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

Windows 2000, Windows Server 2003

5.0

11293724

symantec™

Veritas Storage Foundation and HA Solutions Installation and Upgrade Guide

Storage Foundation 5.0 for Windows HA

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

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the accompanying release notes.

Windows is a registered trademark of Microsoft Corporation.

Licensing and registration

Storage Foundation for Windows and Storage Foundation HA for Windows are licensed products. See the *Storage Foundation and High Availability Solutions for Windows, Installation and Upgrade Guide* for license installation instructions.

Technical support

For technical assistance, visit http://entsupport.symantec.com and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Section 1 Installation

Chapter 1 SFW and SFW HA Preinstallation and planning

Chapter 2 Installing SFW or SFW HA

Section 2 Upgrading

Chapter 3 Upgrading to SFW 5.0

Section 1

Installation

This section includes the following chapters which describe the procedures used to install Veritas Storage Foundation for Windows 5.0 and Veritas Storage Foundation High Availability for Windows 5.0:

Chapter 1

SFW and SFW HA Preinstallation and planning

This chapter contains:

Prerequisites

Please review the following prerequisites.

- Review the release notes for your products.
- Review the requirements.
  See “Prerequisites” on page 11.
- Exit all running applications.

- VVR needs at least two systems running SFW with VVR support. The two systems, primary and secondary, need a network connection between them. Note that neither system supports DHCP. DHCP-enabled IPs cannot be used for configuring VVR replication. DHCP IPs might be re-assigned to another host, and thus are lost.

Requirements

Review these product installation requirements for your systems before installation. Minimum requirements and Symantec recommended requirements may vary.

Disk space requirements

For normal operation, all installations require an additional 50 MB of disk space. Installation on a non-system drive requires space on both the system drive and the non-system drive.

Table 1-1 summarizes disk space requirements for SFW and SFW HA:

Table 1-1 Disk space requirements

Installation options	Installation on system drive	Installation on non-system drive
SFW + all options + client components	1240 MB	Non-system space: 1240 MB System space: 265 MB
SFW + all options	980 MB	Non-system Space: 980 MB System space: 225 MB
Client components	420 MB	Non-system space: 420 MB System space: 80 MB
SFW HA + all options + client components	1675 MB	Non-system space: 1675 MB System space: 345 MB
SFW HA + all options	1230 MB	Non-system space: 1230 MB System space:285 MB
Client components	630 MB	Non-system space: 630 MB System space: 115 MB
Language Pack	325 MB	Non-system space: 325 MB System space: 90 MB

Operating system requirements

SFW and SFW HA have client and server components that run on specific Windows operating systems.

SFW and SFW HA software for servers

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

- Windows 2000 Server, Advanced Server, or Datacenter Server (all require Service Pack 4 with Update Rollup1)
- Windows Server 2003 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition (SP 1 required for all editions)
- Windows Server 2003 R2 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition
- Windows Server 2003 (32-bit): Web Edition: fully supports SFW and supports only file share for SFW HA (SP 1 required)
- Windows Server 2003 for 64-bit Itanium (IA64): Enterprise Edition or Datacenter Edition (SP 1 required for all editions)
- Windows Server 2003 x64 Editions (for AMD 64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition
- Windows Server 2003 x64 Editions (for AMD 64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition

SFW and SFW HA software for clients

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

- Windows 2000 Server, Advanced Server, or Datacenter Server (all require Service Pack 4 with Update Rollup1)
- Windows Server 2003 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition (SP 1 required for all editions)
- Windows Server 2003 R2 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition
- Windows Server 2003 for 64-bit Itanium (IA64): Enterprise Edition or Datacenter Edition (SP 1 required for all editions)
- Windows Server 2003 for Intel Xeon (EM64T) or AMD Opteron: Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition

- Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition
- Windows XP Professional (SP 2 required)
- Windows 2000 Professional (SP 4 required)

General requirements

Before you install the SFW or SFW HA software, verify that your configuration meets the following criteria and that you have reviewed the SFW 5.0 Hardware Compatibility List to confirm supported hardware:

http://entsupport.symantec.com

Memory

1 GB of RAM required

System processor

Processor requirements are as follows:

32-bit

- 800-megahertz (MHz) Pentium III-compatible or faster processor
- 1GHz or faster processor recommended

x64

- 1GHz AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support processor or faster

IA64

- 1GHz Itanium or faster processor
- 1GHz Dual-Core Intel Itanium 2 or faster processor

Display

Display requirements are as follows:

- Minimum resolution: 800 x 600 pixels
- Recommended resolution: 1024 x 768 pixels or higher

- VCS Cluster Manager (Java and Web Console) requires an 8-bit (256 colors) display and a graphics card that can render 2D images

Storage device compatibility

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

For Veritas Dynamic Multi-pathing and clustering configurations, refer to the Hardware Compatibility List at: http://entsupport.symantec.com to determine the approved hardware for SFW.

Remote systems

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

Veritas Volume Replicator static IP address

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

Single instance of SFW

Only one instance of Veritas Storage Foundation 5.0 for Windows should be running on a system.

Driver signing options

When installing on systems running Windows Server 2003, you must set the Windows driver signing option to ignore software authentication warning messages.

Veritas Cluster Server Cluster Management Console

Veritas Cluster Management Console is supported on the following browsers:

- Microsoft Internet Explorer 6.0 with SP2 or newer
- Firefox 1.5 or newer

Veritas Cluster Management requires the Macromedia Flash Plugin v8.0.

Firewall and anti-spyware

Disable spyware monitoring and removal software before installing SFW or SFW HA. You must also disable the firewall to enable discovery of the local client.

Requirements for Veritas Storage Foundation for Windows (SFW)

Supported software requirement

Veritas Storage Foundation 5.0 for Windows (SFW)

System requirements

System requirements for SFW are as follows:

- SCSI, Fibre Channel, iSCSI host bus adapters (HBAs), or iSCSI Initiator supported NICs to access shared storage
- 1 GB of RAM for each system

Permission requirements

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

Additional requirements

The following requirements must also be met.

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

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 SFW 5.0 Hardware Compatibility List to confirm supported hardware at: http://entsupport.symantec.com

For a Disaster Recovery configuration select the Global Clustering Option and optionally select Veritas Volume Replicator.

Supported software

This section lists the following supported software:

Veritas Storage Foundation HA 5.0 for Windows (SFW HA)

System requirements

Systems must meet the following requirements:

- 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.
- SCSI, Fibre Channel, iSCSI host bus adapters (HBAs), or iSCSI Initiator supported NICs to access shared storage.
- Two NICs: one shared public and private, and one exclusively for the private network. Symantec recommends three NICs.
  See "Best practices" on page 19.
- 1 GB of RAM for each system.
- All servers must run the same operating system, service pack level, and system architecture.

Network requirements

This section lists the following network requirements:

- Install SFW HA on servers in a Windows 2000 or Windows Server 2003 domain.
- Disable the Windows Firewall on systems running Windows Server 2003 SP1.
- Static IP addresses for the following purposes:
  - One static IP address available per site for each application virtual server

  - One IP address for each physical node in the cluster
  - One static IP address per cluster used when configuring the following options: Notification, Cluster Management Console (web console), or Global Cluster Option (VVR only). The same IP address may be used for all options.
  - For VVR only, a minimum of one static IP address per site for each application instance running in the cluster.
- 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 a reverse lookup zone exists in the DNS. Refer to the application documentation for instructions on creating a reverse lookup zone.
- DNS scavenging affects virtual servers configured in VCS because the Lanman agent uses 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*.

Permission requirements

This section lists the following permission requirements:

- You must be a domain user.
- You must be a member of the Local Administrators group for all nodes where you are installing.
- You must have write permissions for the Active Directory objects corresponding to all the nodes.
- If you plan to create a new user account for the VCS Helper service, you must have Domain Administrator privileges or belong to the Account Operators group. If you plan to use an existing user account context for the VCS Helper service, you must know the password for the user account.

Additional requirements

Please review the following additional requirements:

- Installation media for all products and third-party applications
- Licenses for all products and third-party applications
- You must install the operating system in the same path on all systems. For example, if you install Windows 2003 on C:\WINDOWS of one node,

installations on all other nodes must be on C:\WINDOWS. Make sure that the same drive letter is available on all nodes and that the system drive has adequate space for the installation.

Best practices

Symantec recommends that you perform the following tasks:

- Configure Microsoft Exchange Server and Microsoft SQL Server on separate failover nodes within a cluster.
- Verify that you have three network adapters (two NICs exclusively for the private network and one for the public network).

  When using only two NICs, lower the priority of one NIC and use the low-priority NIC for public and private communication.
- Route each private NIC through a separate hub or switch to avoid single points of failure.
- Verify that you have set the Dynamic Update option for the DNS server to Secure Only.

Licensing

The SFW and SFW HA licensing is based on the Microsoft Windows 2000 Server or Windows Server 2003 operating systems in use on a specific server. For each system that runs any of the Symantec products, you need a license.

Note: License keys for release 4.3 or earlier of SFW and SFW HA are not supported in release 5.0 of SFW and SFW HA.

Evaluation license key

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

Storage Foundation for Windows Basic (SFW Basic)

Storage Foundation Basic for Windows (SFW Basic) is a free technology specifically designed for edge-tier workloads. It is a zero cost SFW license and includes the Dynamic Multi-pathing option. An SFW Basic license is required for each physical server and certain limitations apply.

See “SFW Basic” on page 25.

Virtual Server license policy

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

Table 1-2 lists Storage Foundation for Windows(SFW) editions and the additional licensing terms that apply:

Table 1-2 SFW licensing terms

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

Client licensing

You do not need a license if you install the SFW and SFW HA client components.

License management

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

Note: License keys for release 4.3 or earlier of SFW and SFW HA are not supported in release 5.0 of SFW and SFW HA. A default evaluation license key is supplied for your use. This license key is valid for a limited evaluation period only. You must purchase the product to obtain a permanent license key.

Symantec License Inventory Manager

The Symantec License Inventory Manager is an enterprise asset management tracking tool. It determines all the Symantec software products and licenses being used in your network. The Symantec License Inventory Manager is available separately. To order a Symantec License Inventory Manager license and media kit, contact your Symantec sales representative.

See “Configuring the Symantec License Inventory Agent” on page 127.

Vxlicrep

Vxlicrep is a command line tool that generates a report of the licenses in use on your system.

To use Vxlicrep to display a license report:

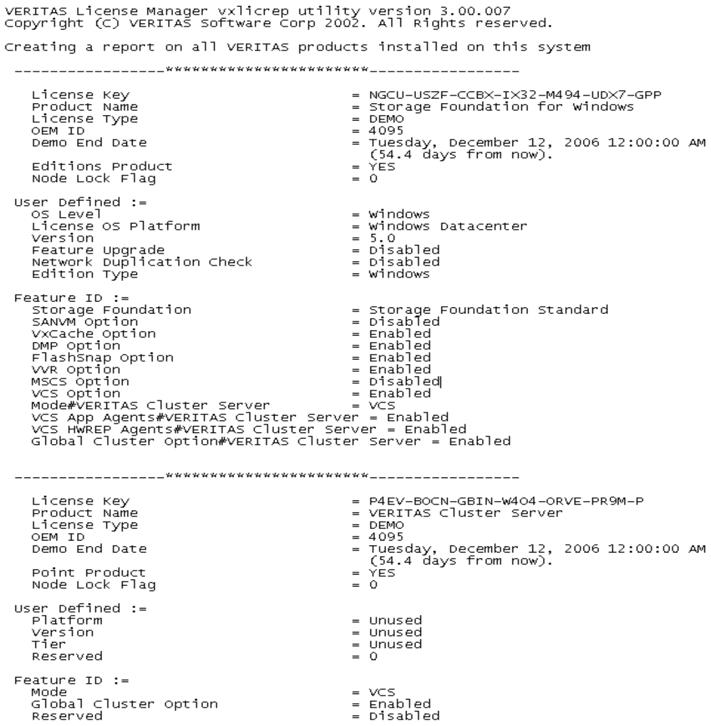
Open the command prompt.

Enter **vxlicrep** without any options to generate a default report.

Optionally, use one of the following options to produce the type of report needed:

-g	default report
-s	short report
-e	enhanced/detailed report
-h	display this help

Below is an output of using vxlicrep with the -e option for a detailed report.



```
VERITAS License Manager vxlicrep utility version 3.00.007
Copyright (C) VERITAS Software Corp 2002. All Rights reserved.

Creating a report on all VERITAS products installed on this system
 -----------------***********************-----------------

   License Key                         = NGCU-USZF-CCBX-IX32-M494-UDX7-GPP
   Product Name                        = Storage Foundation for Windows
   License Type                        = DEMO
   OEM ID                              = 4095
   Demo End Date                       = Tuesday, December 12, 2006 12:00:00 AM
                                         (54.4 days from now).
   Editions Product                    = YES
   Node Lock Flag                      = 0

 User Defined :=
   OS Level                            = Windows
   License OS Platform                 = Windows Datacenter
   Version                             = 5.0
   Feature Upgrade                     = Disabled
   Network Duplication Check           = Disabled
   Edition Type                        = Windows

 Feature ID :=
   Storage Foundation                  = Storage Foundation Standard
   SANVM Option                        = Disabled
   VxCache Option                      = Enabled
   DMP Option                          = Enabled
   FlashSnap Option                    = Enabled
   VVR Option                          = Enabled
   MSCS Option                         = Disabled|
   VCS Option                          = Enabled
   Mode#VERITAS Cluster Server         = VCS
   VCS App Agents#VERITAS Cluster Server = Enabled
   VCS HWREP Agents#VERITAS Cluster Server = Enabled
   Global Cluster Option#VERITAS Cluster Server = Enabled


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

   License Key                         = P4EV-BOCN-GBIN-W4O4-ORVE-PR9M-P
   Product Name                        = VERITAS Cluster Server
   License Type                        = DEMO
   OEM ID                              = 4095
   Demo End Date                       = Tuesday, December 12, 2006 12:00:00 AM
                                         (54.4 days from now).
   Point Product                       = YES
   Node Lock Flag                      = 0

 User Defined :=
   Platform                            = Unused
   Version                             = Unused
   Tier                                = Unused
   Reserved                            = 0

 Feature ID :=
   Mode                                = VCS
   Global Cluster Option               = Enabled
   Reserved                            = Disabled
```

SFW and SFW HA license packages

These license packages are available with SFW or SFW HA. Licenses for some options listed must be purchased separately.Table 1-3 lists the agents and options available with SFW and SFW HA.

Table 1-3 SFW and SFW HA option and agent packages

Product license	Included options and agents	Separately available options and agents
SFW 5.0		Options: ■ FlashSnap Option ■ Dynamic Multi-Pathing Option ■ Cluster Option for MSCS ■ Volume Replicator Option
SFW Enterprise 5.0	■ FlashSnap Option. ■ Dynamic Multi-Pathing Option. ■ Cluster Option for MSCS.	■ Volume Replicator Option
SFW HA 5.0	■ Application Agent: Veritas Cluster Server Application Agent for Microsoft Exchange Database Agents: ■ Veritas Cluster Server Database Agent for Microsoft SQL ■ Veritas Cluster Server Database Agent for Oracle	■ FlashSnap Option ■ Dynamic Multi-Pathing Option ■ Volume Replicator Option
SFW Enterprise HA 5.0	Options: ■ FlashSnap Option ■ Dynamic Multi-Pathing Option Agents (See SFW HA 5.0 for the agent's full name): ■ Application Agent ■ Database Agents	■ Volume Replicator Option

Table 1-3 SFW and SFW HA option and agent packages (continued)

Product license	Included options and agents	Separately available options and agents
SFW HA/DR 5.0	Option: ■ Global Clustering Option Agents (See SFW HA 5.0 for the agent's full name): ■ Application Agent ■ Database Agents Hardware Replication Agents: ■ Veritas Cluster Server Hardware Replication Agent for EMC Symmetrix Remote Data Facility (SRDF). ■ Veritas Cluster Server Hardware Replication Agent for Hitachi TrueCopy. ■ Veritas Cluster Server Hardware Replication Agent for IBM Peer-to-Peer Remote Copy (PPRC). ■ Veritas Cluster Server Hardware Replication Agent for EMC Mirrorview. ■ Veritas Cluster Server Hardware Replication Agent for IBM Metro Mirror	■ FlashSnap Option ■ Dynamic Multi-Pathing Option ■ Volume Replicator Option
SFW Enterprise HA/ DR 5.0	Option: ■ Global Clustering Option ■ FlashSnap Option ■ Dynamic Multi-Pathing Option Agents (See SFW HA 5.0 for the agent's full name): ■ Application Agent ■ Database Agents ■ Hardware Replication Agents (See SFW HA/DR 5.0 for the agent's list)	■ Volume Replicator Option

SFW Basic

This release is also available as SFW Basic. SFW Basic has the same features of SFW and includes the Veritas Dynamic Multi-pathing (DMP) option. However, SFW Basic is limited to a maximum of:

- Four dynamic volumes and/or four file systems which must be located on the same physical server. The aggregate total of volumes and file systems for all virtual servers located on one physical server may not exceed four volumes and/or four file systems.
- Two physical processors
  - One physical CPU is counted as one processor
  - A processor with “n” cores is counted as one processor

SFW Basic can be upgraded to SFW 5.0 or SFW HA 5.0.

