasks
1	Review the pre-upgrade tasks to be performed See "Preparing the SFW HA cluster nodes for upgrade" on page 79.
2	Review the upgrade notes See "SFW or SFW HA upgrade notes" on page 83.
3	If you have configured Microsoft cluster, you must unconfigure the same. Refer to Microsoft documentation for details.

Table 5-5 SFW to SFW HA upgrade tasks *(continued)*

Step	Tasks
4	If your configuration has DMP configured, then it is recommended to reduce the number of paths to each array to one, before you begin the upgrade. For more information about the hardware and software prerequisites for DMP DSM installation, refer to Veritas™ Dynamic Multi-Pathing for Windows Installation and Upgrade Guide. If you do not have DMP DSMs in your existing environment, but plan to add this feature during the upgrade, add the HBA(host bus adapter) hardware before performing the upgrade. Connect no more than one path from the new HBA to the storage array before the upgrade and DMP DSMs installation. Select the DMP DSM option or the appropriate DMP DSMs while running the installer.
5	If VVR is enabled, stop the replication.
6	Perform the upgrade steps See "Installing SFW HA server or client components using CLI" on page 57.
7	Perform the post upgrade tasks See "About the tasks after upgrading SFW HA" on page 109.

Upgrading VCS for Windows to SFW HA

To upgrade VCS for Windows (VCSW) to SFW HA, your system must have VCSW version 6.0.1 installed.

If your current installation does not meet this minimum required level, you must first perform the appropriate upgrades to meet the minimum version level required.

Note the following points before you begin to upgrade VCSW:

- After the upgrade, you will not be able to use the VCS service group configuration wizards to create or modify the service groups with VCS NetApp (NetAppFiler, NetAppSnapDrive, NetAppSnapMirror) or VCS LDM (Mount, DiskRes) storage resource.
  After the upgrade, the VCS service group configuration wizards will support only the MountV and VMDg resources for storage.
  The upgrade does not affect the functioning of such service groups. You can choose to retain those service groups as is. However, for any administrative

tasks after the upgrade, you will have to manually edit these service groups either using the Cluster Manager (Java Console) or the command line.

- While the upgrade does not affect the functioning of the service groups that include NetApp or LDM storage resources, you can choose to delete these service groups and create the service groups that includes MountV and VMDg resources. If you want to delete the service groups that contain NetApp or LDM storage resources, you must use the following process:
  - Take a backup of the application data on all the volumes configured in the service groups.
  - Delete the service groups.
  - Upgrade the cluster to SFW HA.
  - Use VEA to create dynamic cluster disk groups and volumes, as necessary.
  - Copy the backed up application data to the configured volumes.
  - Create the application service groups using the wizards.
  - If you have configured Exchange service group, perform the following changes for each EVS entry in ExchConfig registry key at HKLM\Software\Veritas\VCS\ExchConfig\EVS*EVSName* location:
    - Change the value of “IsRegRepVMDisk” to 1
    - Modify the "RegRepDiskGroupName" to use the diskgroup name
    - Modify the “RegRepVolumeName” registry value to include the volume path
      For example, \Device\HarddiskDmVolumes*DGName**VolumeName*\

Table 5-6 lists the tasks to be performed for upgrading VCSW to SFW HA.

Table 5-6 VCSW to SFW HA upgrade tasks

Step	Task
1	Review the notes mentioned earlier.
2	Review the pre-upgrade tasks to be performed See “Preparing the SFW HA cluster nodes for upgrade” on page 79.
3	Review the upgrade notes See “SFW or SFW HA upgrade notes” on page 83.

Table 5-6 VCSW to SFW HA upgrade tasks *(continued)*

Step	Task
4	If you plan to add the DMP DSMs during the upgrade, you must add the HBA (host bus adapter) hardware before performing the upgrade. Connect no more than one path from the new HBA to the storage array before the upgrade and DMP DSMs installation. Select the DMP DSM option or the appropriate DMP DSMs while running the installer. For more information about the hardware and software prerequisites for DMP DSM installation, refer to *Veritas™ Dynamic Multi-Pathing for Windows Installation and Upgrade Guide*.
5	Perform the upgrade steps See "Installing SFW HA server or client components using CLI" on page 57.
6	Perform the post upgrade steps See "About the tasks after upgrading SFW HA" on page 109.

Chapter 6

Performing the post-upgrade tasks

This chapter includes the following topics:

About the tasks after upgrading SFW

Perform the following tasks after upgrading Storage Foundation for Windows (SFW):

Re-enabling VVR in a Windows Server Failover Cluster environment

In a Microsoft clustered environment after you have completed upgrading SFW on all the cluster nodes, re-enable VVR on the active cluster node.

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

To enable the updated objects on the secondary (DR) site

1. Bring online the Disk Group, IP, and Network Name resource in the Windows Server Failover Cluster 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: Refer to the appropriate Microsoft documentation for details on how to offline and online resources through the command line interface.

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.

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.

