Veritas™ Cluster Server Installation and Upgrade Guide

Windows

6.1

Symantec™

Veritas™ Cluster Server Installation and Upgrade Guide

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

Product version: 6.1

Document version: 6.1 Rev 2

Legal Notice

Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization

- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information

- Upgrade assurance that delivers software upgrades

- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis

- Premium service offerings that include Account Management Services

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

- Hardware information

- Available memory, disk space, and NIC information

- Operating system

- Version and patch level

- Network topology

- Router, gateway, and IP address information

- Problem description:

    - Error messages and log files

    - Troubleshooting that was performed before contacting Symantec

    - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

- Questions regarding product licensing or serialization

- Product registration updates, such as address or name changes

- General product information (features, language availability, local dealers)

- Latest information about product updates and upgrades

- Information about upgrade assurance and support contracts

- Information about the Symantec Buying Programs

- Advice about Symantec's technical support options

- Nontechnical presales questions

- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

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

Documentation

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

doc_feedback@symantec.com

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

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

About Symantec Connect

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

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

Contents

Preinstallation and planning

This chapter includes the following topics:

- About the preinstallation and planning tasks

- Installation requirements

- Supported applications

- Verifying the system configuration using the Windows Data Collector

- Licensing

- Planning a VCS installation

About the preinstallation and planning tasks

Before you begin to install VCS, you must perform the following tasks as a part of product installation planning:

- Review the release notes for your product.

- Review the product installation requirements.

- Review the supported hardware and software list.

- Review the licensing details.

- Review the specific requirements for your configuration.

- Perform the applicable pre-requisite tasks.

- For latest updates refer to the Late Breaking News (LBN)
  http://www.symantec.com/docs/TECH161556

■ Exit all running applications.

Installation requirements

Review the following product installation requirements for your systems.

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

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

Operating system requirements

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

■ Supported operating systems for VCS for Windows servers

■ Supported operating systems for VCS for Windows clients

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

http://www.symantec.com/docs/TECH209010

Supported operating systems for server components

Your server must run one of the operating systems listed below to install the VCS server components.

Note: VCS does not support Hyper-V and parent partitions.

Table 1-1   Supported operating systems for servers

Windows Server	Platform	Edition	Version
Windows Server 2008 R2 Server Core	x64		SP1
Windows Server 2008 R2	x64	Standard, Enterprise, Datacenter	SP1
Windows Web Server 2008 R2	x64		SP1

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

Windows Server	Platform	Edition	Version
Windows Small Business Server 2008 R2	x64	Standard, Premium	SP1
Windows Server 2012 Server Core	x64	Standard, Datacenter, Foundation, Essential, Hyper-V	RTM or SP1
Windows Server 2012	x64	Standard, Datacenter, Foundation, Essential, Hyper-V	RTM or SP1
Windows Server 2012 R2 Server Core	X64	Standard, Datacenter, Hyper-V	RTM
Windows Server 2012 R2	X64	Standard, Datacenter, Hyper-V	RTM

Supported operating systems for client components

Your system must run one of the following operating systems to install the VCS client components:

- Any one of the operating system versions, editions, and architectures that the Server Components are supported on except Server Core:
  See "Supported operating systems for server components" on page 11.

- Windows Server 2008 R2 SP1

- Windows Server 2012, Windows Server 2012 R2

- Windows XP x86 (SP3 required), x64 (SP3 required)

- Windows 7 x86, x64: Professional Edition, Ultimate Edition (RTM or SP1 required)

- Windows 8 x86, x64: Professional Edition, Enterprise Edition

Supported VMware versions

Table 1-2 lists the VMware Servers and management clients that are currently supported.

Table 1-2   Supported VMware Servers and Mangement Clients

VMware Servers and Management Clients	Versions
VMware ESX Server	4.0 (for ApplicationHA initiated reboot only), 4.1, 4.1 Update 1, 4.1 Update 2
VMware ESXi Server	4.0, 4.1, 5.0, 5.5
VMware vSphere Client	4.0, 4.1, 5.0, 5.5
VMware vCenter Server	4.0, 4.1, 4.1 Update 1, 5.0, 5.5 **Note:** VMware Fault Tolerance is not supported in case of vCenter Server 4.1
VMware vCenter Site Recovery Manager (SRM)	5.0, 5.1, 5.5

For the latest list of supported versions refer to the software compatibilty list (SCL) at:

http://www.symantec.com/docs/TECH209010

Disk space requirements

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

Table 1-3 summarizes the disk space requirements for installing VCS.