SFW Basic is available with the use of a specific license key.

Using the Configuration Checker

The Configuration Checker wizard is a tool that enables you to verify your configuration before you install SFW HA or before you perform disaster recovery in a Microsoft Exchange or SQL Server environment. The wizard can be accessed by any of the following ways:

- Symantec Product Installer CD-ROM
- Solutions Configuration Center
- Command line [`C:\Program Files\Common Files\Veritas Shared\VPI\`*`{5.0.0.xx}`*`\setup install_mode=9 solution=1`]

Run the Configuration Checker wizard to:

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

When the wizard has completed the check, it automatically saves a summary report as an HTML file in the following location:

```
<ConfigChecker Installation
directory>\Reports\<TimeStamp>\report.htm
```

The report contains the number of Passed or Failed checks out of the total number of checks done on the selected systems, and gives a consolidated report of every check performed on the systems. Note that you can select multiple systems when running a pre-install check but can select only one system when configuring for disaster recovery.

Pre-install check

When running the Configuration Checker wizard before installing SFW HA, the wizard performs the following checks:

- Presence of SFW or SFW HA
- Software and hardware compatibility
- Operating system versions, service packs, and hotfixes
- Available disk space
- Total physical memory
- Availability of network ports used by Symantec products
- Active Directory
- Network configuration

Running the Configuration Checker wizard

1. Launch the Configuration Checker wizard in one of the following ways:
   - From the installation media, select **Tools > vpi** and double click **LaunchConfigChecker.bat**.
   - Double-click the Solutions Configuration Center icon on your desktop and click **Configuration Checker** in the menu on the right side of the screen.
   - Enter the following at the command line prompt:
     ```
     C:\Program Files\Common Files\Veritas
     Shared\VPI\{5.0.0.xx}\setup install_mode=9 solution=1
     ```
2. Read the information on the Welcome screen and click **Next**.
3. In the Computer Selection screen, select all of the nodes that you want to check. As you select a node, a description of that node appears on the right side of the screen, with the computer name, operating system, and a list of Symantec installed products.
4. If the node does not appear in the list, right-click the domain under which the node should appear. The **Add Computer** dialog box appears. Type the Domain and Computer name and click **OK**.

5 The node should now be listed under the appropriate domain. Select one or more nodes from the list and click **Next** to open the Account Information dialog box. Type the Username and Password for the selected computer and click **OK**.

If you select a node in a secure cluster, log in with your Windows domain account information. Make sure you type "<domain name>\" before your username.

6 In the Option Selection screen, select either **SFW Pre-Install Check** or **SFW HA Install Check**. By default, all of the options under the SFW/SFW HA Pre-Install Check are selected. Click an option to deselect it if you do not want that check run. When you are done selecting your options, click **Next**.

7 The Validation screen appears, and the Configuration Checker proceeds with the check. When status is complete, click **Next**.

8 The Summary screen lists the completed checks. An option with a green check means that the check completed successfully. However, an option with a red X means that the check failed.

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

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

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

Post-install check

When running the Configuration Checker wizard after installing SFW or SFW HA, the wizard can perform the following checks:

- Generic check

  Provides a system check for compatible software and hardware, total physical memory; available memory; OS version; driver signing policy settings; presence of Active Directory; availability of DNS, Domain Controller, and Global Category; status of VM volumes; and port availability.

- SFW HA check

  Checks for drive letter in use; available NIC cards; presence of Active Directory; consistency of Windows Services across clusters; consistency of system environment variables across clusters; consistency of license files; consistency between VCS service groups across clusters; and consistency between VCS resource types across clusters.

- Exchange Disaster Recovery Check

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

- SQL Server Disaster Recovery Check

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

Running the Configuration Checker wizard

1. Launch the Configuration Checker wizard in one of the following ways:
   - From the installation media, select **Tools > vpi** and double click **LaunchConfigChecker.bat**.
   - Double-click the Solutions Configuration Center icon on your desktop and click **Configuration Checker** in the menu on the right side of the screen.
   - Enter the following at the command line prompt:

     ```
     C:\Program Files\Common Files\Veritas
     Shared\VPI\{5.0.0.xx}\setup install_mode=9 solution=1
     ```
2. Read the information on the Welcome screen and click **Next**.
3. In the Computer Selection screen, select the node that you want to check. When you select a node, a description of that node appears on the right side of the screen, with the computer name, operating system, and a list of Symantec installed products.
4. If the node does not appear in the list, right-click the domain under which the node should appear. The **Add Computer** dialog box appears. Type the Domain and Computer name and click **OK**.
5. The node should now be listed under the appropriate domain. Select the node from the list and click **Next** to open the Account Information dialog box. Type the Username and Password for the selected computer and click **OK**.

   If you select a node in a secure cluster, log in with your Windows domain account information. Make sure you type “<domain name>\” before your username.
6. In the Option Selection screen, select one or more of the checks that you want to run. By default, all of the options for the desired check are selected. Click an option to deselect it if you do not want it run. When you are done selecting your options, click **Next**.

7 The Validation screen appears, and the Configuration Checker proceeds with the check. When status is complete, click **Next**.

8 The Summary screen lists the completed checks. An option with a green check means that the check completed successfully. However, an option with a red X means that the check failed.

For example, if the option **Available Memory** failed, click the option to select it and the Description pane will specify the reason for the failure.

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

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

Planning an SFW HA installation

During an SFW HA installation, the product installer automatically installs Veritas Storage Foundation for Windows and Veritas Cluster Server. You may select other applicable options during the installation. You may also choose to install simultaneously on more than one system during the installation process. After the initial installation, run the VCS Configuration Wizard to complete the VCS cluster configuration. The VCS Configuration Wizard presents the opportunity to configure optional VCS features including security options, Cluster Management Console, notification, and the global cluster wide-area connection resource.

Depending on your environment you may choose to configure the Symantec Product Authentication Service and the Cluster Management Console on systems outside the cluster.

Review the following information and decide how you want to configure your enironment:

- About Symantec Product Authentication Service
- About Veritas Cluster Management Console
- About notification
- About global clusters

About Symantec Product Authentication Service

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

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

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

- Root broker
  A root broker serves as the main registration and certification authority; it has a self-signed certificate and can authenticate other brokers.
- Authentication brokers
  Authentication brokers serve as intermediate registration and certification authorities. Authentication brokers have certificates that are signed by the root. Each node in the cluster serves as an authentication broker.

The *Symantec Product Authentication Service Quick Start Guide* describes the best practices and options for configuring the root broker in your environment.

About Veritas Cluster Management Console

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

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

- If you want to use Cluster Management Console to manage multiple clusters, you must set up a standalone management server.
- If you want to use the Cluster Management Console to manage a single cluster, choose the option to configure the Cluster Management Console, also known as the Web console from the VCS Configuration Wizard.

Configuring the Cluster Management Console may be done during initial cluster configuration or at a later time.

Operational mode	Configuration description
Local management of one cluster (single-cluster mode)	The Cluster Management Console is installed on each node in the cluster and can be configured as part of the ClusterService service group by using the VCS Configuration Wizard to configure the Web console. The Cluster Management Console offers robust cluster management capability and can be run from any supported Web browser on any system.
Centralized, comprehensive, enterprise-wide administration of multiple clusters (multi-cluster mode)	One instance of the Cluster Management Console is installed outside all clusters on a standalone server. The console enables users to visually and intuitively input commands to the multi-cluster management engine, the *management server*. The management server initiates monitoring and management actions based upon those commands. The management server uses a database to store cluster configurations, cluster status, events, event policies, report jobs, report outputs, and more. If the management server and cluster nodes are separated by a firewall, a component called *cluster connector* is installed on each cluster node. Cluster connector enables communication with clusters through firewalls. Cluster connector also provides buffering for cluster data. If the console goes offline and then comes back online, it can retrieve data collected during the offline period from the cluster connector buffer. See the *Veritas Cluster Management Console Implementation Guide*.

The configurational differences between the operational modes mean that you cannot switch a single Cluster Management Console installation from one mode to the other. The modes are also incompatible on the same system. Consequently, one system cannot offer both operational modes. However, the modes *can* co-exist in the same multi-cluster environment, with single-cluster-mode installations on VCS cluster nodes, and a multi-cluster-mode installation on a management server host. Such a deployment can be desirable if different IT administrators in your enterprise have different scopes of responsibility.

About notification

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

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

See the *Veritas Cluster Server Administrator's Guide*.

About global clusters

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

Global clusters may be configured either through the Disaster Recovery Configuration Wizard available from the Solutions Configuration Center or through the Global Group Configuration Wizard. Both processes require a wide-area connector resource for inter-cluster communication. This resource is configured automatically as part of the Disaster Recovery Configuration Wizard or may optionally be configured using the VCS Configuration Wizard.

The Disaster Recovery Configuration Wizard is described in the Solutions Guides. The Global Group Configuration Wizard and VCS Configuration Wizard are descibed in the *Veritas Cluster Server Administrator's Guide*.

See the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange*, the*Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL* or the *Veritas Storage Foundation and High Availability Solutions, Solutions Guide*.

or

See the *Veritas Cluster Server Administrator's Guide*.

Planning an SFW with MSCS installation

If you plan to set up an MSCS cluster with SFW please review the following recommendations:

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

Planning a VVR installation

Replication between servers running Windows 2000 and Windows Server 2003 (32-bit) is supported in the following environments:

- Storage Foundation for Windows with the VVR option on standalone servers (no clustering)
- Storage Foundation for Windows HA with the VVR and Global Cluster (GCO) Options
- Storage Foundation for Windows with the VVR and MSCS options

Replication between servers running Windows 2000 and Windows Server 2003 (32-bit) is not supported in a Replicated Data Cluster configuration.

Chapter 2

Installing SFW or SFW HA

This chapter contains:

About installing SFW or SFW HA

This chapter covers the installingVeritas Storage Foundation 5.0 for Windows (SFW) or Veritas Storage Foundation High Availability 5.0 for Windows (SFW HA). It also covers licensing, adding features, and uninstalling information.

Installing using the product installer

The product installer enables you to install the software for Veritas Storage Foundation for Windows or Veritas Storage Foundation HA for Windows. An SFW HA installation includes Veritas Storage Foundation for Windows and Veritas Cluster Server. You may select other applicable options during the installation. The steps in this section are based on a server installation.

Setting Windows driver signing options

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

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

Table 2-1 Installation behavior with unsigned drivers

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

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

To change the driver signing options on each system

1 Log on locally to the system.

2 Open the Control Panel and click **System**.

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

4 In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.

5 Click **OK**.

6. Repeat for each computer.

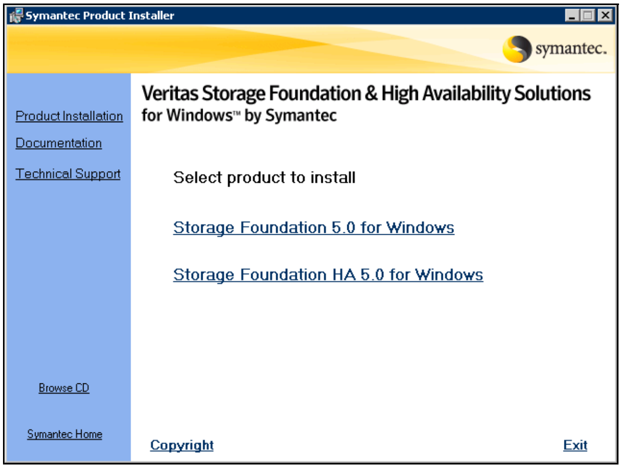
   If you do not change the driver signing option, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing option to its previous state.

Installing Storage Foundation HA for Windows

Install Veritas Storage Foundation HA for Windows.

To install the product

1. Allow the autorun feature to start the installation or double-click **Setup.exe.**
2. Choose the language for your installation and click **OK**. The SFW Select Product screen appears.
3. Click **Storage Foundation HA 5.0 for Windows.**



Veritas Storage Foundation & High Availability Solutions for Windows™ by Symantec

Select product to install

Symantec Product Installer
symantec.
Product Installation
Documentation
Technical Support
Storage Foundation 5.0 for Windows
Storage Foundation HA 5.0 for Windows
Browse CD
Symantec Home
Copyright
Exit

This page also contains the following links:

Product Installation — Click this link to return to this Product Installation screen.

Documentation — Click this link to see links for the Getting Started Guide and the Release Notes.

Technical Support — Click this link to see information about Symantec technical support.

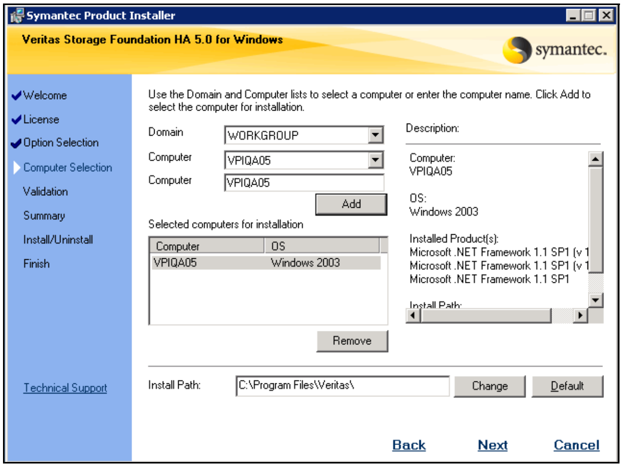
Browse CD — Click this link to see the contents of the CD.

Symantec Home	Click this link to go to: http://www.symantec.com.

4. Do one of the following:
   - Click **Complete/Custom** to begin installation.
   - Click the **Administrative Console** link to install only the client components.
5. Review the Welcome message and click **Next**.
6. Read the License Agreement by using the scroll arrows in the view window. If you agree to the license terms, click the radio button for **I accept the terms of the license agreement**, and click **Next**.
7. Enter the product license key before adding license keys for features. Enter the license key in the top field and click **Add**.

   If you do not have a license key, click **Next** to use the default evaluation license key. This license key is valid for a limited evaluation period only.
8. Repeat for additional license keys. Click **Next**
   - To remove a license key, click the key to select it and click **Remove**.
   - To see the license key’s details, click the key.
9. Select the appropriate SFW or SFW HA product options and click **Next**.

10 Select the domain and the computers for the installation and click **Next**.



Use the Domain and Computer lists to select a computer or enter the computer name. Click Add to select the computer for installation.

Domain: WORKGROUP

Computer: VPIQA05

Computer: VPIQA05

Selected computers for installation

Computer	OS
VPIQA05	Windows 2003

Description:

Computer:
VPIQA05

OS:
Windows 2003

Installed Product(s):
Microsoft .NET Framework 1.1 SP1 (v 1
Microsoft .NET Framework 1.1 SP1 (v 1
Microsoft .NET Framework 1.1 SP1

Install Path:

Install Path: C:\Program Files\Veritas\

Domain

Select a domain from the list.

Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.

Computer

To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**.

To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**.

Click a computer's name to see its description.

Install Path

Optionally, change the installation path.

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

11 When the domain controller and the computer running the installation program are on different subnets, the installer may be unable to locate the

target computers. In this situation, after the installer displays an error message, enter the host names or the IP addresses of the missing computers manually.

12 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**.
If a computer fails validation, address the issue, and repeat the validation. Click the computer in the list to display information about the failure. Click **Validate Again** to begin the validation process again.

13 If you are using multiple paths and selected DMP ASLs or a specific DSM you receive the Veritas Dynamic Multi-pathing warning. At the Veritas Dynamic Multi-pathing warning:

- For DMP ASLs installations—make sure that you have disconnected all but one path of the multipath storage to avoid data corruption.
- For DMP DSMs installations—the time required to install the Veritas Dynamic Multi-pathing DSMs feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, connect only one physical path during installation. After installation, reconnect additional physical paths before rebooting the system.

14 Click **OK**.

15 Review the information and click **Install**. Click **Back** to make changes, if necessary.

16 The Installation Status screen displays status messages and the progress of the installation.
If an installation fails, click **Next** to review the report and address the reason for failure. You may have to either repair the installation or uninstall and re-install.

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

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

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

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

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

Resetting the driver signing options

After completing the installation sequence, reset the driver signing options on each computer.