In the procedure for preparing the primary site for upgrade, you migrated the primary role to the secondary site.

After both the primary and secondary sites have been upgraded, 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).

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.

Re-configuring the Veritas Scheduler Service

After you upgrade SFW or SFW HA, the Scheduler Service is configured under a "Local System account". If you have configured Automatic Volume Growth settings, you must re-configure the Veritas Scheduler Service under a domain user account having administrator privileges on all the systems.

To re-configure the user account for Veritas Scheduler Service

1 From Windows Computer Management or Windows Administrative Tools, access Services, and select Veritas Scheduler Service.

2 Right-click Veritas Scheduler Service and select Properties from the context menu.

3 Click the Log On tab on the Properties GUI.

4 Select **This Account** and enter the domain user ID and password.

The user account must have administrator privileges on all the systems.

5 Confirm the password and click **Apply**, and then click **OK**.

6 In the Windows Services GUI, restart the Veritas Scheduler Service for the changes to take effect.

Re-configuring the VxSAS service

If you are using Veritas Volume Replicator (VVR) replication, you must re-configure the VxSAS service on all cluster nodes on both the primary and secondary sites.

Note the following pre-requisites to configure the VxSAS service:

- 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.

Importing the configured rules

If you have exported the configured rules for event notification messages and actions, you must import them after the upgrade is complete.

To import the configured rules

1. From the VEA Control Panel perspective, select the server in the left pane.
2. Double-click Rule Manager in the right pane.
3. In the Rule Manager window, click **Import**.
4. Browse to the temporary location and select the XML file that you had saved.

Upgrading the dynamic disk group version

The dynamic disk group version is not upgraded after you upgrade SFW or SFW HA. If a service group in the previous configuration contains a dynamic disk group, you must upgrade its version after you complete the SFW or SFW HA upgrade.

You can upgrade the dynamic disk group, using the Veritas Enterprise Administrator (VEA) console or the CLI.

To upgrade the disk group, using CLI, run the following command. You must run this command for each dynamic disk group separately.

```
vxdg -gDynamicDiskGroupName [-T version] upgrade
```

Where,

DynamicDiskGroupName= Name of the dynamic disk group

version= Target version of the dynamic disk group

After the disk group version is upgraded, run the following command to verify the upgraded version.

```
vxdg -gDynamicDiskGroupName dginfo
```

Perform the following steps to upgrade the dynamic disk group version, using VEA. You must perform these steps for each dynamic disk group separately.

To upgrade the dynamic disk group version, using VEA

1. From the VEA console, right-click the disk group.
2. Select **Upgrade Dynamic Disk Group Version**.

   A notification indicating that the disk group version has been upgraded is seen in the alert logs. You can also verify the disk group properties to confirm the upgraded version.

About the tasks after upgrading SFW HA

Perform the following tasks after upgrading SFW HA:

Bringing the print share service group online after the SFW HA upgrade

Note: You need not perform this task if you are upgrading from 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. Click **Next** on the subsequent wizard panels and complete the wizard steps. You can now bring the printshare service group online.

Including custom resources in the upgraded SFW HA cluster

The VCS Cluster 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 the SFW HA installation, 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 cluster.
5. If resources for a custom resource type are dependent on resources for agents bundled with VCS, 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 Release Notes*.

   For information on the attribute values and descriptions, see the *Veritas Cluster Server Bundled Agents Reference Guide*.
6. 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.
7. Start the VCS engine (HAD) on the node where you changed the configuration. Type the following at the command prompt:

   ```
   C:\> hastart
   ```

8. Start the VCS engine (HAD) on all the other cluster nodes.

Removing the VRTSWebApp resource from the SFW HA cluster configuration

Support for the VCS Cluster Management Console (Single Cluster Mode) is discontinued in 5.1 SP2. The VCS VRTSWebApp agent has been deprecated and is uninstalled during the upgrade. Also, the VCS Cluster Configuration Wizard (VCW) no longer provides the option to configure the Cluster Manager service components.

If VRTSWebApp resource is configured in ClusterService group, after upgrading to 6.0.1 the resource fails to get probed and the ClusterService group fails to come online in the cluster. You must manually delete the VRTSWebApp resource from the ClusterService group. Use the Cluster Manager (Java Console), the command line (`hares -delete`), or the Veritas Operations Manager (VOM) to remove the resource.

Re-enabling VVR in a VCS cluster

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.

Re-configuring the Veritas Scheduler Service

After you upgrade SFW or SFW HA, the Scheduler Service is configured under a "Local System account". If you have configured Automatic Volume Growth settings, you must re-configure the Veritas Scheduler Service under a domain user account having administrator privileges on all the systems.

To re-configure the user account for Veritas Scheduler Service

1. From Windows Computer Management or Windows Administrative Tools, access Services, and select Veritas Scheduler Service.
2. Right-click Veritas Scheduler Service and select Properties from the context menu.
3. Click the Log On tab on the Properties GUI.
4. Select **This Account** and enter the domain user ID and password.