To reset the driver signing options

1. Open the Control Panel, and click **System**.
2. Click the **Hardware** tab and click **Driver Signing**.
3. In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.
4. Click **OK**.
5. Repeat for each computer.

Installing from the command line

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

Presented at the end of this section are command examples showing a local installation of the SFW client and SFW server, as well as a remote installation of an SFW server.

See “Silent installation example: SFW client” on page 45.

See “Silent installation example: SFW server” on page 45.

See “Silent installation example: remote installation of an SFW server” on page 46.

To start the installation from the command window

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 CD.
4. Use the following command syntax to install SFW:

   ```
   Setup.exe /s INSTALL_MODE=InstallMode SOLUTION=Solution
   [LICENSEKEY="LicenseKey"] [OPTIONS="a,b,c,..."]
   [INSTALLDIR="InstallDirPath"] [NODE=SysA]
   [REBOOT=RebootMode]
   ```

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

Parameters for setup.exe

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

Table 2-2 Parameters for setup.exe

Parameter	Use
/s	Set for silent mode. If not set, boots the product installer GUI.
INSTALL_MODE	Set to indicate an installation or uninstallation. ***1*** = To install ***5*** = To uninstall Example: **INSTALL_MODE=1**
SOLUTION	Set to the type of installation. ***1*** = SFW Server ***2*** = SFW HA Server ***3*** = SFW Client ***4*** = SFW HA Client ***5*** = Language Pack ***6*** = VCS Server (VCS Agent for NetApp SnapMirror installation) ***7*** = VCS Client (VCS Agent for NetApp SnapMirror installation) Example: **SOLUTION=*1*** **Note:** To install the server and matching client components, run two setup.exe /s commands sequentially, one with the SOLUTION parameter set for the server component and the other set for the matching client component. If you use a script to install the server and client, consider first installing the client and then the server, so that the script can reboot the system after server installation.
LICENSEKEY	Set the license key for the installation. Enter multiple keys by separating them with a comma—do *not* put spaces around the comma. The license key must start and end with a quotation mark ("). *LicenseKey* has no default setting. Example: **LICENSEKEY="*123-234-123-234-345,321-543-765-789-321*"**

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

Parameter	Use
OPTIONS	Set the desired options, if any, for the type of installation. The list of options must start and end with a quotation mark ("). **Note:** There are no default settings. See Table 2-3 for a complete list and description of the available options. **Note:** DMP Device Specific Modules (DSMs) and DMP Array Support Libraries (ASLs) can not co-exist on the same server simultaneously. Example: **OPTIONS="*MSCS,VVR*"**
INSTALLDIR	Use only to set a non-default path for the installation directory. The path must start and end with a quotation mark ("). The default setting, used when you do not specify a path, is `SystemDrive:\Program Files\Veritas` Example: **INSTALLDIR="*C:\InstallationDirectory*"**
NODE	Set the node name. Specify only one node at a time. The local node is the default setting when the node is unspecified. Example: **Node=*SysA***
REBOOT	Setting for the automatic reboot of the system at the completion of the installation. ***0*** = No reboot ***1*** = Reboot The default setting is 0 for no system reboot. Example: **REBOOT=*1*** **Note:** Reboot the system at the end of installation to ensure the correct installation of the SFW drivers for the server component. You do not have to reboot after installing the client components.

Options differ depending on your product and environment. Table 2-3 shows the available options:

Table 2-3 Available Options

Option	Description	SFW	SFW HA
vvr	Volume Replicator (VVR) replicates data across multiple sites for disaster recovery	✔	✔

Table 2-3 Available Options (continued)

Option	Description	SFW	SFW HA
flashsnap	FlashSnap allows you to create and maintain split-mirror, persistent snapshots of volumes	✔	✔
vxcache	VxCache uses a portion of system memory to improve I/O performance	✔	✔
mscs	Cluster option for MSCS	✔	
dmp	DMP Array Support Libraries (ASLs)	✔ (32-bit only)	✔ (32-bit only)
vemcsymm	EMC Symmetrix/DMX DSM (Windows Server 2003 only)	✔	✔
vemcclar	EMC Clariion DSM (Windows Server 2003 only)	✔	✔
vhdsaa	Hitachi TagmaStore/HP XP DSM (Windows Server 2003 only)	✔	✔
vhdsap	Hitachi 95xx-AMS-WM DSM (Windows Server 2003 only)	✔	✔
vhpeva	HP EVA-MSA DSM (Windows Server 2003 only)	✔	✔
vibmaads	IBM DS8000/ESS DSM (Windows Server 2003 only)	✔	✔
vibmap	IBM DS6000 DSM (Windows Server 2003 only)	✔	✔
vengap	IBM DS4000/Sun 6000 DSM (Windows Server 2003 only)	✔	✔
vnetapp	NETAPP DSM (Windows Server 2003 only)	✔	✔
gco	Global Cluster Option (GCO) enables you to link clusters to provide wide-area failover and disaster recovery.		✔
sql	Database agent for Microsoft SQL Server		✔
oracle	Database agent for Oracle		✔ (32-bit only)

Table 2-3 Available Options (continued)

Option	Description	SFW	SFW HA
srdf	Hardware replication agent for EMC SRDF		✔
truecopy	Hardware replication agent for Hitachi TrueCopy		✔
exchange	Enterprise agent for Microsoft Exchange		✔ (32-bit only)
mirrorview	Hardware replication agent for EMC MirrorView		✔
metromirror	Hardware replication agent for MetroMirror		✔
pprc	Hardware replication agent for IBM PPRC		✔

Silent installation example: SFW client

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

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

Silent installation example: SFW server

This sample command installs the SFW Server with a license key of 123-234-123-234-345, along with the MSCS and VVR options and their license keys. It 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 SOLUTION=1
    LICENSEKEY="123-234-123-234-345,321-543-765-789-321,
    321-543-765-789-789" OPTIONS="MSCS,VVR"
    INSTALLDIR="C:\InstallationDirectory" REBOOT=1
```

Silent installation example: remote installation of an SFW server

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

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

Possible next tasks

Configuring an SFW HA cluster

After installing SFW HA, run the VCS Configuration Wizard to complete the VCS cluster configuration. See "Planning an SFW HA installation" on page 29 for information more information.

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

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

Configuring an iSCSI SAN with SFW

On an iSCSI initiator node, SFW enables you to define iSCSI target portals, log into and out of iSCSI targets, and view the target portal group configuration. With SFW, you can also connect to and manage iSNS objects on a Microsoft iSNS server. If your server's iSCSI initiator is connected to a Microsoft iSCSI Software Target, you can view the set of LUNs that are accessible to your initiator.

Prerequisites

When configuring an iSCSI SAN with SFW, you should consider the following prerequisites and the requirements for each as described in the documentation that accompanies them:

- Microsoft iSCSI initiator 2.02 or above.
- iSCSI HBA or dedicated NIC card.
- Windows Storage Server R2 with VDS 1.1 Update.
- Microsoft VDS iSCSI Hardware Provider
  (if you are connecting to a Microsoft iSCSI Software Target).

Setting up an iSCSI SAN

Setting up an iSCSI SAN requires configuring target portals, setting up the iSCSI targets and iSCSI initiators, configuring the storage, assigning access rights, and registering with an iSNS server.

Setting up the iSCSI targets and configuring the storage should be done according to the instructions of the manufacturer of the storage device.

Setting up the iSCSI initiators requires that iSCSI initiator software be installed on each server to enable them to connect to the iSCSI targets. Optionally, the iSNS server software needs to be installed on a server to allow automatic discovery of the iSCSI targets on the network.

To assign access rights

1. In the tree view of the VEA GUI, click the iSCSI node. Since the iSNS server automatically discovers the initiators and targets, expanding the iSCSI node displays all the available initiators and targets in the network.
2. Login to the desired targets to make them available to the initiator.
   - Select a target and select Login from its context menu.
   - Check any desired optional login settings. The available login settings are to allow persistent restore of the login or to enable multi-path login.
   - To set any security settings, such as CHAP or IPsec, check Advanced Settings to access the security settings dialog.

Make sure that the security settings are compatible with the settings that were set up for the storage device.

Using SFW iSCSI late start

SFW and SFW HA normally import dynamic (non-cluster) disk groups during system start up. At start up, however, the products can neither discover nor import Microsoft iSCSI Software Initiator managed storage devices. To allow SFW and SFW HA the time to discover and import this managed storage, you must configure the Veritas DG Delayed Import Service (VxDgDI) and use the `vxdg latestart` command.

vxdg latestart

The vxdg latestart command is entered at the command line using the following form:

`vxdg -g`***`DynamicDiskGroupName`***` latestart on|off`

where ***`DynamicDiskGroupName`*** is the name of the Microsoft iSCSI Software Initiator managed dynamic disk group.

Specifying `on` in the `vxdg latestart` command enables the dynamic disk group that is referenced in `-g`***`DynamicDiskGroupName`*** to be imported after system start up by the Veritas DG Delayed Import Service (VxDgDI). The VxDgDI can import the dynamic disk group after it is made dependent on the service that controls the storage. This allows the required time for the storage to become available. Applications that rely on storage imported by the VxDgDi service may also need to be made dependent on VxDgDI so that they may proceed when their storage is available.

For example, iSCSI storage needs to be imported after system start up because it is not available at system start up time. When VxDgDI is made dependent on the iSCSI service, the import of the dynamic disk group occurs after system start up when the iSCSI service is ready. Applications that rely on the iSCSI storage and have been made dependent on the VxDgDI service may then proceed.

As long as the dynamic disk group remains on the same host, the `vxdg latestart` is enabled, even through reboots. If the dynamic disk group is deported and imported on another host, the `vxdg latestart` is disabled and must be re-enabled on the new host. In a clustered environment, the cluster application imports disk groups and does not need to have vxdg latestart enabled.

To use `vxdg latestart`

1. In the Windows Services dialog, change the Veritas DG Delayed Import Service startup type from **Manual** to **Automatic**.
2. Edit the Windows registry to make VxDgDI dependent on the service that controls the storage. (For Windows 2003, use regedit to configure the service. For Windows 2000, use regedt32 to configure the service.)

The following procedure to make the VxDgDI dependent on the Microsoft iSCSI Initiator service (MSiSCSI) on Windows 2003 is given as an example.

- Open the Registry Editor (regedit) to edit the Windows registry.
- Select the registry key:
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \VxDgDI`
- Right-click the **DependOnService** value and select **Modify**. If the DependOnService value does not exist, right-click empty space in the right pane of the Registry Editor to bring up a context menu to create the value. Select **New > Multi-String Value** and name the new value **`DependOnService`**. Right-click the **DependOnService** value and select **Modify.**
- In the Edit String dialog that appears, enter **`MSiSCSI`** on a new line below the other entries that appear in the Value Data pane.
- Click **OK** and close the Registry Editor.
- Reboot the system to apply the changes.
- Do not reboot your system at this point if you also need to edit the registry as indicated in step 4 below.
- Reboot your system now if you do not need to make any additional changes to the registry.

3 Enter the `vxdg latestart` command at the command line.
For example:
`vxdg -gDynDskGrp2 latestart on`
Enables the dynamic disk group DynDskGrp2 to be imported after system startup.

4 Applications that rely on storage which is imported by the VxDgDI service have their storage available after the Veritas DG Delayed Import Service completes its startup process. However you need to make applications that start as a Windows service, such as Microsoft Exchange, dependent on the Veritas DG Delayed Import Service by editing the Windows Registry Editor before their storage is available. (For Windows 2003, use regedit to configure the service. For Windows 2000, use regedt32 to configure the service.)
The following example makes the service for Microsoft Exchange (Microsoft Exchange Information Store service) dependent on VxDgDI on Windows 2003:

- Open the Registry Editor (regedit) to edit the Windows registry.
- Select the registry key
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \MSExchangeIS`

- Right-click the **DependOnService** value and select **Modify**. If the DependOnService value does not exist, right-click empty space in the right pane of the Registry Editor to bring up a context menu to create the value. Select **New > Multi-String Value** and name the new value `DependOnService`. Right-click the **DependOnService** value and select **Modify.**
- In the Edit String dialog that appears, enter VxDgDI on a new line below the other entries that appear in the Value Data pane.
- Click **OK** and close the Registry Editor.
- Reboot the system to apply the changes.

Updating SFW or SFW HA

The product installer allows you to update the SFW and SFW HA client and server components you have installed.

To update SFW and SFW HA

1. Open the Windows Control Panel and click **Add or Remove Programs**.
2. Select **Veritas Storage Foundation with High Availability 5.0 for Windows (Server) Components** and click **Change**.
3. The Symantec Product Installer screen appears. Select **LiveUpdate**. Click **Next**.
4. The LiveUpdate screen appears. Choose to check if updates are available automatically by selecting **On (automatically check for updates)** or choose to check if updates are available manually by selecting **Off (manually check for updates)**.
5. Choose a LiveUpdate mode. If **On (automatically check for updates)** is selected you have a choice to select **Express** to have updates automatically downloaded and installed or select **Interactive** to view a list of available updates and choose which to download and install on your computer.
6. Select **Check for latest update after “Finish” is clicked.** Click **Finish**.

Adding or removing features

The product installer allows you to add or remove features. You can only add or remove features on the local system.

To add or remove features

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

2 Select **Veritas Storage Foundation with High Availability 5.0 for Windows (Server) Components** and click **Change**.

3 The Symantec Product Installer screen appears. Select **Add or Remove**. Click **Next**.

4 The Server Components screen appears. Select or clear the option check boxes in the tree navigation structure to add or remove a component respectively.

To add a license key for an option:

1 Right-click on the option and select **Add License**.

2 In the pop-up window that appears, enter the license key for the option and click **OK**.

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

Validation and Summary

1 The Validation screen appears. The installer checks the prerequisites for the selected options and displays the results. Review the information and click **Next**.
If a system fails validation, click the system in the systems list to display information about the failure. Address the problem and click **Validate Again** to repeat the validation process.

2 The Summary screen appears. Review the information and click **Update** to begin the product update.

3 The Update Status screen appears and displays status messages and the update progress.

4 When complete, review the summary and click **Next**.

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

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

Repairing the installation

The product installer can repair an existing installation of SFW and SFW HA client and server components. This installer can only repair the local system.

To repair the installation

1. Open the Windows Control Panel and click **Add or Remove Programs**.
2. Select **Veritas Storage Foundation with High Availability 5.0 for Windows (Server) Components** and click **Change**.
3. The Symantec Product Installer screen appears. Select **Repair**. Click **Next**.
4. The Validation screen appears. The installer checks the prerequisites for the systems and displays the results. Review the information and click **Next**.

   If a system fails validation, click the system in the systems list to display information about the failure. Address the problem and click **Validate Again** to repeat the validation process.
5. The Summary screen appears. Review the information and click **Repair** to begin the repair process.
6. The Repair Status screen appears. Status messages and the progress of the repair are displayed.

   If a repair fails, click **Next** to review the report and address the reason for failure. You may have to uninstall and re-install the software.
7. When complete, review the summary and click **Next**.
8. On the Thank You screen, click **Finish**.
9. In the message box, click **Yes** to reboot your system.

License management

The product installer allows you to add or remove license keys for options in your installation of SFW and SFW HA client and server components.

To add or remove license keys

1. Open the Windows Control Panel and click **Add or Remove Programs**.
2. Select **Veritas Storage Foundation with High Availability 5.0 for Windows (Server) Components** and click **Change**.
3. The Symantec Product Installer screen appears. Select **License Management**. Click **Next**.

4 The license key screen appears. Enter the license key you want to add and click **Update.** If you want to remove a license key, select the license key in the Licenses field and click **Remove**.

Uninstalling using the product installer

In order to uninstall the software from remote computers, the local computer where you uninstall must have SFW or SFW HA installed on it.

The steps in the following procedure apply to a SFW uninstallation of the server and client components from a Windows 2000 system. The steps for uninstalling the client components and high availability server are similar. For SFW HA uninstallations, you must unconfigure the cluster before uninstalling.

To uninstall using the product installer

1 In the Windows Control Panel, select **Add or Remove Programs**.

2 Click **Veritas Storage Foundation 5.0 for Windows (Server Components)**.

3 Click **Remove**.

4 Click **Next**.

5 On the Client Components screen, uninstall client components in addition to the server components by selecting the check box. Click **Next**.

6 Select the systems that you want to uninstall from the Domain and Computer drop-down menus and click **Add**. Optionally, type the computer's name in the Computer field. Repeat to uninstall from other systems.
To remove a system from the **Selected computers for uninstall** list, click the system and click **Remove**.

7 Click **Next**.

8 On the Validation screen, the installer checks the prerequisites for the selected systems and displays the results. Review the information and click **Next**.
If a system fails validation, click the system in the systems list to display information about the failure. Address the problem and click **Validate Again** to repeat the validation process.

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

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

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

11 When complete, review the summary and click **Next**.

12 Reboot the remote nodes.Note that you cannot reboot the local node now.

- Click the check box next to the remote nodes that you want to reboot.
- Click **Reboot**.
- When the nodes have finished rebooting successfully, the Reboot Status shows Online and the **Next** button is available. Click **Next**.
- Once the remote nodes have rebooted, click **Next**.

13 On the Thank You screen, review the log file and click **Finish**.

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

Uninstalling from the command line

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

At the end of this section, two command examples show how to uninstall the client components.

See "Setup.exe example: Uninstalling the SFW client components" on page 57.
See "Setup.exe example: Uninstalling the SFW server components" on page 57.

To start the uninstallation 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 CD.
4. Use the following command syntax to silently uninstall SFW:

```
Setup.exe /s INSTALL_MODE=InstallMode SOLUTION=Solution
[REBOOT=RebootMode] [NODE=SysA]
```

Information about the possible parameter values follows:

Table 2-4 Parameters for uninstalling the product

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

Table 2-4 Parameters for uninstalling the product

Parameter	Use
SOLUTION	Set to the type of uninstallation. ***1*** = SFW Server ***2*** = SFW HA Server ***3*** = SFW Client ***4*** = SFW HA Client ***5*** = Language Pack ***6*** = VCS Server (VCS Agent for NetApp SnapMirror installations) ***7*** = VCS Client (VCS Agent for NetApp SnapMirror installations) The default setting is ***1*** for SFW Server. Example: **SOLUTION=*1*** **Note:** To uninstall the server and matching client components, run two `setup.exe /s` commands, one with the SOLUTION parameter set for the server component and the other set for the matching client component.
REBOOT	Setting for the automatic reboot of the system at the completion of the installation. ***0*** = No reboot ***1*** = Reboot The default setting is ***0*** for no system reboot. Example: **REBOOT=*1***
NODE	Set the node name. Specify only one node at a time. The local node is the default setting when the node is unspecified. Example: **Node=*SysA*** **Note:** Reboot the system at the end of installation to ensure that the SFW drivers for the server component are installed correctly. You do not have to reboot after installing the client.

Setup.exe example: Uninstalling the SFW client components

This sample command completely uninstalls the SFW server components, and tells the system to reboot at the end of the uninstallation.

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

Setup.exe example: Uninstalling the SFW server components

This sample command completely uninstalls the SFW server components, and tells the system to reboot at the end of the uninstallation.

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

Installing and uninstalling Veritas Dynamic Multi-pathing

This section contains the following topics:

- "Introduction" on page 57
- "Selecting DMP ASLs or DMP DSMs" on page 58
- "Prerequisites" on page 58
- "Installing and uninstalling DMP Device Specific Modules (DSMs)" on page 59
- "Installing and uninstalling DMP Array Support Libraries (ASLs)" on page 63

For more detailed instructions, see the *Veritas Storage Foundation Administrator's Guide*.

Introduction

The Veritas Dynamic Multi-pathing option adds fault tolerance by supporting multiple paths between a server and a storage array. Veritas Dynamic Multi-pathing (DMP) is implemented through either:

- Dynamic Multi-pathing Array Support Libraries (ASLs), or
- Dynamic Multi-pathing Device Specific Modules (DSMs).

Note: DMP ASLs and DMP DSMs *are different products* and *cannot run on the same computer*.

Selecting DMP ASLs or DMP DSMs

Choosing between DMP ASLs or DMP DSMs depends on your environment. Before implementing either option, some factors to consider are operating system versions and support for a specific array. Refer to the Hardware Compliance List on the Symantec Support web site at http://entsupport.symantec.com to determine the approved hardware for SFW or SFW HA.

DMP DSMs

DMP DSMs are the dynamic multi-pathing method that work with the Microsoft Windows Server 2003 Multipath Input/Output solution. DMP DSMs support the following:

- Windows Server 2003
- Windows Storport driver
- Microsoft iSCSI Initiator
- Dynamic Least Queue Depth load balancing
- Active/Active dynamic multi-pathing with clustering

DMP ASLs

DMP ASLs are the Dynamic Multi-pathing method used in earlier SFW releases. DMP ASL supports the following:

- Windows 2000 and Windows Server 2003
- Windows miniport driver
- SCSI port driver
- Load balance policy
- 32-bit operating systems only

Prerequisites

Please review the following prerequisites:

- Make sure that your host has an HBA 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 only one path.

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).

Installing and uninstalling DMP Device Specific Modules (DSMs)

This section includes the following topics:

- "Setting up DMP Device Specific Modules (DSMs)" on page 59
- "Installing DMP Device Specific Modules (DSMs) on a new standalone server" on page 60
- "Installing SFW HA and DMP Device Specific Modules (DSMs) on a cluster for the first time" on page 60
- "Installing SFW MSCS and DMP Device Specific Modules (DSMs) on a cluster for the first time" on page 61
- "Adding DMP Device Specific Modules (DSMs) to an existing standalone server" on page 61
- "Adding DMP DSMs to an existing SFW HA or MSCS cluster" on page 62

Setting up DMP Device Specific Modules (DSMs)

In general, the steps for adding DMP DSMs to any configuration are as follows:

- Install the new host adapter hardware.
- Make sure that only a single path is connected to the array storage to shorten installation time.
- Install the software by selecting DMP DSMs as part of the SFW or SFW HA installation process.

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

Note: DMP DSMs cannot co-exist with DMP ASLs and that you must uninstall DMP ASLs before installing DMP DSMs.

It is very important to install the correct hardware drivers for DMP DSMs. Refer to your hardware documentation for detailed information about hardware drivers.

Installing DMP Device Specific Modules (DSMs) on a new standalone server

Follow these steps to install DMP DSMs on a new standalone server.

To install DMP DSMs on a new standalone server

1. Install the necessary hardware and the appropriate drivers.
2. Connect only one path from the array to the computer.
3. During installation, on the Option Selection screen, under Dynamic Multi-pathing, select **DMP Device Specific Modules (DSMs)**.
4. Complete the wizard, rebooting where instructed.
5. Physically reconnect the additional path.

Installing SFW HA and DMP Device Specific Modules (DSMs) on a cluster for the first time

Active/Active or Active/Passive load balance settings can be used for DMP DSMs in a cluster environment. DMP DSMs automatically set the load balancing to Active/Passive for disks under SCSI-2 reservation. For Active/Active load balancing in a cluster environment, the array must be enabled for SCSI-3 Persistent Group Reservations (SCSI-3 PGR). SCSI-3 PGR is available only on Windows Server 2003 and is disabled by default. For more information on DMP DSMs and enabling or disabling SCSI-3 PGR see the *Veritas Storage Foundation Administrator's Guide* and the SFW 5.0 Hardware Compliance List (HCL) located at: http://entsupport.symantec.com

Note: Symantec maintains a Hardware Compliance List (HCL) for Veritas Storage Foundation & High Availability Solutions 5.0 for Windows Products on the Symantec Support web site. The HCL gives information on HBAs, firmware, and switches that have been tested with each supported array. Check the HCL for details about your hardware before using DMP ASLs or DMP DSMs.

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

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

1. Before running the installation, connect only one path from the array to the computer.
2. Install SFW HA and DMP DSMs at the same time on all nodes in the cluster. During installation select the appropriate features.
3. Reboot after installation.
4. Physically reconnect the additional path.
5. After rebooting, run the various VCS wizards to complete the VCS cluster configuration. For more information on creating and configuring the VCS cluster, see the *Veritas Storage Foundation Administrator's Guide*.

Installing SFW MSCS and DMP Device Specific Modules (DSMs) on a cluster for the first time

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

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

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

1. Create the MSCS cluster.
2. Before running the installation, connect only one path from the array to the computer.
3. Install SFW and DMP DSMs at the same time. During installation select the appropriate features.
4. Reboot after installation.
5. Physically reconnect the additional path.
6. Set up and configure the MSCS cluster.

Adding DMP Device Specific Modules (DSMs) to an existing standalone server

Follow these steps to add DMP DSMs to an existing server.

To add DMP DSMs to an existing server

1. Install additional hardware and its appropriate drivers.
2. Connect only one path from the array to the computer.

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

4 Select **Change or Remove Programs**.

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

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

7 The Option Selection screen appears. Under Dynamic Multi-pathing, select **DMP Device Specific Modules (DSMs)**.

8 To add a license key for an option:

- Click the **Add License** link located at the far right of the screen
- The Add License link appears only for unlicensed options.
- In the pop-up window that appears, enter the license key for the option and click **OK**.
- Select the check box to add the option and click **Next**.

9 Reboot the system.

10 Reconnect the additional physical path.

11 Verify that the additional path exits.

- Open the Veritas Enterprise Administrator console.
- In the System field, expand the Disks tree.
- Click any external hard disk.
- Above the console, click the DMP tab.
- Verify that the path exists.

Adding DMP DSMs to an existing SFW HA or MSCS cluster

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

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

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

2 Install additional hardware and its appropriate drivers.

3 Connect only one path from the array to the computer.

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

5 Select **Change or Remove Programs**.

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

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

8 The Option Selection screen appears. Under Dynamic Multi-pathing, select **DMP Device Specific Modules (DSMs)**.

   To add a license key for an option:

   - Click the **Add License** link located at the far right of the screen.
   - The Add License link appears only for unlicensed options.
   - In the pop-up window that appears, enter the license key for the option and click **OK**.
   - Select the check box to add the option.

   Click **Next**.

9 Reconnect the additional physical path.

10 Reboot the system.

11 Verify that the additional path exists.

   - Open the Veritas Enterprise Administrator console.
   - In the System field, expand the Disks tree.
   - Click any external hard disk.
   - Above the console, click the DMP tab.
   - Verify that the path exists.

Uninstalling DMP DSMs

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

See“Adding or removing features” on page 51.

Installing and uninstalling DMP Array Support Libraries (ASLs)

This section covers the following topics:

- “Setting up DMP Array Support Libraries (ASLs)” on page 64
- “Including the disk array storage after installing DMP ASLs” on page 65
- “Installing DMP ASLs on a new standalone server” on page 65
- “Installing SFW HA and DMP ASLs for the first time on a cluster” on page 66
- “Installing MSCS and DMP ASLs for the first time on a cluster” on page 67
- “Adding DMP ASLs to an existing standalone server” on page 68
- “Adding DMP ASLs to an existing SFW HA or SFW MSCS cluster” on page 69
- “Uninstalling DMP ASLs” on page 70

If you have DMP Array Support Libraries (ASLs) already on your system and you are upgrading to SFW or SFW HA, see the following:

See "Before upgrading to SFW 5.0" on page 75.

See "Before upgrading to SFW HA 5.0" on page 99.

Setting up DMP Array Support Libraries (ASLs)

Connect only one of the paths to the disk array before installing SFW or SFW HA with DMP Array Support Libraries (ASLs). Once you have installed DMP Array Support Libraries (ASLs), bring the array under DMP ASLs control and connect the additional path. Steps for including the disk array—bringing it under DMP ASLs control—and connecting the paths follow.

Note: DMP ASLs cannot co-exist with DMP DSMs. Uninstall existing DMP DSMs before installing DMP ASLs.

Warning: Before connecting additional data paths to shared storage, make sure that you place the array under DMP ASLs control. Attaching a second path and using storage that is not under DMP ASLs control can lead to unpredictable operating system behavior and data corruption.

For hardware questions, refer to the hardware's documentation.

For full information on DMP ASLs functions and for information on adding DMP ASLs to a new or existing cluster with step-by-step instructions, see the *Veritas Storage Foundation 5.0 Administrator's Guide*.

Note that the general steps for adding DMP ASLs to any configuration are the same.

The steps are as follows:

- Install the new host adapter hardware, but make sure to connect only one path to the array storage.
- Install the software by selecting DMP ASLs as a part of the SFW or SFW HA installation process.
- At the end of the configuration process, after configuring the installation, bring the array under DMP ASLs control and attach the additional path.

Installing DMP ASLs on a new standalone server

Before running the installation, make sure that you have only one path to the array connected on each node.

Note: DMP ASLs run on 32-bit operating systems only.

To install DMP ASLs on a new standalone server

1. Install the necessary hardware and the appropriate drivers.
   See “Setting up DMP Array Support Libraries (ASLs)” on page 64.
2. Before installation, connect only one path from the array to the computer.
3. During installation, on the Option Selection page, under dynamic multi-pathing**,** select **DMP ASLs**.
4. Complete the installation and reboot the computer.
5. Include the disk array storage under DMP ASLs, connect the additional path from the computer, and rescan and verify that you can see the path.
   For details on this task, see the preceeding section.
   See “Including the disk array storage after installing DMP ASLs” on page 65.

Including the disk array storage after installing DMP ASLs

In this section, you bring the array storage under DMP ASLs control—you include it—and attach an additional path.

To include the disk array after installing DMP ASLs

1. Open the Veritas Enterprise Administrator by clicking **Start** > **Programs** > **Symantec** >**Veritas Storage Foundation > Veritas Enterprise Administrator**.
2. In the tree view under the Disks folder, select a disk from the storage array.
3. In the right pane, click the **Paths** tab for the disk. One path appears in the Paths tab.
4. Right-click the path and select **Array Settings** from the path context menu.
5. In the Array Settings window, clear the **Exclude** checkbox.
6. Using appropriate cables, connect the additional paths on the server to the switch and complete any switch configuration.
7. Rescan.

8 Verify that you can see the paths:
   - Open the Veritas Enterprise Administrator console.
   - In the System field, expand the Disks tree.
   - Click any external hard disk.
   - Above the console, click the DMP Paths tab.
   - Verify that the paths exist.

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

To support SFW HA and DMP ASLs simultaneously on a cluster, you must adhere to the following steps. Failure to follow these steps results in disk signature discrepancies, causing SFW HA or other applications to fail.

Before running the installation, make sure that you have only one path to the array connected on each node.

Note: DMP ASLs run on 32-bit operating systems only.

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

1 Install the necessary hardware.

2 Before installation, connect only one path from the array to the computer.

3 Install Storage Foundation HA 5.0 for Windows on all nodes in the cluster.

4 On the Option Selection page, under Dynamic Multi-pathing**,** select **DMP ASLs**.

5 Complete the installation, rebooting where necessary.

6 From the Veritas Enterprise Administrator, include the disk array storage under DMP ASLs:
   - In the tree view under the Disks folder, select a disk from the storage array.
   - In the right pane, click the **Paths** tab for the disk. One path appears in the Paths tab.
   - Right-click the path and select **Array Settings** from the path context menu.
   - In the Array Settings window, clear the **Exclude** checkbox.

7 Using appropriate cables, connect the additional paths on the server or servers to the switch and complete switch configuration.

8 Rescan.

9 Verify that you can see the additional paths:
  - Open the Veritas Enterprise Administrator console.
  - In the System field, expand the Disks tree.
  - Click any external hard disk.
  - Above the console, click the DMP Paths tab.
  - Verify that two paths exist.

10 Use the VEA and VCS wizards to complete the VCS cluster configuration.

Installing MSCS and DMP ASLs for the first time on a cluster

To support SFW MSCS and DMP ASLs simultaneously on a cluster, you must adhere to the following steps. Failure to follow these steps results in disk signature discrepancies, causing MSCS or other applications to fail.

Before running the installation, make sure that you have only one path to the array connected on each node.

Note: DMP ASLs run on 32-bit operating systems only.

To install SFW and MSCS on a cluster for the first time

1 Create the MSCS cluster.

2 Install Storage Foundation 5.0 for Windows.

3 On the Option Selection page, select **DMP ASLs** and the **MSCS** options.

4 Finish the wizard, rebooting where necessary.

5 From the Veritas Enterprise Administrator, include the disk array storage under DMP ASLs:
  - In the tree view under the Disks folder, select a disk from the storage array.
  - In the right pane, click the **Paths** tab for the disk. One path appears in the Paths tab.
  - Right-click the path and select **Array Settings** from the path context menu.
  - In the Array Settings window, clear the **Exclude** checkbox.

6 Using appropriate cables, connect the additional paths on the server or servers to the switch and complete switch configuration.

7 Rescan

8 Verify that you can see the following paths:

- Open the Veritas Enterprise Administrator console.
- In the System field, expand the Disks tree.
- Click any external hard disk.
- Above the console, click the DMP Paths tab.
- Verify that the paths exist.

9 Configure and set up the MSCS cluster.

Adding DMP ASLs to an existing standalone server

Follow these steps to add DMP ASLs to an existing standalone server.

To add DMP ASLs to an existing standalone server

1 Install additional hardware and confirm that only one path is attached to the disk array.

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

3 Select **Change or Remove Programs**.

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

5 The installer screen appears. Select **Add or Remove**. Click **Next**.

6 The Option Selection screen appears. Under Dynamic Multi-pathing, select **DMP Array Support Libraries (ASLs)**.
To add a license key for an option do the following:

- Click the **Add License** link located at the far right of the screen.
- The Add License link appears only for unlicensed options.
- In the pop-up window that appears, enter the license key for the option and click **OK**.
- Select the check box to add the option.

Click **Next**.

7 Finish the wizard, rebooting where necessary.

8 From the Veritas Enterprise Administrator, include the disk array storage under DMP ASLs:

- In the tree view under the Disks folder, select a disk from the storage array.
- In the right pane, click the **Paths** tab for the disk. Only one path should display in the Paths tab, since the disk is not yet under DMP ASLs control.