   The user account must have administrator privileges on all the systems.
5. Confirm the password and click **Apply**, and then click **OK**.
6. In the Windows Services GUI, restart the Veritas Scheduler Service for the changes to take effect.

Re-configuring the VxSAS service

If you are using Veritas Volume Replicator (VVR) replication, you must re-configure the VxSAS service on all cluster nodes on both the primary and secondary sites.

Note the following pre-requisites to configure the VxSAS service:

- 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.

Associating the replication logs and starting the replication

You must perform this task, if you have upgraded SFW HA in a VVR environment. Perform the task on any one of the upgraded node.

From the Veritas Enterprise Administrator, right-click the secondary RVG resource and select **Associate Replicator Log** option from the menu that appears. Also, select **Start Replication** option to enable VVR to begin the replication.

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.

Migrating 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**.

Upgrading the dynamic disk group version

The dynamic disk group version is not upgraded after you upgrade SFW or SFW HA. If a service group in the previous configuration contains a dynamic disk group, you must upgrade its version after you complete the SFW or SFW HA upgrade.

You can upgrade the dynamic disk group, using the Veritas Enterprise Administrator (VEA) console or the CLI.

To upgrade the disk group, using CLI, run the following command. You must run this command for each dynamic disk group separately.

```
vxdg -gDynamicDiskGroupName [-T version] upgrade
```

Where,

DynamicDiskGroupName= Name of the dynamic disk group

version= Target version of the dynamic disk group

After the disk group version is upgraded, run the following command to verify the upgraded version.

```
vxdg -gDynamicDiskGroupName dginfo
```

Perform the following steps to upgrade the dynamic disk group version, using VEA. You must perform these steps for each dynamic disk group separately.

To upgrade the dynamic disk group version, using VEA

1. From the VEA console, right-click the disk group.
2. Select **Upgrade Dynamic Disk Group Version**.

   A notification indicating that the disk group version has been upgraded is seen in the alert logs. You can also verify the disk group properties to confirm the upgraded version.

Re-installing the hotfixes

You must perform this task only if you have performed any of the following upgrades:

- DMP 6.0.1 to SFW HA 6.0.1
- DMP 6.0.1 to SFW 6.0.1
- SFW 6.0.1 to SFW HA 6.0.1
- VCSW 6.0.1 to SFW HA 6.0.1

The installer removes all hotfixes installed on the existing version before performing the upgrade. You must thus re-install the hotfixes, after the upgrade is complete.

For the list of hotfixes applicable to SFW HA 6.0.1, refer to the following:

https://sort.symantec.com/patch/matrix

Working with fire drills after upgrading to 6.0.1

In 6.0.1, the fire drill feature has been enhanced to support running DR fire drills for service groups in Veritas Operations Manager (VOM). As part of this enhancement, certain changes were made to the way in which fire drill service groups are configured. When you upgrade to 6.0.1, any existing fire drill service groups are left unchanged.

Also, if your setup contains multiple RVGs configured on a single disk, the corresponding fire drill service groups will no longer work after you upgrade to 6.0.1. For more information, see the *Solutions Guide*.

To successfully perform a DR fire drill using existing service groups after upgrading to 6.0.1:

- In a VVR environment, use the Fire Drill Wizard to delete the fire drill service groups and create corresponding new ones.
  See "Re-creating fire drill service groups in a VVR environment" on page 117.

- In a Hitachi TrueCopy or EMC SRDF environment, edit the dependency link between the fire drill service groups and the corresponding application service groups.
  See "Editing fire drill service groups in a Hitachi TrueCopy or EMC SRDF environment" on page 118.

Re-creating fire drill service groups in a VVR environment

In releases earlier than 6.0.1, fire drill service groups contained a VMDg resource. The Fire Drill Wizard performed certain tasks required to make the storage available for performing a DR fire drill. In 6.0.1, the VVRSnap resource replaces the VMDg resource, and performs some of the tasks that the Fire Drill Wizard previously performed. To successfully perform a DR fire drill after upgrading, you must use the Fire Drill Wizard to delete the existing fire drill service groups and create corresponding new ones.

To re-create a fire drill service group using the Fire Drill Wizard

1. Launch the Fire Drill Wizard, and specify the primary system and application service group.
2. Select the secondary site and the system on which to perform the fire drill.
3. Depending on how RVGs are configured in your existing fire drill service group, the wizard allows you to proceed in one of the following ways:
   - If multiple RVGs are configured on a single disk, the wizard does not allow you to re-create the service group.
     Step through the wizard to delete the service group. The associated snapshots are also deleted.
     To create a new fire drill service group, relaunch the Fire Drill Wizard and perform the fire drill preparation steps.
   - If a single RVG is configured on each disk, the wizard allows you to re-create the service group.
     Step through the wizard to delete the existing service group and re-create it as part of the fire drill preparation steps. The associated snapshots are not deleted in this case.

You can continue using the wizard to test the fire drill service group, or you can close the wizard and perform a fire drill later.

Note: You can now run a fire drill by bringing the service group online, and restore the fire drill configuration by taking the service group offline.

Editing fire drill service groups in a Hitachi TrueCopy or EMC SRDF environment

To successfully perform a fire drill after upgrading to 6.0.1, you must manually edit any existing fire drill service groups.

To edit a fire drill service group

1. Make sure that the fire drill service group is offline.
2. Set the offline-local-firm dependency between the service groups, where the fire drill service group is the parent and the application service group is the child.

Then, test the edited service groups by running fire drills.

Note: You can now run a fire drill by bringing the service group online, and restore the fire drill configuration by taking the service group offline.

Reinstalling the custom agents

After performing the product upgrade, the installer does not upgrade the custom agents installed on the existing version of the product. You must re-install the custom agents, after the upgrade is complete. For more information, see the *Veritas™ Cluster Server Agent Developer's Guide*.

Chapter 7

Application upgrades

This chapter includes the following topics:

About the application upgrades in a SFW HA cluster

This section describes the tasks to be performed if you plan to upgrade your application or its compatible service pack in a SFW HA environment.

Before you begin to upgrade, refer to, the list of supported applications.

See "Supported applications" on page 22.

For application upgrade,

See "Upgrading SQL Server" on page 120.

See "Upgrading Oracle in a SFW HA cluster" on page 129.

For service pack upgrade,

See "Upgrading application service packs in a SFW HA cluster" on page 135.

Note: If you plan to upgrade your applications while you upgrade SFW HA, you must upgrade SFW HA before you begin to upgrade the application.

See "Upgrading SFW HA" on page 91.

Upgrading SQL Server

This section describes the following Microsoft SQL Server upgrade scenarios, in an SFW or SFW HA environment:

SQL Server upgrade scenarios	Refer to
Upgrading from Microsoft SQL Server 2005 to Microsoft SQL Server 2008 or 2008 R2	See "Upgrading from Microsoft SQL Server 2005 to SQL Server 2008 or SQL Server 2008 R2" on page 120.
Upgrading Microsoft SQL Server 2008 or 2008 SP1	See "Upgrading Microsoft SQL Server 2008 or SQL Server 2008 R2 " on page 123.

Note: If you plan to upgrade SQL Server with its compatible service pack

See "Upgrading the SQL Server service packs" on page 140.

Upgrading from Microsoft SQL Server 2005 to SQL Server 2008 or SQL Server 2008 R2

The following steps describe how to upgrade your existing clustered SQL Server 2005 setup to SQL Server 2008 or SQL Server 2008 R2, in a VCS cluster. Complete these steps on all the cluster nodes that are part of the SQL service group, one node at a time.

Note: These steps are applicable only if you already have SQL Server 2005 set up in your cluster environment.

At a high level, upgrading to SQL Server 2008 or 2008 R2 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 Server 2005 service group, including the service group at the DR site, if applicable.

- Create a SQL Server 2008 or SQL Server 2008 R2 service groups, using the SQL Server 2008 Configuration Wizard. In case of a DR setup, create a service group at the secondary site also.

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.

Ensure that you perform the following before the upgrade:

- Take a backup of the SQL databases.
- In case of a Disaster Recovery environment, ensure that the databases on the primary and secondary sites are synchronized and then stop the replication between the sites.
- Ensure that you have installed SFW HA on all the SQL service group cluster nodes that you wish 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. 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 any one of the cluster node on which you want to upgrade SQL Server, take all the SQL Server 2005 service group resources (excluding the storage resources) offline and delete the same.

   If the resources are already offline, bring the storage resources online. To bring the resource online, from the VCS Cluster Manager (Java Console), right-click each of the resource and select **Online**. Click **Yes** in the confirmation pop-up to bring the resource online.

2. Take a backup of the SQL Server 2005 database from the shared disk and store them in a temporary location.

   You will need the backed-up directories while upgrading SQL Server on the additional failover nodes.

3 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.

4 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 node

1 Bring the storage resources online. From the VCS Cluster Manager (Java Console), right-click each of the resource and select **Online**. Click **Yes** in the confirmation pop-up box to bring the resource online.

2 Rename the SQL Server data directories on the shared disks. These directories are updated when SQL Server is installed on the first node. You can also delete these directories, if desired.

3 Copy the backed-up SQL Server 2005 data directories from the temporary location to the shared disks.

   The backed-up directories are the same that you had backed up earlier while upgrading SQL Server on the first cluster node.

4 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.

5 Take the entire service group offline on the node.

Note: If there are no additional nodes for upgrade, you need not offline the service group.

This completes the upgrade steps on the additional failover node. Delete the existing SQL Server 2005 service group and proceed to create SQL Server 2008 or 2008R2 service group in the cluster.

Create SQL Server 2008 or 2008 R2 service group in a SFW HA cluster

To configure the SQL Server 2008 or 2008 R2 service group, run the SQL Server 2008 Configuration Wizard, from the last upgraded node.