- Right-click the path and select **Array Settings** from the path context menu.

- In the Array Settings window, clear the **Exclude** checkbox.

9 Connect the path from the server.

10 Rescan.

11 Verify that you can see the paths:

- Open the Veritas Enterprise Administrator console.
- In the System field, expand the Disks tree.
- Click any external hard disk.
- Above the console, click the DMP Paths tab.
- Verify that the paths exist.

See "Including the disk array storage after installing DMP ASLs" on page 65.

Adding DMP ASLs to an existing SFW HA or SFW MSCS cluster

Symantec recommends that you perform a rolling installation for DMP ASLs on each node separately.

Note: DMP ASLs run on 32-bit operating systems only.

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

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

2 Install additional hardware and confirm that only one path is attached to the disk array.

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

4 Select **Change or Remove Programs**.

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

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

7 The Option Selection screen appears. Under Dynamic Multi-pathing, select **DMP Array Support Libraries (ASLs)**.
To add a license key for an option:

- Click the **Add License** link located at the far right of the screen.
- The Add License link appears only for unlicensed options.
- In the pop-up window that appears, enter the license key for the option and click **OK**.
- Select the check box to add the option and click **Next**.

8 Complete the wizard, rebooting where necessary.

9. From the Veritas Enterprise Administrator, include the disk array storage under DMP ASLs:
    - In the tree view under the Disks folder, select a disk from the storage array.
    - In the right pane, click the **Paths** tab for the disk. Only one path should display in the Paths tab, since the disk is not yet under DMP ASLs control.
    - Right-click the path and select **Array Settings** from the path context menu.
    - In the Array Settings window, clear the **Exclude** checkbox.
10. Using appropriate cables, connect the additional paths on the server or servers to the switch or array and complete any necessary configuration of the switch or array.
11. Rescan.
12. Verify that the paths exist:
    - Open the Veritas Enterprise Administrator console.
    - In the System field, expand the Disks tree.
    - Click any external hard disk.
    - Above the console, click the DMP Paths tab.
    - Verify that the paths exist.
13. Repeat the above procedure for other nodes.

Uninstalling DMP ASLs

If you plan to uninstall DMP ASLs or uninstall SFW or SFW HA with DMP ASLs, it is important that you detach all but the primary path to the array storage before you uninstall. If you are upgrading, you also need to limit the paths to the primary path.

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

To limit the paths under DMP ASLs to a single path

1. In SFW or SFW HA, exclude (make sure to check the Exclude check box) each multiple-path array from DMP ASLs management.
2. Physically remove all but the primary path from each multiple-path array.
3. Rescan.

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

See “Adding or removing features” on page 51.

For information on how to uninstall SFW or SFW HA, see “Uninstalling using the product installer” on page 53.

Section 2

Upgrading

This section includes the following chapters which describe the procedures used to upgrade to Veritas Storage Foundation for Windows 5.0 or Veritas Storage Foundation High Availability for Windows 5.0:

Upgrading to SFW 5.0

This chapter covers upgrading to Veritas Storage Foundation 5.0 for Windows (SFW 5.0). This chapter contains:

Before upgrading to SFW 5.0

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

Warning: Rules created using the SFW 4.x Rule Manager will not automatically be upgraded and will not work in SFW 5.0. See http://entsupport.symantec.com/docs/285845 for more information.

Checking the supported minimum product versions

To upgrade to SFW 5.0, your system must have version 4.1 or higher of SFW already installed. The previously installed version of SFW must meet the minimum product version, which the product installer checks before it upgrades.

If your current installation does not meet the minimum level required by the installer, you must manually apply the appropriate product upgrades to meet the minimum product level required before proceeding with the installer. You can get intermediate versions of the products on the Symantec Support site: http://entsupport.symantec.com. For license keys, contact Symantec Sales. You can also uninstall the older versions of the product and install the new product.

Preparing for the upgrade

Upgrading the product requires the following steps:

- Back up all your data in a safe location.
- Back up the system state.
- Check the hardware requirements for the software upgrade.
- Check to see if you need to update the Microsoft Active Directory to support the upgraded software. For example, upgrading from Microsoft Exchange 2000 to Exchange 2003 requires updating the Active Directory.
- Test the system after each upgrade, especially after applying product upgrades to meet the minimum version required. An incremental upgrade eases the troubleshooting process.

Additional upgrade information

This section includes the following information for upgrades with SFW and MSCS.

- During an upgrade, you might encounter messages while the installer validates the selected systems. These informational messages do not indicate an error. If an error occurs, the system’s status confirms the problem.
- To perform this upgrade, use a rolling upgrade procedure that involves installing SFW 5.0 on inactive nodes of the cluster. You then use the **Move Group** command in MSCS to move the active node and install SFW on the cluster’s remaining nodes.

Japanese language pack upgrade information

To upgrade the Japanese language pack, do the following tasks:

- Upgrade fully to SFW 5.0 using the English language disc in each of the following procedures.
- Use the Japanese language disc to upgrade the Japanese version of SFW 5.0.

Upgrading from previous 4.x versions

Follow these tasks in order when upgrading from SFW 4.1, 4.2, 4.3 or 4.3 MP1 to SFW 5.0.

If you have already installed and configured VVR or DMP, you must take the following steps before and after the upgrade to SFW 5.0.

- "Preparing a VVR environment for upgrading" on page 77
- "Preparing to add DMP to the upgraded environment" on page 78 *or* "Preparing an existing DMP environment for upgrading" on page 79
- "Preparing to add DMP DSMs to the upgraded environment" on page 79
- "Upgrading to SFW 5.0" on page 79
- "Re-enabling VVR after the upgrade" on page 86
- "Re-enabling DMP after the upgrade" on page 88
- "Upgrading dynamic disk groups" on page 89

Preparing a VVR environment for upgrading

If you use VVR to replicate data from a primary site to a secondary site, follow the procedures below to stop the replicated volume group (RVG) and detach the replication links (RLINKs).

To prepare the primary site

1. Stop the application that uses VVR to replicate data between the sites.
2. Open a command window by clicking **Start** > **Run**. In the Open field, enter **cmd**, and click **OK**.
3. Run the **vxprint -lVP** command on the primary site, where `Diskgroup` is *`diskgroup_name`*.
4. Stop the RVG to prevent the application from accessing or modifying the volumes during the upgrade. From the Veritas Enterprise Administrator console, right-click the RVG and select the **Disable Data Access** option from the menu that appears.
5. Verify that the data on the Replicator Log is written to the secondary site by running this command on the primary site.
   `vxrlink [-g`*diskgroup_name*`] status` ***`rlink_to_secondary`***
   Verify that the RLINKs are up-to-date before proceeding to the next step.
6. 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.

7 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.

To prepare the secondary site

1 Open a command window by clicking **Start** > **Run** in the taskbar. In the Open field, enter **cmd**, and click **OK**.

2 Run the **vxprint -lVP** command to find the RLINK and RVG names, where `Diskgroup` is *`diskgroup_name`*.

3 Stop RVG to prevent the application from accessing or modifying the volumes during the upgrade. From the Veritas Enterprise Administrator, right-click the RVG and select the **Disable data access** option from the menu that appears.

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

Preparing to add DMP to the upgraded environment

If you do not have DMP in your existing environment, but plan to add it while upgrading to SFW 5.0, add the host adapter hardware before performing the upgrade. Do not connect paths from the new host adapters to the array storage before upgrading to SFW and installing DMP. Select the DMP option in the Options screen while running the installer.

Refer to the Hardware Compliance List on the Symantec Support web site at http://entsupport.symantec.com to determine the approved hardware for SFW.

Note: DMP ASLs cannot co-exist with DMP DSMs. Uninstall DMP DSMs before installing DMP ASLs.

Warning: After the upgrade to SFW 5.0, place the array under the control of DMP before connecting additional data paths to shared storage. Attaching a second path and using storage that is not under DMP control can lead to unpredictable operating system behavior and data corruption.

Preparing an existing DMP environment for upgrading

If you have a previous installation of DMP on your system, detach all but the primary path to the array storage before you either upgrade the software or uninstall an older version of Volume Manager. For more information see the following:

- “Installing and uninstalling Veritas Dynamic Multi-pathing” on page 57.
- *Veritas Storage Foundation and High Availability Solutions 5.0 Solutions Guide*.

Preparing to add DMP DSMs to the upgraded environment

If you do not have DMP DSMs in your existing environment, but plan to add it while upgrading to SFW 5.0, add the host adapter hardware before performing the upgrade. Select the DMP DSMs option in the Options screen when you run the installer for the upgrade process. Before installing make sure that you have disconnected all but one path of the multipath storage to shorten installation time.

Refer to the Hardware Compliance List on the Symantec Support web site at http://entsupport.symantec.com to determine the approved hardware for SFW.

Note: DMP DSMs cannot co-exist with DMP ASLs. Uninstall DMP ASLs before installing DMP DSMs.

Upgrading to SFW 5.0

The installer can upgrade Volume Manager 4.x, SFW 4.1, 4.2, and 4.3 install options to SFW 5.0.

Changing driver signing options

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

Table 3-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers.

Table 3-1 Installation behavior with unsigned drivers

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

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

To change the driver signing options on each system

1 Log on locally to the system.

2 Open the Control Panel and click **System**.

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

4 In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.

5 Click **OK**.

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

Upgrading the software

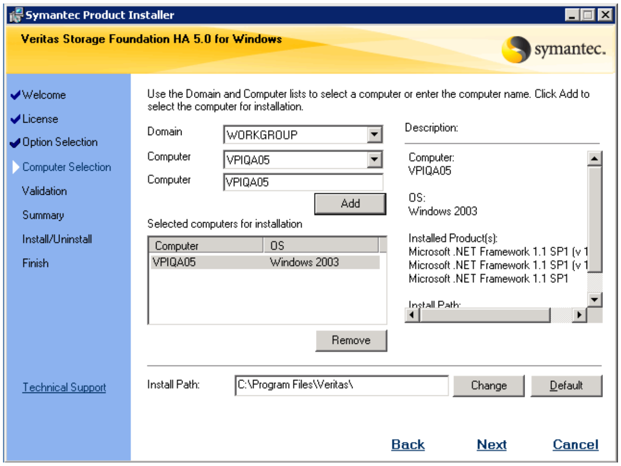
Use the product installer to upgrade the software.

To upgrade to SFW 5.0

1. Allow the autorun feature to start the installation or double-click **Setup.exe**.
2. Choose the default language for your installation and click **OK**.
3. Click **Storage Foundation 5.0 for Windows**.
4. Click the **Complete/Custom** link. The installer starts to copy files.
5. Review the Welcome window and click **Next**.
6. Read the License Agreement. If you agree to the license terms, click the **I accept the terms of the license agreement** radio button, and click **Next**.
7. Enter license keys for each Symantec product option that you are upgrading or installing:
   - Enter the license key in the top field.
   - To add a key, click **Add**. To remove a key, click the key to select it, and click **Remove**.
   - Repeat the first two bulleted steps for each Symantec product and feature that you want to install. Click a key to see its details.
   - Click **Next**.
8. Choose the options that you want to install by selecting or clearing the appropriate check boxes. You must select all currently installed options for upgrade. Click **Next**.

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

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



Use the Domain and Computer lists to select a computer or enter the computer name. Click Add to select the computer for installation.

Domain: WORKGROUP

Computer: VPIQA05

Computer: VPIQA05

Selected computers for installation

Computer	OS
VPIQA05	Windows 2003

Description:

Computer:
VPIQA05

OS:
Windows 2003

Installed Product(s):
Microsoft .NET Framework 1.1 SP1 (v 1
Microsoft .NET Framework 1.1 SP1 (v 1
Microsoft .NET Framework 1.1 SP1

Install Path:

Install Path: C:\Program Files\Veritas\

Domain

Select a domain from the list.

Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.

Computer

To add a computer for installation, select it from the Computer list or type the computer’s name in the Computer field. Then click **Add**.

To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**.

Click a computer’s name to see its description.

Install Path

Optionally, change the installation path.

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

10 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the

Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

11 If applicable, at the Veritas Dynamic Multi-pathing warning, do one of the following:

- For DMP ASLs installations—make sure that you have disconnected all but one path of the multipath storage to avoid data corruption.
- For DMP DSMs installations—the time required to install the Veritas Dynamic Multi-pathing DSMs feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, connect only one physical path during installation. After installation, reconnect additional physical paths before rebooting the system.

Click **OK**.

12 Review the pre-upgrade summary and click **Install**. Click **Back** to make necessary changes.

13 If the installation is successful on all computers, the installer automatically proceeds to the summary page described in step 14.

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

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

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

- Select the upgraded remote computers.
- Click **Reboot**.
- Click **Next**.

16 Click **Finish**.

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

- If you upgraded or installed the Volume Replicator (VVR) option, you can launch the wizard for Veritas Volume Replicator Security Service (VxSAS) after the reboot to configure security services for all computers.

  See “Configuring the VxSAS service (VVR only)” on page 84.

  For details on this required service for VVR, see the *Veritas Storage Foundation 5.0 Veritas Volume Replicator, Administrator's Guide*.

- After upgrading, reset the driver signing option to its original setting. Failure to do this can compromise system security. If you are performing more upgrades, do not reset the options until you have completed the upgrade.
  See "Resetting the driver signing options" on page 95.

Configuring the VxSAS service (VVR only)

Complete the following procedure to configure the VxSAS service for VVR.

The procedure has these prerequisites:

- You must be logged on with administrative privileges on the server for the wizard to be launched.
- The account you specify must have administrative and log-on as service privileges on all the specified hosts.
- Avoid specifying blank passwords. In a Windows Server 2003 environment, accounts with blank passwords are not supported for log-on service privileges.
- Make sure that the hosts on which you want to configure the VxSAS service are accessible from the local host.

Note: The VxSAS wizard 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 *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.
  The Welcome page appears. This page displays important information that is useful as you configure the VxSAS service. Read the information provided on the Welcome page and click **Next**.

2 Complete the Account Information wizard page as follows:

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

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

3 Select the required domain to which the hosts that you want to configure belong, from the Domain Selection wizard page.

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

After specifying the domain click **Next**.

4 Select the required hosts from the Host Selection page.

Selecting Hosts	The Available Hosts pane lists the hosts that are present in the specified domain. Select the required host by moving the appropriate name 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, then add it using the **Add Host** option. 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 the **Configure** button to proceed with configuring the VxSAS service.

5 After the configuration completes, the Configuration Results page is displayed. If the operation is successful then the Status column displays the appropriate message to indicate that the operation was successful.

If the operation was not successful then the page displays the status as failed and the corresponding details on why the account update failed. It

also displays the possible reasons for failure and recommendations on getting over the failure.
Click **Back** to change any information you had provided earlier.

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

Resetting the driver signing options

After completing the installation sequence, reset the driver signing options on each computer.

To reset the driver signing options

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

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

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

4 Click **OK**.

5 Repeat for each computer.

Re-enabling VVR after the upgrade

After upgrading an environment where VVR replicates data from a primary site to a secondary site.

To begin replication use the following procedures:

- For sites with VVR and a cluster (either VCS or MSCS) the steps to re-enable VVR in a cluster environment must be completed.
  See "Re-enabling VVR in a cluster environment after the upgrade".
- For sites without a cluster (VCS or MSCS), see "Re-enabling VVR in an environment without clusters"

Re-enabling VVR in a cluster environment after the upgrade

After performing an upgrade re-enable VVR in the cluster.

To enable the updated objects from the VCS java console

1 On the primary site, bring the RVG Service Group online. From the VCS Java Console, right-click the RVG Service Group and select the **Online** menu option.

2 On the secondary site, bring the RVG Service Group online. From the VCS Java Console, right-click the RVG Service Group and select the **Online** menu option.

3 On the primary site, bring the application Service Group online. From the VCS Java Console, right-click the application service group and select the **Online** menu option.

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

To enable the updated objects from the command line

1 Open a command window by clicking **Start > Run** in the taskbar. In the Open field, enter `cmd`, and click **OK**.

2 On the primary site, run the `hagrp` command to bring the RVG Service Group online.