Note: In case of a Disaster Recovery setup, repeat these steps on the first cluster node at the secondary site and then reconfigure the DR components.

Refer to the *Veritas Cluster Server Implementation Guide for Microsoft SQL Server 2008* for instructions.

To create the SQL Server 2008 or 2008 R2 service group

1. Rename the Registry (RegRep) directory, if present, on the shared disk.
2. Create the SQL Server 2008 or 2008 R2 service group using the SQL Server 2008 Configuration Wizard.
3. After creating the SQL Server service group, verify the configuration by switching the service group to another node in the cluster.
4. Delete the RegRep directory that you renamed in the first step.

Upgrading Microsoft SQL Server 2008 or SQL Server 2008 R2

The following steps describe how to upgrade SQL Server 2008 or SQL Server 2008 R2 in a SFW HA cluster. Complete these steps on all the cluster nodes that are part of the SQL service group, one node at a time.

Note: These steps are applicable only if you already have SQL Server 2008 or SQL Server 2008 R2 set up in a SFW HA cluster environment.

At a high level, upgrading Microsoft SQL Server 2008 or SQL Server 2008 R2 involves the following tasks:

- Ensure that you have installed SFW HA on all the SQL service group cluster nodes that you wish to upgrade.
- Take a backup of the SQL databases.
- Upgrade SQL Server on the first cluster node.
- Upgrade SQL Server on each additional failover node.
- In case of a Disaster Recovery configuration, ensure that the databases on the primary and secondary sites are synchronized and then proceed to upgrade the cluster.

You can upgrade the cluster using one of the following method:

- Adding a temporary disk and creating the volumes similar to that on the primary site.
  To upgrade the cluster using this method, perform the set of pre-upgrade tasks and then proceed to upgrade the cluster on both the sites. You must follow the same upgrade sequence simultaneously at both sites, upgrade first node and then the additional nodes, as described in the procedures.
  See "Preupgrade tasks for upgrading SQL Server 2008 or 2008 R2 in a disaster recovery environment" on page 124.
- Deleting the SQL Server 2008 or SQL Server 2008 SP1 and then creating the service group for the target version of SQL Server.
  Follow this method only if the data size is small. After you re-create the service groups and setup replication across the two sites, the entire data will be replicated. This involves a considerable amount of time.
  See "Deleting the SQL Server 2008 or 2008 R2 service group and creating the service group for the target version of SQL Server " on page 128.

- Run the SQL Server 2008 configuration wizard in the modify mode, to modify the SQL Server 2008 service group.

Preupgrade tasks for upgrading SQL Server 2008 or 2008 R2 in a disaster recovery environment

Before you proceed to upgrade the cluster nodes in case of a disaster recovery setup, ensure that you perform the following tasks on the secondary site for the SQL instances you want to upgrade.

- Freeze the service group using the VCS Cluster Manager (Java Console).
- Obtain the drive letter on which the system database and the analysis service reside, using the following command:
  `hadiscover -discover SQLServer2008 StartUpParams:`*`INSTANCE2K8`*
  The sample output is similar to the following:

```
<Discovery>
<Attr_Name>
StartUpParams:INSTANCE2K8
</Attr_Name>
<Discover_value>
<Scalar_value>
SQLDataPath: E:\Program Files\Microsoft SQL Server\
MSSQL10.INSTANCE2K8\MSSQL\DATA\
</Scalar_value>
</Discover_value>
```

```
<Discover_value>
<Scalar_value>
SQLErrLogPath: E:\Program Files\Microsoft SQL Server\
MSSQL10.INSTANCE2K8\MSSQL\LOG\ERRORLOG
</Scalar_value>
</Discover_value>
<Discover_value>
<Scalar_value>
OLAPDataPath: E:\Program Files\Microsoft SQL Server\
MSAS10.INSTANCE2K8\OLAP\Data
</Scalar_value>
</Discover_value>
</Discovery>
```

- Attach a temporary disk and create a volume with the drive letter same as that for the instance on which the system database resides.

  Note: If you are upgrading more than one instance having system database path and the OLAP data path on separate volumes, you must complete the upgrade of each instance on both the sites and then proceed to upgrade the next instance.

- Review the SQLDataPath, SQLErrLogPath and the OLAPDataPath directory and create the same on the temporary disk.

  Note: In case the directory path exists on different volumes, ensure that you create similar volumes and then create the required directory paths.

- Copy the following files from the primary site to the data path created on the secondary site.
  - master.mdf
  - mastlog.ldf
  - model.mdf
  - modellog.ldf
  - MSDBData.mdf
  - MSDBLog.ldf
  - tempdb.mdf

- templog.ldf

Upgrading SQL Server 2008 or 2008 R2 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 (excluding the storage resources) offline.

   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.

2. Take a backup of the SQL Server 2008 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.

3. Delete the RegRep resource.

4. Freeze the SQL service group using the VCS Cluster Manager (Java Console).

   From the VCS Cluster Manager (Java Console), right-click the SQL Server service group in tree view on the left pane, and click **Freeze** > **Persistent**.

5. Launch the Microsoft SQL Server installer for the target version of SQL Server, and install SQL Server on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so. Also, ensure that the instance name or id is the same on all the cluster nodes.

   The SQL Server installer then automatically places the SQL data files in the appropriate location.

   Refer to the Microsoft SQL Server documentation for instructions.

6. 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 the first cluster node. Proceed to upgrading SQL on the additional failover nodes.

Upgrading SQL Server 2008 or 2008 R2 on additional failover nodes

Perform the following steps on each additional failover node that is a part of the SQL service group.

To upgrade SQL Server on the additional node

1. Bring the storage resources 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.
2. Delete the original RegRep folder and rename the SQL Server data directories on the shared disks. These directories are updated when the intended version of SQL Server is installed on the first node. You can also delete these directories, if desired.
3. Copy the backed-up SQL Server 2008 databases 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. Freeze the SQL service group.

   From the VCS Cluster Manager (Java Console), right-click the SQL Server service group in tree view on the left pane and click **Freeze** > **Persistent**.
5. Launch the Microsoft SQL Server installer for the version to which the SQL Server is to be upgraded, and install SQL Server 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 installer then automatically places the SQL data files in the appropriate location.

   Refer to the Microsoft SQL Server documentation for instructions.
6. 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.

   Note: If there are no additional nodes for upgrade, you need not offline the service group.

   This completes the upgrade steps on the additional failover node. Proceed to modify the SQL Server service group configuration.

Modifying the SQL Server 2008 service group configuration

From the last upgraded node, run the SQL Server 2008 Configuration Wizard in modify mode to modify the SQL Server 2008 service group configuration.

Note: In case of a Disaster Recovery setup, repeat these steps on the first cluster node at the secondary site and then reconfigure the DR components.

To modify the SQL Server configuration

1. Rename the Registry (RegRep) directory on the shared disk.
2. On the first cluster node, bring the storage resources of the SQL service group, online.
3. Run the SQL Server 2008 wizard in the modify mode and follow the wizard steps.

   When asked for, provide the location for the RegRep resource. This creates a new RegRep for the version of SQL Server to which SQL Server is to be upgraded.

   Refer to *Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008* for detailed instructions on how to create the service group.
4. After modifying the SQL Server service group, verify the configuration by switching the service group to another node in the cluster.
5. Delete the RegRep directory that you renamed in the first step.

Deleting the SQL Server 2008 or 2008 R2 service group and creating the service group for the target version of SQL Server

Perform this task only if you are upgrading SQL Server 2008 or 2008 R2 in the following environment:

- The SFW HA cluster is set up in a disaster recovery environment.
- You have chosen to follow the upgrade by deleting the SQL Server 2008 or 2008 R2 service group and then creating the service group for the target version of SQL Server.

Perform the following tasks, to delete the SQL Server 2008 or 2008 R2 service group and then create the service group for the target version of SQL Server

- Using the VCS Cluster Manager (Java Console), offline and delete the service group for the instance you want to upgrade, on both the sites.
- Stop the replication between the primary and the secondary site.
- For the selected instance mount the created volumes and LUNs on any one of the cluster node, on both the sites.

Note: Ensure that the instance name and id is the same on all the cluster nodes.

- Launch the Microsoft SQL Server installer for the target version and install SQL Server on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so.
- To upgrade the additional nodes, dismount the volumes on the upgraded node and mount them on the node to be upgraded. Launch the SQL Server installer to install target version of SQL Server.
  Repeat this task for each additional node.
- Create the SQL Service group, reconfigure the DR components and then set the required resource dependency.
  For details, refer to *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL* .

Upgrading Oracle in a SFW HA cluster

This section describes the tasks necessary to upgrade Oracle in a SFW HA cluster.

Note: For information about supported Oracle upgrade paths, refer to the Oracle product documentation.

Upgrading the Oracle application in a SFW HA cluster

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.

For details, refer to the Oracle product documentation.

Additional tasks after upgrading Oracle in a SFW HA cluster

Perform the following tasks to configure Oracle in a SFW HA environment:

- Associate the updated database with the listener for Oracle 10g and 11g.
  See "Associating the updated Oracle database with the listener" on page 130.

- Configure the database and listener to use the virtual IP address.
  See "Configuring the Oracle database and listener to use the virtual IP address" on page 131.
- Configure Oracle and listener services.
  See "Configuring Oracle and listener services" on page 134.
- Modify the ServiceName attribute for the Netlsnr resource.
  See "Modifying the ServiceName attribute for the netlsnr resource" on page 134.

Associating the updated Oracle database with the listener

The following procedures describe how to associate oracle databases with listeners:

Prerequisites to associate Oracle 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 Oracle 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 Oracle 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.

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 133.

See "Setting the dispatchers parameter in SPFILE" on page 133.