```
hagrp -online group_name -sys system_name
```

3 On the secondary site, run the `hagrp` command to bring the RVG Service Group online.

```
hagrp -online group_name -sys system_name
```

4 On the primary site, run the `hagrp` command to bring the application Service Group online.

```
hagrp -online group_name -sys system_name
```

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

Re-enabling VVR in an environment without clusters

To enable the updated objects from VEA

1 Select the primary RVG, right-click, and select the **Enable Data Access** option from the menu.

2 Select the secondary RVG, right-click, and select the **Enable Data Access** option from the menu.

3 If needed, perform any necessary tasks to start the application. Depending on options in your environment, these tasks may include mounting databases or manually starting the application.

To enable the updated objects from the command line

1 Open a command window by clicking **Start > Run** in the taskbar. In the Open field, enter `cmd`, and click **OK**.

2. On the secondary site, enable data access to the volumes under RVG using the `vxrvg` command.

   ```
   vxrvg -g diskgroup start rvg_name
   ```

3. On the primary site, enable data access to the volumes under RVG using the `vxrvg` command.

   ```
   vxrvg -g diskgroup start rvg_name
   ```

4. If needed, perform any necessary tasks to start the application. Depending on options in your environment, these tasks may include mounting databases or manually starting the application.

Re-enabling DMP after the upgrade

Do not connect the second path to the storage (the second host bus adapter on each server connected to the SAN) until you have installed DMP and the storage array is included under DMP at the end of the configuration process. If you allow two paths to the storage without DMP control, data can become corrupted.

Warning: Always back up your data before upgrading.

To restore DMP protection to each dual-path array

Include each array that has multiple paths under DMP management from the Veritas Enterprise Administrator.

1. In the tree view under the **Disks** folder, select a disk from the storage array.
2. In the right pane, click the **Paths** tab for the disk. Only one path should display in the **Paths** tab because the disk is not yet under DMP control.
3. Right-click the path and select **Array Settings**.
4. In the Array Settings window, clear the **Exclude** check box.
5. Physically connect any additional paths that were disconnected previously.
6. Rescan the disks.

Upgrading dynamic disk groups

If your previous installation included Volume Manager 4.x, upgrade the disk group types to make use of the current program features.

See the *Veritas Storage Foundation 5.0 Administrator's Guide*.

Note: If you upgrade a disk group to SFW 5.0, you cannot import it to another server that is running an earlier version of Volume Manager or Disk Management. After upgrading a disk group, the group cannot revert to an earlier version.

To upgrade a dynamic disk group version

1. In the tree view, right-click the disk group you want to upgrade and select **Upgrade Dynamic Disk Group Version**.
2. Click **Yes** to upgrade the dynamic disk group.

In earlier versions of Volume Manager for Windows 2000 or Windows NT, you could have a dynamic disk group name longer than the 18-character limit put into effect with Volume Manager 3.0. If you upgrade the dynamic group version of such a disk group, you need to shorten the name. You may also need to create a name less than 18 characters if the disk group's volumes have long names.

Upgrading in an MSCS environment

In the MSCS environment, you can upgrade from VM 4.x, SFW 4.1 to SFW 5.0. This section applies to all of these upgrades.

When you upgrade from VM 4.x or from SFW 4.1 with Microsoft Cluster Server (MSCS) to SFW, SFW requires a reboot. Rebooting an active cluster node causes it to fail over. To avoid this, use a rolling installation. With a rolling installation, you upgrade first on an inactive cluster node, switch the active cluster node to a second node, and then upgrade the first node.

If DMP is installed and configured in your existing configuration, you have additional steps to take before and after the upgrade to SFW 5.0.

If VVR is installed and configured in your existing configuration, you have no additional steps to take to upgrade to SFW 5.0.

The DMP and operating system upgrade steps are optional and may not apply to your environment.

In this section, the two nodes in the cluster are Node A and Node B. Initially, Node A is the inactive cluster node and Node B is the active cluster node. After completing the following upgrade steps, Node A becomes the active cluster node. You can use the Cluster Administrator console to make Node B the active cluster node after finishing the upgrade.

To upgrade from VM 4.x, SFW 4.1 - 4.3 MP1 to SFW 5.0 in an MSCS configuration

1. For Node A, if you have DMP installed, follow the pre-upgrade procedures in, “Preparing an existing DMP environment for upgrading on Node A (Node B active)” on page 91.
2. For Node A, upgrade to SFW 5.0.
   See “Upgrading to SFW 5.0 on Node A (Node B active)” on page 91.
3. For Node A, if you have DMP installed, follow the post-upgrade procedures in, “Re-enabling DMP after the upgrade on Node A (Node B active)” on page 95.
4. Move the active node.
   See “Making Node A the active node” on page 96.
5. For Node B, if you have DMP installed, follow the pre-upgrade procedures in,“Preparing an existing DMP environment for upgrading on Node B (Node A active)” on page 96.
6. For Node B, upgrade to SFW 5.0.
   See “Upgrading SFW 5.0 on Node B (Node A active)” on page 96.
7. If you have DMP installed, follow the post-upgrade procedures in, “Re-enabling DMP after the upgrade on Node B (Node A active)” on page 97.
8. If you want to upgrade the dynamic disk groups, see “Upgrading dynamic disk groups (Node A active)” on page 97.

Preparing an existing DMP environment for upgrading on Node A (Node B active)

Make sure the active node of the cluster is Node B before starting this process.

Warning: Failure to limit paths to a single path that is under DMP control for an array, before upgrading or uninstalling, can lead to data corruption.

To limit the paths under DMP to a single path

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

After an array is excluded from DMP monitoring, the status of its paths in the Paths tab does not update. Thus, if a path fails after the array is excluded, its state may be displayed as Healthy in the Paths tab.

Upgrading to SFW 5.0 on Node A (Node B active)

Before you begin the upgrade do the following:

- Make sure the active Node of the cluster is Node B.
- Set the Windows driver signing options to ignore warning messages.

Changing driver signing options

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

Table 3-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers.

Table 3-2 Installation behavior with unsigned drivers

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

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

To change the driver signing options on each system

1. Log on locally to the system.
2. Open the Control Panel and click **System**.
3. Click the **Hardware** tab and click **Driver Signing**.
4. In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.
5. Click **OK**.
6. Repeat for each computer.
   If you do not change the driver signing option, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing option to its previous state.

Installing the software

Use the product installer to install the software.

To install SFW 5.0 on Node A

1. Navigate to the root directory of the CD and double-click **Setup.exe**.
2. Click **Storage Foundation 5.0 for Windows**.

3 Click **Complete/Custom** to upgrade the server components and optional client components.

4 On the Welcome page, click **Next**.

5 If you accept the terms of the license, click **Next**.

6 Enter a license key and click **Add**. To delete a key from the license key list, select it and click **Remove**.

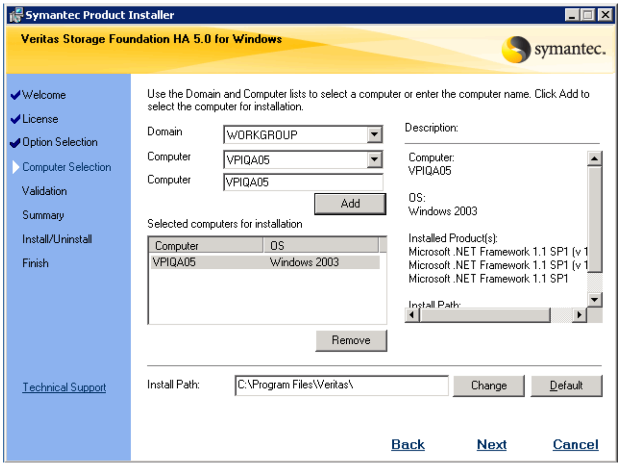
7 Make sure that you have a Symantec license for each product that you are upgrading. Select a key in the key list to view details about the specified license.

8 Click **Next**.

9 Select the MSCS option and other appropriate options (for example, DMP). Click **Next**.

10 Select the option to install client components and click **Next**.

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



Use the Domain and Computer lists to select a computer or enter the computer name. Click Add to select the computer for installation.

Domain: WORKGROUP

Computer: VPIQA05

Computer: VPIQA05

Selected computers for installation

Computer	OS
VPIQA05	Windows 2003

Description:

Computer:
VPIQA05

OS:
Windows 2003

Installed Product(s):
Microsoft .NET Framework 1.1 SP1 (v 1
Microsoft .NET Framework 1.1 SP1 (v 1
Microsoft .NET Framework 1.1 SP1

Install Path:

Install Path: C:\Program Files\Veritas\

Domain

Select a domain from the list.

Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.

Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description.
Install Path	Optionally, change the installation path. ■ To change the path, select a computer in the Selected computers for installation field, type the new path, and click **Change**. ■ To restore the default path, select a computer and click **Default**. The default path is: C:\Program Files\Veritas For 64-bit installations, the default path is: C:\Program Files (x86)\Veritas

12. After the installer validates the systems for the installation, click **Next**.
    If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.
13. Click **OK** to ensure optimal arbitration time settings for the dynamic quorum.
    The minimum and maximum time settings define the period that MSCS allows for quorum arbitration. Quorum arbitration is the process that occurs when the controlling node of the cluster is no longer active and other nodes of the cluster attempt to gain control of the quorum resource and the cluster.
14. Review the summary information and click **Install**. If necessary, click **Back** to make any necessary changes.
15. The progress meter indicates the status of the installation. If a security alert asks you to accept the Symantec driver software, click **Yes**.
    If the installation is successful on the system, the install report screen appears.
    If an installation is not successful on any one of the systems, the status screen shows that the installation failed. Click **Next** to view the install report.
16. Review the report and click **Next**.
17. Click **Finish**.
18. Reboot the local node.

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

Resetting the driver signing options

After completing the installation sequence, reset the driver signing options on each computer.

To reset the driver signing options

1. Open the Control Panel, and click **System**.
2. Click the **Hardware** tab and click **Driver Signing**.
3. In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.
4. Click **OK**.
5. Repeat for each computer.

Re-enabling DMP after the upgrade on Node A (Node B active)

Make sure the active node of the cluster is on Node B before starting this task.

Warning: Always back up your data before upgrading.

Do not connect the second path to the storage (second host bus adapter on each server connected to the SAN) until DMP is installed and the storage array is included under DMP at the end of the configuration process. If you allow two paths to the storage without DMP control, data can become corrupted.

To restore dynamic multipath protection to each dual-path array

1. In the Array Settings screen for the storage array tree view, select a disk from the storage array under the **Disks** folder.
2. In the right pane, click the **Paths** tab for the disk. Only one path should display in the **Paths** tab because the disk is not yet under DMP control.
3. Right-click the path and select **Array Settings**.
4. In the Array Settings window, clear the **Exclude** check box.
5. Physically connect any additional paths that were disconnected previously.
6. Rescan the disks.

See "Installing and uninstalling Veritas Dynamic Multi-pathing" on page 57.
See *Veritas Storage Foundation and High Availability Solutions 5.0 Solution Guide*.

To reapply the DMP registry setting (if upgrading to windows server 2003)

Reapply the VM 4.x, SFW 4.1 DMP registry setting that you previously saved to:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VXD
MPEMC
\Tunable.
```

Making Node A the active node

Do the following steps to make node A the active node.

To make Node A the active node

1. From the Cluster Administrator 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.

Preparing an existing DMP environment for upgrading on Node B (Node A active)

Make sure the active node of the cluster is Node A before starting this task.

To prepare an existing DMP environment for Node B, refer to the guidelines for Node A, see "Preparing an existing DMP environment for upgrading on Node A (Node B active)" on page 91.

Upgrading SFW 5.0 on Node B (Node A active)

Make sure the active node of the cluster is Node A before starting this task.

To upgrade SFW 5.0 on Node B, refer to the guidelines for Node A, see "Upgrading to SFW 5.0 on Node A (Node B active)" on page 91.

Re-enabling DMP after the upgrade on Node B (Node A active)

Make sure the active node of the cluster is Node A before starting this task.

To re-enable DMP after the upgrade on Node B, refer to the guidelines for Node A, see "Re-enabling DMP after the upgrade on Node A (Node B active)" on page 95.

Upgrading dynamic disk groups (Node A active)

Make sure the active node of the cluster is Server A before starting this task.

If your previous installation included Volume Manager 4.x or higher, upgrade the disk group types to make use of the current program features. The steps must be done on the active node.

See the *Veritas Storage Foundation 5.0 Administrator's Guide*.

Note: If you upgrade a disk group to SFW, you cannot import it to another server that is running an earlier version of Volume Manager or Disk Management. After upgrading a disk group, the group cannot revert to an earlier version.

To upgrade a dynamic disk group version

1. In the tree view of SFW 5.0 of the active node, right-click the disk group you want to upgrade and select **Upgrade Dynamic Disk Group Version**.
2. Click **Yes** to upgrade the dynamic disk group.
   In earlier versions of Volume Manager for Windows 2000 or Windows NT, you could have a dynamic disk group name longer than the 18-character limit put into effect with Volume Manager 3.0. If you upgrade the dynamic group version of such a disk group, you need to shorten the name. You may also need to create a name less than 18 characters if the disk group's volumes have long names.

Upgrading to SFW HA 5.0

This chapter covers upgrading from previous Veritas products to Veritas Storage Foundation HA 5.0 for Windows (SFW HA 5.0).

This chapter contains the following topics:

Before upgrading to SFW HA 5.0

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

Warning: Rules created using the SFW 4.x Rule Manager will not automatically be upgraded and will not work in SFW 5.0. See http://entsupport.symantec.com/docs/285845 for more information.

Further information on upgrading SFW HA in Microsoft Exchange, Microsoft SQL Server, and Oracle environments is available from the Symantec Support website.

See http://entsupport.symantec.com/docs/286178 for additional information about upgrading SFW HA in a Microsoft Exchange environment.

See http://entsupport.symantec.com/docs/286179 for additional information about upgrading SFW HA in a Microsoft SQL Server environment.

See http://entsupport.symantec.com/docs/286182 for additional information about upgrading SFW HA in an Oracle environment.

Checking the supported minimum product versions

To upgrade to SFW HA 5.0, your system must have version 4.1 or higher of SFW or SFW HA already installed. The previously installed products need to meet minimum product versions, which the product installer checks before it upgrades.

If your current installation does not meet the minimum level required by the installer, Symantec recommends manually applying 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. For license keys, contact Symantec Sales. You can also uninstall the older versions of the product and install the new product.

Preparing for the upgrade

When upgrading the product, perform the following tasks:

- Back up all your data in a safe location.
- Back up the system state.
- Check the hardware requirements for the software upgrade.
- Check to see if you need to update the Microsoft Active Directory to support the upgraded software. For example, upgrading from Microsoft Exchange 2000 to Exchange 2003 requires updating the Active Directory.
- Test the system after each upgrade, especially after applying product upgrades to meet the minimum version required. An incremental upgrade eases the troubleshooting process.

Additional upgrade information for VCS customers

While upgrading a configuration, the product installer performs the following tasks:

- Replaces the attribute types and names in the VCS 4.x configuration with those compatible with a SFW HA 5.0 configuration. For example, the Exchange application agent attribute E2kService is upgraded to ExchService.
- Maps default attribute values in a VCS 4.x configuration to the default attribute values in a VCS 5.0 configuration.
- Deletes attributes that are no longer required by SFW HA 5.0. For example, the wizard removes the AgentDebug attribute.

- Updates user passwords. Using a different encryption mechanism, SFW HA 5.0 decrypts the passwords and re-encrypts them using the VCS 5.0 encryption mechanism.

Japanese language pack upgrade information

When upgrading a previous version of the Japanese language pack, you must:

- Upgrade fully to SFW HA 5.0 using the English language disc in each of the following procedures.
- Use the Japanese language disc to upgrade the Japanese version of SFW HA 5.0.

Upgrading from previous 4.x versions

This section describes upgrading from SFW 4.1, or 4.2; or SFW HA 4.1, 4.2, 4.3 or 4.3 MP1. If you have already installed and configured VVR or DMP, you must take additional steps before and after the upgrade to SFW 5.0.

The following VVR and DMP upgrade procedures are optional and may not apply to your environment.

- "Preparing a VVR environment for upgrading" on page 102
- "Preparing to add DMP to the upgraded environment" on page 103 *or* "Preparing an existing DMP environment for upgrading" on page 103
- "Preparing to add DMP DSMs to the upgraded environment" on page 104
- "Preparing to upgrade to SFW HA 5.0" on page 105
- "Upgrading to SFW HA 5.0" on page 105
- "Optional tasks after a VCS upgrade" on page 112
- "Re-enabling VVR after the upgrade" on page 115
- "Re-enabling DMP after the upgrade" on page 117
- "Upgrading dynamic disk groups" on page 118

Preparing a VVR environment for upgrading

If you use VVR to replicate data from a primary site to a secondary site, follow the procedures below to stop the replicated volume group (RVG) and detach the replication links (RLINKs).