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 133.

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
```

Upgrading application service packs in a SFW HA cluster

This section describes the tasks to be performed if you plan to upgrade your application to its compatible service pack in a SFW HA environment.

The outlined procedures are applicable only if you already have the application setup in a SFW HA cluster environment.

See "Upgrading the Exchange service packs" on page 136.

See "Upgrading the SQL Server service packs" on page 140.

Note: If you plan to upgrade your applications while you upgrade SFW HA, you must upgrade SFW HA before you begin to upgrade the application.

See "Upgrading SFW HA" on page 91.

Upgrading the Exchange service packs

This section describes how to upgrade Microsoft Exchange servers to their corresponding service packs. The outlined procedures are applicable only if you already have your Exchange setup in a VCS cluster environment.

Exchange Server service pack upgrade scenarios	Refer to
Microsoft Exchange 2007 to 2007 SP3	See "Upgrading Microsoft Exchange Server 2007 to 2007 SP3 in a SFW HA cluster " on page 136.
Microsoft Exchange 2010 to 2010 SP1	See "Upgrading Microsoft Exchange 2010 to Exchange 2010 SP1 in a SFW HA cluster" on page 140.

Upgrading Microsoft Exchange Server 2007 to 2007 SP3 in a SFW HA cluster

This section describes how to upgrade Exchange 2007 to Exchange 2007 SP3, using the Exchange 2007 Upgrade Wizard. It is applicable only if you already have Exchange 2007 set up in a SFW HA cluster environment.

Note: The procedure given below describes how to upgrade Exchange 2007 to Exchange 2007 SP1. This procedure can also be used to upgrade Exchange 2007 SP1 or SP2 to Exchange 2007 SP3.

To configure a new HA and DR environment for Exchange 2007, refer to

Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007.

Before you proceed to upgrade the Exchange Server service pack, 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.

- Ensure that the Exchange database and registry replication files are configured on separate volumes. Configuring the Exchange database and the registry replication files on the same volume may cause data corruption, after you upgrade Exchange with the latest service pack.
  If you fail to configure the Exchange database and the registry replication files on separate volumes, and the data gets corrupt after upgrading Exchange with the latest service pack, perform the following steps as a workaround:
  - Delete or rename the file that could not be restored. Refer to the agent logs for the list of files that could not be restored.
  - Bring the Regrep resource online.

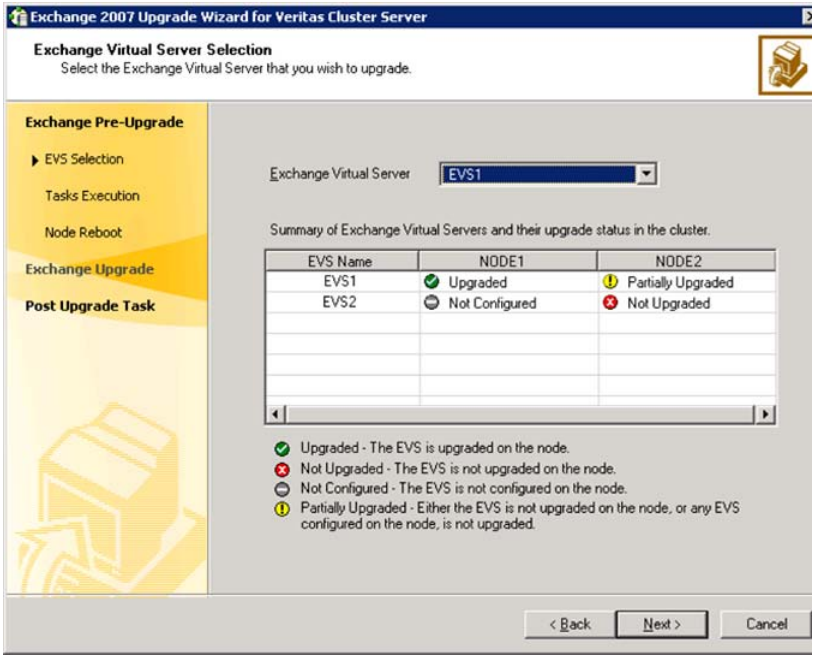
Complete the following steps on all cluster nodes that are part of the Exchange 2007 service group, one node at a time.

To upgrade Exchange 2007 to Exchange 2007 SP3

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.

Upgrading Microsoft Exchange 2010 to Exchange 2010 SP1 in a SFW HA cluster

This section describes how to upgrade Exchange 2010 to Exchange 2010 SP1. It is applicable only if you already have Exchange 2010 setup in a SFW HA cluster environment.

Before you proceed to upgrade the Exchange Server service pack, ensure that you have met the following pre-requisites:

- You have met all the necessary pre-requisites for installing Exchange 2010 SP1 on all the cluster nodes where you are upgrading Exchange.
  For details refer to Microsoft documentation.
- Ensure that you have upgraded SFW HA on all the cluster nodes.

To upgrade Exchange 2010 to Exchange 2010 SP1

1. Using the VCS Cluster Manager (Java Console), bring the Exchange service group online.
2. Stop HAD on all the cluster nodes where you want to upgrade the Exchange installation. At the command prompt, type:

   ```
   hastop -local -force
   ```

3. Launch the Exchange 2010 SP1 installer and install the service pack.

   You can install the service pack parallel on all the nodes, where you are upgrading Exchange. In case of disaster recovery, you can simultaneously upgrade both the sites.

Upgrading the SQL Server service packs

This section describes how to upgrade Microsoft SQL Server to its corresponding service packs. The outlined procedures are applicable only if you already have your SQL Server setup in a VCS cluster environment.

SQL Server service pack upgrade scenarios	Refer to
Microsoft SQL Server 2005 to 2005 SP1	See "Upgrading Microsoft SQL 2005 to 2005 SP1 in a SFW HA cluster environment" on page 141.
Microsoft SQL Server 2005 to 2005 SP2 or later	See "Upgrading Microsoft SQL 2005 to 2005 SP2 or later in a SFW HA cluster environment" on page 142.
Microsoft SQL Server 2008 to 2008 SP1 or 2008 SP2	See "Upgrading SQL Server 2008 or 2008 R2 with the latest service packs in a SFW HA cluster" on page 147.

Upgrading Microsoft SQL 2005 to 2005 SP1 in a SFW HA cluster environment

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 15 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 SFW HA cluster environment

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.

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.

Also, if you are performing the upgrade in a disaster recovery environment you must first upgrade all the cluster nodes at the secondary site and then upgrade the passive nodes at the primary site.

After all the primary site passive nodes are upgraded, you must upgrade the active nodes.

While you upgrade the cluster nodes on the secondary site, you may or may not choose to stop the replication. Replication does not affect the SQL Server upgrade.

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 7-1 lists the configuration objects referenced in the following procedures.

Table 7-1 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 145.

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 144.

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 SQL Server 2008 or 2008 R2 with the latest service packs in a SFW HA cluster

Use this procedure to perform the following upgrades:

- SQL Server 2008 to SQL Server 2008 SP1, SQL Server 2008 SP2, or SQL Server 2008 SP3.
- SQL Server 2008 R2 to SQL Server 2008 R2 SP1

Consider the following points before you proceed to upgrade SQL Server 2008 or 2008 R2 with the latest service packs in a SFW HA environment:

- 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 SFW HA version installed is 5.1 SP2 or later.
- Refer to the Microsoft documentation for prerequisites related to SQL Server 2008 Service Pack installation.

Consider 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.

You can upgrade SQL Server in any of the following ways:

- Upgrade SQL Server on all the nodes parallely
  See "To parallely upgrade SQL Server on all the cluster nodes" on page 147.
- Upgrade SQL Server on the passive node first and then upgrade the active nodes
  See "To upgrade SQL Server on the passive nodes first" on page 148.

Use the following procedure to parallely upgrade SQL Server on all the cluster nodes.

To parallely upgrade SQL Server on all the cluster nodes

1 Freeze (persistent) the service group on Node A (active node).

2 Upgrade the SQL 2008 instance on Node A and Node B.

3 Reboot the nodes.

4 Unfreeze the service group on Node A, if it is still frozen.

Use the following procedure to upgrade SQL Server on the passive node first and subsequently on the active node.

To upgrade SQL Server on the passive nodes first

1. Freeze the service group on Node A (active node).
2. Confirm all SQL services are stopped on Node B.
3. Upgrade the SQL Server 2008 instance on Node B.
4. Reboot node B.
5. Unfreeze the service group on node A.
6. Fail over the service group to Node B.
7. After the service group comes online, freeze the service group on Node B.
8. Confirm all SQL services are stopped on Node A.
9. Upgrade the SQL Server 2008 instance on Node A.
10. Reboot Node A.
11. Unfreeze the service group on node B.
12. Fail back the service group to Node A.

Appendix A

Services and ports used by SFW HA

This appendix includes the following topics:

About SFW HA services and ports

If you have configured a firewall, then ensure that the firewall settings allow access to the services and ports used by SFW HA.

Table A-1 displays the services and ports used by SFW HA .

Note: The port numbers that appear in bold are mandatory for configuring SFW HA.

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
14149	TCP/UDP	VCS Authentication Service	vcsauthserver.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
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
5634	HTTPS	Veritas Storage Foundation Messaging Service	xprtld.exe

Appendix B

About SORT

This appendix includes the following topics:

- About Symantec Operations Readiness Tools

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a Web site that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

Among its broad set of features, SORT lets you do the following:

- Generate server-specific reports that describe how to prepare your servers for installation or upgrade of Symantec enterprise products.
- Access a single site with the latest production information, including patches, agents, and documentation.
- Create automatic email notifications for changes in patches, documentation, and array-specific modules.

To access SORT, go to:

https://sort.symantec.com

Index

U

V