To prepare the primary site

1. Use Cluster Manager to take the application that uses VVR to replicate data between the sites offline.
2. Open a command window by clicking **Start** > **Run** in the taskbar. In the Open field, enter **cmd**, and click **OK**.
3. Run the **vxprint -lVP** command on the primary site, where `Diskgroup` is *`diskgroup_name`*.
4. Verify that the data on the Replicator Log is written to the secondary site by running the command on the primary site:

   `vxrlink [-g`*`diskgroup`*`] status` ***`rlink_to_secondary`***

   Verify that the RLINKs are up-to-date before proceeding to the next step.
5. Use Cluster Manager to take the VvrRvg resource offline in the VVR replication service group.
6. 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.
7. 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.

To prepare the secondary site

1. Use Cluster Manager to take the VvrRvg resource offline in the VVR replication service group.
2. Open a command window by clicking **Start** > **Run** in the taskbar. In the Open field, enter **cmd**, and click **OK**.
3. Run the **vxprint -lVP** command on the secondary site, where `Diskgroup` is *`diskgroup_name`*.
4. Disassociate the Replicator Log from the RVG. From the Veritas Enterprise Administrator, right-click the Replicator Log and select **Dissociate Replicator Log** option from the menu that appears.

Preparing to add DMP to the upgraded environment

If you do not have DMP in your existing environment, but plan to add it while upgrading to SFW HA 5.0, add the host adapter hardware before upgrading the SFW HA 5.0 software. Do not connect paths from the new host adapters to the array storage before upgrading to SFW HA and installing DMP. Select the DMP option in the Options screen while running the installer.

Refer to the Hardware Compliance List on the Symantec Support web site at http://entsupport.symantec.com to determine the approved hardware for SFW HA.

Note: DMP ASLs cannot co-exist with DMP DSMs. Uninstall DMP ASLs before installing DMP DSMs.

Warning: After completing the upgrade to SFW HA 5.0, make sure to place the array under the control of DMP before connecting additional data paths to shared storage. Attaching a second path and using storage that is not under DMP control can lead to unpredictable operating system behavior and data corruption.

Preparing an existing DMP environment for upgrading

If you have a previous installation of DMP on your system, detach all but the primary path to the array storage before you either upgrade the software or uninstall an older version of Volume Manager.

Physically remove all but the primary path of the multiple-path array. Using the VEA console, exclude each multiple-path array from DMP management and rescan the environment.

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

To limit the paths under DMP to a single path

1. Open the VEA console.
2. Display the Array Settings screen for the array you are excluding.
3. In the tree view under the Disks folder, select a disk from the storage array.
4. In the right pane, click the Paths tab for the disk.

5 Right-click a path and select Array Settings from the path context menu that appears.

6 In the Array Settings screen, check the **Exclude** check box.

7 Click **OK**. You have excluded the array from DMP control.

8 If VEA does not allow you to exclude the array, make sure that the primary path is the one remaining connection to the array.

9 Select **Actions** > **Rescan** from the VEA menu bar. It rescans the array and updates the display.

Uninstalling the DDI package

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

1 Make sure that only one path is attached for each array managed by DMP DSM.

2 Open the Windows Add/Remove Programs to uninstall the DDI. Select the Symantec support for DMP DSM entry and click **Remove** to begin the uninstallation.

3 Reboot the system when the uninstall process completes.

Preparing to add DMP DSMs to the upgraded environment

If you do not have DMP DSMs in your existing environment, but plan to add multi-pathing after upgrading to SFW 5.0, add the host adapter hardware before performing the upgrade. Select the appropriate DMP DSMs in the Options screen when you run the installer for the upgrade process. Before installing make sure that you have disconnected all but one path of the multipath storage to shorten installation time.

For a list of compatible hardware, see the Hardware Compatibility List located at: http://entsupport.symantec.com.

Note: DMP DSMs cannot co-exist with DMP ASLs. Uninstall DMP ASLs before installing DMP DSMs.

Preparing to upgrade to SFW HA 5.0

Before starting the upgrade process, use the VCS Java Console to “save and close” the VCS configuration. This operation involves saving the latest configuration to disk and changing the configuration state to read-only mode. You must also stop VCS before attempting the upgrade process. Perform these steps on both the VVR primary and secondary clusters.

To save and close the configuration

From the VCS Java Console, click **Save and Close Configuration** on the Cluster Explorer toolbar.

From the command prompt, type:

```
C:\> haconf -dump -makero
```

To take the service groups offline

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.

Repeat this command for all service groups that are online.

To stop VCS services

1. Stop HAD on all the cluster nodes. Type:

   ```
   C:\> hastop -all -force
   ```

2. Stop the Veritas VCSComm Startup service on all the cluster nodes. Type:

   ```
   C:\> net stop vcscomm
   ```

3. Stop GAB and LLT on all the cluster nodes. Type:

   ```
   C:\> net stop gab
   C:\> net stop llt
   ```

Upgrading to SFW HA 5.0

The installer automatically upgrades Volume Manager 4.x; SFW 4.1 or 4.2; or SFW HA 4.1, 4.2 or 4.3 to SFW HA 5.0. If the cluster has VCS enterprise agents and options, make sure to select the same enterprise agents and options while upgrading to SFW HA 5.0. If you do not want to include the enterprise agents and options in the upgraded cluster, uninstall the agents from the cluster before proceeding.

You must upgrade SFW HA on servers in a Windows 2000 or Windows Server 2003 domain; Symantec does not support Windows NT 4.0 domains.

Changing driver signing options

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

Table 4-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers.

Table 4-1 Installation behavior with unsigned drivers

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

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

To change the driver signing options on each system

1. Log on locally to the system.
2. Open the Control Panel and click **System**.
3. Click the **Hardware** tab and click **Driver Signing**.
4. In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.
5. Click **OK**.
6. Repeat for each computer.
   If you do not change the driver signing option, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing option to its previous state.

Upgrading the software

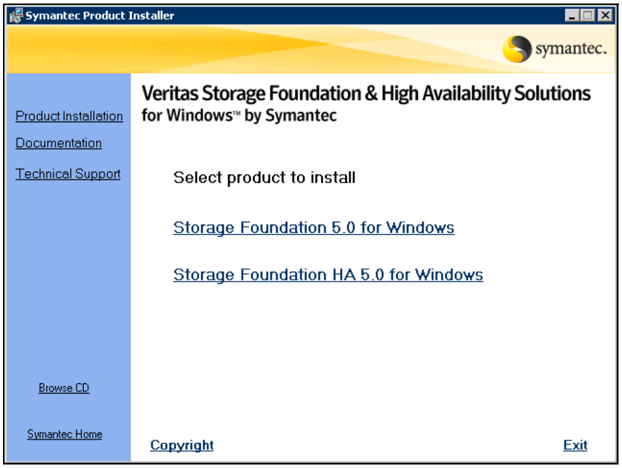
Use the product installer to upgrade the software.

To upgrade the product using the installer

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

2 Choose the default language for your installation and click **OK**. The Symantec product selection screen appears.

3 Click **Storage Foundation HA 5.0 for Windows**.



Veritas Storage Foundation & High Availability Solutions
for Windows™ by Symantec

Select product to install

Storage Foundation 5.0 for Windows

Storage Foundation HA 5.0 for Windows

4 Click **Complete/Custom** to begin installation. The **Administrative Console** link allows you to install only the Client components.

5 Review the welcome message and click **Next**.

6 If you agree to the terms of the license agreement, click **Next**.

7 Enter the license key for each Symantec product option that you are upgrading or installing in the top field.

8 To add a key, click **Add**.
To remove a key, click the key to select it, and click **Remove**.

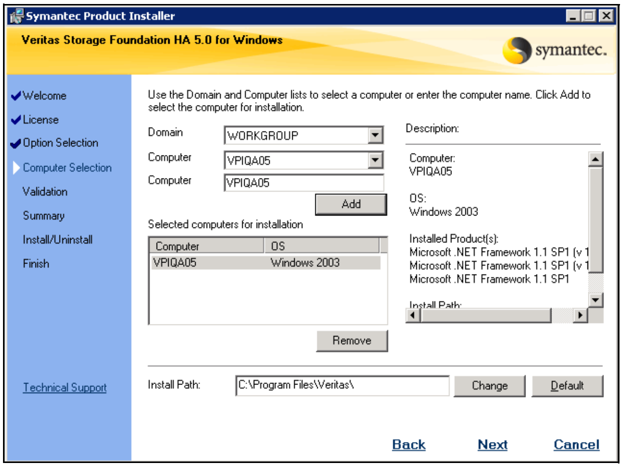
9 Repeat step 7 and step 8 for each Symantec product and feature that you want to install. Click a key to see its details.

10 Click **Next**.

11 Select the appropriate Storage Foundation HA options and click **Next**. If any previous VCS agents and options are installed on the node, make sure you select the same agents and options while upgrading. If you do not want to

include the agents and options in the upgraded cluster, uninstall them from the cluster before proceeding.

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



Use the Domain and Computer lists to select a computer or enter the computer name. Click Add to select the computer for installation.

Domain: WORKGROUP
Computer: VPIQA05
Computer: VPIQA05

Selected computers for installation

Computer	OS
VPIQA05	Windows 2003

Description:
Computer:
VPIQA05
OS:
Windows 2003
Installed Product(s):
Microsoft .NET Framework 1.1 SP1 (v 1
Microsoft .NET Framework 1.1 SP1 (v 1
Microsoft .NET Framework 1.1 SP1
Install Path:

Install Path: C:\Program Files\Veritas\

Domain

Select a domain from the list.

Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.

Computer

To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**.

To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**.

Click a computer's name to see its description.

Install Path

Optionally, change the installation path.

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

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

14 If applicable, at the Veritas Dynamic Multi-pathing warning, do one of the following:

- For DMP ASLs installations—make sure that you have disconnected all but one path of the multipath storage to avoid data corruption.
- For DMP DSMs installations—the time required to install the Veritas Dynamic Multi-pathing DSMs feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, connect only one physical path during installation. After installation, reconnect additional physical paths before rebooting the system.

Click **OK**.

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

16 If the installation is successful on all nodes, the installer automatically proceeds to the summary page.

Click **Next** after the progress indicator shows the installation is complete to proceed to the summary report in order to review the details of the failed installation. Note that if a security alert asks you to accept the Symantec driver software, click **Yes**.

17 Review the installation report, taking action where necessary, and click **Next**.

18 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Select the upgraded remote computers and click **Reboot**.

Wait for the remote computer to come back online. Click **Next**.

19 Click **Finish**.

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

- If you upgraded or installed the Volume Replicator (VVR) option, you can launch the wizard for Veritas Volume Replicator Security Service (VxSAS) after the reboot to configure security services for all nodes.
  See "Configuring the VxSAS service (VVR only)" on page 110.
- If you did not change the driver signing options for the remote Windows Server 2003 systems and you need to configure VxSAS see, "Configuring the VxSAS service (VVR only)" on page 110."

Configuring the VxSAS service (VVR only)

Complete the following procedure to configure the VxSAS service for VVR.

The procedure has these prerequisites:

- You must be logged on with administrative privileges on the server for the wizard to be launched.
- The account you specify must have administrative and log-on as service privileges on all the specified hosts.
- Avoid specifying blank passwords. In a Windows Server 2003 environment, accounts with blank passwords are not supported for log-on service privileges.
- Make sure that the hosts on which you want to configure the VxSAS service are accessible from the local host.

Note: The VxSAS wizard 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 *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.
The Welcome page appears. This page displays important information that is useful as you configure the VxSAS service. Read the information provided on the Welcome page and click **Next**.

2 Complete the Account Information wizard page as follows:

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

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

3 Select the required domain to which the hosts that you want to configure belong, from the Domain Selection wizard page.

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

After specifying the domain click **Next**.

4 Select the required hosts from the Host Selection page.

Selecting Hosts	The Available Hosts pane lists the hosts that are present in the specified domain. Select the required host by moving the appropriate name 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, then add it using the **Add Host** option. 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 the **Configure** button to proceed with configuring the VxSAS service.

5 After the configuration completes, the Configuration Results page is displayed. If the operation is successful then the Status column displays the appropriate message to indicate that the operation was successful.

If the operation was not successful then the page displays the status as failed and the corresponding details on why the account update failed. It also displays the possible reasons for failure and recommendations on getting over the failure.

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

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

Resetting the driver signing options

After completing the installation sequence, reset the driver signing options on each computer.

To reset the driver signing options

1. Open the Control Panel, and click **System**.
2. Click the **Hardware** tab and click **Driver Signing**.
3. In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.
4. Click **OK**.
5. Repeat for each computer.

Optional tasks after a VCS upgrade

The following tasks are optional depending on your cluster configuration.

Including custom resources in the upgraded cluster

The VCS Configuration Wizard does not upgrade custom resources. If a service group in the previous configuration contains custom resources, the wizard does not include the service group in the upgraded cluster.

To include a service group with custom resources in the upgraded cluster

1. Make sure the agent binaries for the custom agent are available under *%VCS_HOME%*`\bin` where the variable *%VCS_HOME%* represents the VCS installation directory, typically `C:\Program Files\Veritas\cluster server`.
2. Stop the VCS engine (HAD) on all the nodes in the cluster. From the command prompt, type:
   C:\> **`hastop -all -force`**
3. During installation of the SFW HA 5.0 software, the installer copies previous configuration files to a backup location. Locate the backed up types.cf and main.cf files: `C:\Documents and Settings\All Users\Application Data\Veritas\cluster server\vpibackup`.
4. Copy the resource type definition for the custom resource from the backed up types.cf and add it to the types.cf file for the VCS 5.0 cluster.
5. Copy the service group configuration containing the custom resource from the backed up main.cf and add it to the main.cf file for the VCS 5.0 cluster.
6. If resources for a custom resource type are dependent on resources for agents bundled with VCS 5.0, you must update the resource definition of the

VCS bundled agent to include the new attributes or remove the deprecated attributes.

For information on new and deprecated attributes see the *Veritas Storage Foundation and High Availability Solutions 5.0 Release Notes*.

For information on the attribute values and descriptions see the *Veritas Cluster Server 5.0 Bundled Agents Reference Guide*.

7 Verify the configuration. Type:

```
C:\> hacf -verify config_directory
```

The variable `config_directory` refers to the path of the directory containing the main.cf and types.cf.

8 Start the VCS engine (HAD) on the node where you changed the configuration. Type the following at the command prompt:

```
C:\> hastart
```

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

Adding a GCO resource to the ClusterService group

VCS 5.0 provides the Global Cluster Option to enable a collection of VCS clusters to work together for wide-area disaster recovery. See the *Veritas Cluster Server 5.0 Administrator's Guide*.

Establishing secure communication within the global cluster

A global cluster is created in non-secure mode by default. If the local clusters are running in secure mode, you may continue to allow the global cluster to run in non-secure mode or choose to establish secure communication between clusters.

The following prerequisites are required for establishing secure communication within a global cluster:

- The clusters within the global cluster must be running in secure mode.
- You must have Administrator privileges for the domain.

The following information is required for adding secure communication to a global cluster:

- The active host name or IP address of each cluster in the global configuration.
- The user name and password of the administrator for each cluster in the configuration.
- If the local clusters do not point to the same root broker, the host name and port address of each root broker.

Adding secure communication involves the following tasks:

- Taking the ClusterService-Proc (wac) resource in the ClusterService group offline on the clusters in the global environment.
- Adding the -secure option to the StartProgram attribute on each node.
- Establishing trust between root brokers if the local clusters do not point to the same root broker.
- Bringing the ClusterService-Proc (wac) resource online on the clusters in the global cluster.

To take the ClusterService-Proc (wac) resource offline on all clusters

1. From Cluster Monitor, log on to a cluster in the global cluster.
2. In the **Service Groups** tab of the Cluster Explorer configuration tree, expand the **ClusterService** group and the Process agent.
3. Right-click the **ClusterService-Proc** resource, click **Offline**, and click the appropriate system from the menu.
4. Repeat step 1 to step 3 for the additional clusters in the global cluster.

To add the -secure option to the StartProgram resource

1. In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the **ClusterService-Proc** resource under the **Process** type in the **ClusterService** group.
2. Click **View**, and then **Properties** view.
3. Click the Edit icon to edit the **StartProgram** attribute.
4. In the Edit Attribute dialog box, add `-secure` switch to the path of the executable Scalar Value. For example:
   ```
   C:\Program Files\Veritas\Cluster Server\bin\wac.exe -
   secure
   ```
5. Repeat step 4 for each system in the cluster.
6. Click **OK** to close the Edit Attribute dialog box.
7. Click the **Save and Close Configuration** icon in the tool bar.
8. Repeat step 1 to step 7 for each cluster in the global cluster.

To establish trust between root brokers if there is more than one root broker

- ◆ Establishing trust between root brokers is only required if the local clusters do not point to the same root broker.

  Log on to the root broker for each cluster and set up trust to the other root brokers in the global cluster. The complete syntax of the command is:

```
vssat setuptrust --broker <host:port> --securitylevel
<low|medium|high> [--hashfile <filename> | --hash <root
hash in hex>]
```

For example, to establish trust with a low security level in a global cluster comprised of Cluster1 pointing to RB1 and Cluster2 pointing to RB2:

from RB1, type:

```
vssat setuptrust --broker RB2:14141 --securitylevel low
```

from RB2, type:

```
vssat setuptrust --broker RB1:14141 --securitylevel low
```

To bring the ClusterService-Proc (wac) resource online on all clusters

1. In the **Service Groups** tab of the Cluster Explorer configuration tree, expand the **ClusterService** group and the Process agent.
2. Right-click the **ClusterService-Proc** resource, click **Online**, and click the appropriate system from the menu.
3. Repeat step 1 and step 2 for the additional clusters in the global cluster.

Re-enabling VVR after the upgrade

After upgrading an environment where VVR replicates data from a primary site to a secondary site, use the following procedures to begin replication.

- For sites with VVR and a cluster (either VCS or MSCS), before preparing the cluster, complete the VVR steps in: “Re-enabling VVR in a cluster environment after the upgrade”.
- For sites without a cluster (VCS or MSCS), proceed to: “Re-enabling VVR in an environment without clusters”

Re-enabling VVR in a cluster environment after the upgrade

To enable the updated objects from the VCS Java Console

1. On the primary site, bring the RVG Service Group online. From the VCS Java Console, right-click the RVG Service Group and select the **Online** menu option.
2. On the secondary site, bring the RVG Service Group online. From the VCS Java Console, right-click the RVG Service Group and select the **Online** menu option.
3. On the primary site, bring the application Service Group online. From the VCS Java Console, right-click the application service group and select the **Online** menu option.

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

To enable the updated objects from the command line

1 Open a command window by clicking **Start > Run** in the taskbar. In the Open field, enter `cmd`, and click **OK**.

2 On the primary site, run the `hagrp` command to bring the RVG Service Group online.

```
hagrp -online group_name -sys system_name
```

3 On the secondary site, run the `hagrp` command to bring the RVG Service Group online.

```
hagrp -online group_name -sys system_name
```

4 On the primary site, run the `hagrp` command to bring the application Service Group online.

```
hagrp -online group_name -sys system_name
```

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

Re-enabling VVR in an environment without clusters

To enable the updated objects from VEA

1 Select the primary RVG, right-click, and select the **Enable Data Access** option from the menu.

2 Select the secondary RVG, right-click, and select the **Enable Data Access** option from the menu.

3 If needed, perform any necessary tasks to start the application. Depending on options in your environment, these tasks may include mounting databases or manually starting the application.

To enable the updated objects from the command line

1 Open a command window by clicking **Start > Run** in the taskbar. In the Open field, enter `cmd`, and click **OK**.

2 On the secondary site, enable data access to the volumes under RVG using the `vxrvg` command.

```
vxrvg -g diskgroup start rvg_name
```

3 On the primary site, enable data access to the volumes under RVG using the `vxrvg` command.

```
vxrvg -g diskgroup start rvg_name
```

If needed, perform any necessary tasks to start the application. Depending on options in your environment, these tasks may include mounting databases or manually starting the application.

Reconnecting DMP DSM paths after the upgrade

Once you have finished upgrading SFW HA, reconnect all paths to the DMP DSM array.

Re-enabling DMP after the upgrade

Do not connect the second path to the storage (second host bus adapter on each server connected to the SAN) until DMP is installed and the storage array is included under DMP at the end of the configuration process. If you allow two paths to the storage without DMP control, data can become corrupted.

Warning: Back up your data before proceeding.

To re-enable DMP after the upgrade

With SFW HA on the first server, bring up DMP and include the disks on the storage array. To include the storage array:

1 From the Veritas Enterprise Administrator, display the Array Settings screen for the storage array with the following steps:

  - In the tree view under the **Disks** folder, select a disk from the storage array.
  - In the right pane, click the **Paths** tab for the disk. Only one path should display in the **Paths** tab because the disk is not yet under DMP control.
  - Right-click the path and select **Array Settings**.

2 In the Array Settings window, clear the **Exclude** check box.

3 Using appropriate cables, connect the second path on the server to the second switch:

  - Connect the path through the second HBA and second controller of the storage array.
  - Complete any necessary configuration of the switch.

4 Rescan the disks and verify that two paths are shown in the Paths tab of the DMP GUI. Access the Array Settings dialog for the storage array and make sure that the array load balancing settings are set to Active/Passive. A cluster disk requires the Active/Passive settings.

5 Repeat this procedure for the additional nodes.

Upgrading dynamic disk groups

If your previous installation included Volume Manager 4.x, upgrade the disk group types to make use of the current program features.

See the *Veritas Storage Foundation 5.0 Administrator's Guide*.

Note: If you upgrade a disk group to SFW HA 5.0, you cannot import it to another server that is running an earlier version of Volume Manager or Disk Management. After upgrading a disk group, the group cannot revert to an earlier version.

To upgrade a dynamic disk group version

1 In the tree view, right-click the disk group you want to upgrade and select **Upgrade Dynamic Disk Group Version**.

2 Click **Yes** to upgrade the dynamic disk group.

Chapter 5

Microsoft Service Pack upgrades

This chapter contains:

Configuring Microsoft Exchange 2003 SP2 in a VCS Environment

This section covers configuring Microsoft Exchange 2003 SP2 in a VCS environment, if you already have Microsoft Exchange 2003 installed and you want to apply Exchange 2003 SP2.

Upgrading to Microsoft Exchange 2003 SP2

This section covers upgrading Microsoft Exchange installation in a VCS cluster.

Prerequisites

Prerequisites to upgrading to Microsoft Exchange 2003 SP2 are as follows:

- Make sure to set the "DetailMonitor" attribute of all "ExchService" type resources to zero.
- Make sure the cluster is configured to run in a non-secure mode before installing the service pack.

Perform the following steps to upgrade Exchange 2003 installation on a node that is part of the Exchange service group. Make sure all the nodes, which are part of the Exchange service group, have the same version and service pack level as Microsoft Exchange.

To upgrade to Microsoft Exchange 2003 SP2

Make sure that you do not mount the Exchange databases on the failover nodes.

1. Bring the Exchange service group on the node where you are upgrading the Exchange installation online.
2. Stop HAD on the node where Exchange installation will be upgraded. At the command prompt, type:
   ```
   C:\> hastop -local -force
   ```
3. Install Microsoft Exchange 2003 SP2 on the node where the service group is online. If prompted to install the hotfix for Internet Information Services (IIS) 6.0, refer to the Microsoft Knowledge Base Article: 831464.
4. Start HAD on the node. At the command prompt, enter:
   ```
   C:\> hastart
   ```
5. Repeat step 1 through step 4 on all remaining nodes that are part of the Exchange service group.
6. Update the ExchConfig registry information on every system where Exchange is upgraded. To update the registry on the local system from the command line enter:
   ```
   Setup.exe /UpdateExchVersion
   ```
   To update the registry on more than one system enter:
   ```
   Setup.exe /UpdateExchVersion system_name1 system_name2
   ...
   ```

Configuring Microsoft SQL 2000 service pack 4 in a VCS environment

This section outlines the procedure needed to install Microsoft SQL 2000 Server Service Pack 4 on a computer running Veritas Storage Foundation HA for Windows 5.0.

Consider the following points before applying Microsoft SQL 2000 Service Pack 4 to a production server:

- Make sure that you have a recent backup of your system and user databases.
- Server down time is required for this procedure.

Note: This procedure assumes you have a recent flat-file backup of the MSSQL Data Files directory on the shared disk, in this example, S:\MSSQL$SQL2000.SP3A, and that your current SQL directory is called S:\MSSQL$SQL2000, in this example, on the same drive letter. If yours are named differently, substitute your directory names where appropriate.

To install Microsoft SQL 2000 server service pack 4

1. From the Veritas Cluster Manager Console, right-click the SQL Server Service Group and select **Offline** on all nodes.
2. On the node where the SQL Server Service Group was taken offline, online the MountV resource for the shared drive containing the SQL databases (for example, S:\MSSQL$SQL2000).
3. On the shared disk, make a copy of your recent MSSQL data files directory (S:\MSSQL$SQL2000) and rename it, for example to S:\MSSQL$2000.SP3A.
4. From the Veritas Cluster Manager Console, right-click the SQL Server Service Group which is now online, and select **Freeze >Persistent**.
5. Install Microsoft SQL 2000 Service Pack 4 on the active node (where the SQL Server Service Group is online), using the instructions provided by Microsoft.
6. Repeat step 5 for each additional SQL instance in this service group, if you have more than one instance in this service group.
7. From the Veritas Cluster Manager Console, right-click the SQL Server Service Group which is still online and select **Unfreeze**.
8. From the Veritas Cluster Manager Console, right-click the SQL Server Service Group and select **Offline** on the node where it was online.
9. In a Disaster Recovery environment, switch the Replication Service Group to one of the other, additional or failover, nodes in this cluster.
10. On the failover node, online the MountV resource for the shared drive containing the SQL databases (for example, S:\MSSQL$SQL2000).
11. On the shared disk, rename the S:\MSSQL$SQL2000 directory to S:\MSSQL$SQL2000.SP4. If S:\MSSQL$SQL2000.SP4 already exists on the shared disk, then delete it before renaming the S:\MSSQL$SQL2000 directory.
12. On the shared disk, rename the S:\MSSQL$SQL2000.SP3A directory to S:\MSSQL$SQL2000. If there are additional nodes in this cluster to be updated, copy the S:\MSSQL$SQL2000.SP3A directory to S:\MSSQL$SQL2000 instead of renaming the directory.

13 From the Veritas Cluster Manager Console, right-click the SQL Server Service Group which is now online and select **Freeze >Persistent**.

14 Install Microsoft SQL 2000 Service Pack 4 on the active node (where the SQL Server Service Group is online), using the instructions provided by Microsoft.

15 Repeat step 14 for each additional SQL instance in this service group, if you have more than one instance in this service group.

16 From the Veritas Cluster Manager Console, right-click the SQL Server Service Group which is still online and select **Unfreeze**.

17 From the Veritas Cluster Manager Console, right-click the SQL Server Service Group and select **Offline** on the node where it was online.

18 Repeat step 9 through step 17 on each additional node if more than two SQL 2000 nodes are in use.

19 For a Disaster Recovery environment, repeat this procedure at the secondary site.

20 When Microsoft SQL 2000 Server Service Pack 4 has been completely installed on all nodes, test user connectivity to the instances.

21 Test the SQL Server Service Group by bringing it online and failing it over from node to node. When testing is complete, the upgrade is complete.

22 If more than one SQL Server Service Group is present, repeat this entire procedure for each SQL Server Service Group.

Configuring Microsoft SQL 2005 service pack 1 in a VCS environment

This section outlines the procedure needed to install Microsoft SQL 2005 Server Service Pack 1 on a computer running Veritas Storage Foundation HA for Windows 5.0.

Consider the following points before applying Microsoft SQL 2005 Server Service Pack 1 to a production server:

- Make sure that you have a recent backup of your system and user databases.
- Server down time is required for this procedure.

Note: This procedure assumes you have a recent flat-file backup of the MSSQL Data Files directory on the shared disk, in this example, S:\Microsoft SQL Server, and that your current SQL directory is called S:\MSSQL$SQL2000, in this example, on the same drive letter. If yours are named differently, substitute your directory names where appropriate.

To install Microsoft SQL 2005 server service pack 1

1. From the Veritas Cluster Manager Console, 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 Veritas Cluster Manager Console, right-click the SQL Server Service Group which is now online, and select **Freeze >Persistent**.
4. Verify that the VVR RVG service group is online on the node where Microsoft SQL 2005 Service Pack 1 is to be installed. 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.
   See the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL*.
5. Repeat step 5 for each additional SQL instance in this service group, if you have more than one instance in this service group.
6. From the Veritas Cluster Manager Console, right-click the SQL Server Service Group which is still online and select **Unfreeze**.
7. From the Veritas Cluster Manager Console, right-click the SQL Server Service Group and select **Offline** on the node where it was online.

8 On the failover node, online the SQL 2005 resource for the shared drive containing the SQL databases.

9 From the Veritas Cluster Manager Console, right-click the SQL Server Service Group which is now online and select **Freeze >Persistent**.

10 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.

11 Repeat step 14 for each additional SQL instance in this service group, if you have more than one instance in this service group.

12 From the Veritas Cluster Manager Console, right-click the SQL Server Service Group which is still online and select **Unfreeze**.

13 From the Veritas Cluster Manager Console, right-click the SQL Server Service Group and select **Offline** on the node where it was online.

14 Optionally reboot and online each service group to verify the database connect for each node.

15 Repeat step 9 through step 17 on each additional node if more than two SQL 2005 nodes are in use.

16 For a Disaster Recovery environment, repeat this procedure at the secondary site.

17 When Microsoft SQL 2005 Server Service Pack 1 has been completely installed on all nodes, test user connectivity to the instances.

18 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.

19 If more than one SQL Server Service Group is present, repeat this entire procedure for each SQL Server Service Group.

Section 3

Appendix

This section includes an appendix which describes the Symantec Licensing Inventory Agent:

- Appendix A, "Configuring the Symantec License Inventory Agent" on page 127

Appendix A

Configuring the Symantec License Inventory Agent

This appendix includes the following topics:

About the Symantec License Inventory Manager

The Symantec License Inventory Manager (license inventory manager) is an enterprise asset management tracking tool. It inventories Symantec Information Availability products in your network and consolidates critical information on the deployment of these products. You can use the information to:

- Determine all the Symantec software products and licenses being used in your enterprise
- Achieve easier license self-compliance management
- Know your Enterprise License Agreement deployment status
- Reduce administrative overhead for managing license compliance
- Renew the support and maintenance agreements that are based on the licenses you have deployed
- Gain more control over your Symantec software usage
- Manage the department chargebacks based on actual software usage

- Use more flexible licensing and pricing models
- Exploit detailed deployment data to perform return on investment analyses for purchased software

The license inventory manager is a three-tiered system that consists of a server tier, access point tier, and an agent tier. The server tier is the Symantec License Inventory Server, which consolidates and stores the information that it gathers from the agents and access points.

The optional access point tier includes Symantec License Inventory Access Points and serves as a consolidation layer between the agents and server.

The agent tier includes Symantec License Inventory Agents, which are deployed on individual hosts in a network. Each agent gathers product information on the supported Symantec products that are installed on the agent's host. The agents then send the information they have gathered to an access point or the server.

When the Symantec License Inventory Agent is installed

The Symantec License Inventory Manager is installed using installation media available separately. To order a Symantec License Inventory Manager license and installation media kit, contact your Symantec sales representative.

The installation media provides online documentation for the Symantec License Inventory Manager. You can order printed copies of the documentation from your sales representative. The documents you can order include:

- *Symantec License Inventory Manager Installation and Configuration Guide*
- *Symantec License Inventory Manager Administrator's Guide*
- *Symantec License Inventory Manager User's Guide*

The installation media provides online documentation with details on all of the topics that are discussed in this appendix.

For the latest information on updates, patches, and software issues regarding this product, read the release notes located at:

http://entsupport.symantec.com/docs/285602

The Symantec product installer installs or upgrades the agent on the host with the Symantec product. The agent is installed in the following folder:

```
C:\Program Files\Veritas\License Inventory Manager\Agent
```

The agent is installed with a default configuration that minimizes its impact on a running system. The minimum configuration prevents remote communication with the agent to keep its data and interfaces secure.

When the server and access points are installed

The server and access points are not installed automatically. If you want to use the Symantec License Inventory Manager, you must manually install the server and, optionally, the access points. After you install the server and access points, the agents can gather information and you can create inventory reports.

You can install the server and access points from the Symantec License Inventory Manager installation media.

What you can do with the agent

After the agent is installed, you can use it to track Symantec products on the system on which it was installed. You can remove the agent if you choose not to use it.

To use the agent, however, you must manually configure it to enable remote communication between the agent and its server or access point. Complete instructions for reconfiguring the agent are provided in the *Symantec License Inventory Manager 4.2 Release Notes*. You can download this document from the following URL: http://entsupport.symantec.com/docs/285602

How to remove the agent

If you do not want to use the Symantec License Inventory Manager, you can remove the agent using Add/Remove Programs. It is listed as the Symantec License Inventory Agent program in Add/Remove Programs.

Later, you can reinstall the agent with the Symantec License Inventory Manager installation disc. This disc is available in the Symantec License Inventory Manager kit.

Index