Table 1-3   Disk space requirements

Installation options	Required disk space
VCS + all options	832 MB
VCS Client components	287 MB

Hardware requirements

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

http://www.symantec.com/docs/TECH208993

Table 1-4 displays the required hardware requirements.

Table 1-4   Hardware requirements

Requirements	Specifications
Memory	1 GB of RAM required
32-bit processor requirements (for client components only)	800-megahertz (MHz) Pentium III-compatible or faster processor 1GHz or faster processor recommended
x64 processor requirements	1GHz AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support processor or faster
Display	Minimum resolution: 1024 X 768 pixels or higher VCS Cluster Manager (Java Console) requires an 8-bit (256 colors) display and a graphics card that can render 2D images
Storage requirememts	■ 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 or Fibre Channel 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: one public and two for the VCS private network.

Network requirements

Ensure that you have performed the following tasks and kept the required network information handy, before you install Symantec Cluster Server.

■ Verify that the systems on which you install the software are part of a Windows Active Directory domain.

■ Ensure that the static IP addresses are available for the following purposes:

   ■ One IP address per site for each virtual server.

   ■ One IP address for each physical node in the cluster

   ■ One IP address per cluster when configuring Notification. The same IP address can be used for other options, such as GCO.

■ Configure name resolution for each node.

■ Verify that the DNS Services are available. 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 Dynamic DNS (DDNS) to map virtual names with IP addresses. If you use scavenging, then you must set the DNSRefreshInterval attribute for the Lanman agent. This will enable the Lanman agent to refresh the resource records on the DNS servers.

  Refer to the Lanman agent description in the *Symantec Cluster Server Bundled Agents Reference Guide* for more information.

- If Network Basic Input/Output System (NetBIOS) is disabled over the TCP/IP, then you must set the Lanman agent's DNSUpdateRequired attribute to 1 (True).

- Make sure that the NetApp filers and the systems on which you plan to install VCS reside in the same domain.

- Make sure that the NetApp filers are reachable; ensure that you can ping the filers using the DNS name.

- If you plan to set up a disaster recovery configuration, make sure that:

  - The volumes at both sites are of the same size.

  - The NetApp filers can replicate in both directions.

- For IPv6 networks, VCS supports the following:

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

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

- In an IPv6 environment, the Lanman agent relies on the DNS records to validate the virtual server name on the network. If the virtual servers configured in the cluster use IPv6 addresses, you must specify the DNS server IP, either in the network adapter settings or in the Lanman agent's AdditionalDNSServers attribute.

- If you plan to use Fibre Channel (FC) for connecting the LUNs, type hba_info on the command prompt, and verify that the FC initiators are displayed.
  If FC initiators are not displayed, install the mini port driver provided by your vendor and run the command again to verify that the FC initiators are displayed.

- Ensure that the LUNs are mounted. In case of Multi Pathing I/O (MPIO), ensure that the LUNs are mounted using the required initiators.

Note: MPIO support is available only with FC.

- Do not install VCS on servers that are assigned the role of a Domain Controller. Configuring a cluster on a domain controller is not supported.

- If the domain controller and the computer running the installation program are on different subnets, the installer may be unable to locate the computers selected for installation. In this situation, after the installation program displays an error message, type the host names and the IP addresses of the missing computers manually.

Firewall port settings and anti-spyware

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

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

Supported applications

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

- Microsoft Exchange Server 2007 SP1, SP2, or SP3 – Standard, or Enterprise Edition (Mailbox server role required)

- Microsoft Exchange Server 2010 RTM, SP1, or SP2 – Standard, or Enterprise Edition (Mailbox server role required)

- Microsoft SQL Server 2008 SP1, SP2, and SP3 – 32-bit Standard, Enterprise, or Web Edition

- Microsoft SQL Server 2008 SP1, SP2, and SP3 – 64-bit Standard, Enterprise, or Enterprise Web Edition

- Microsoft SQL Server 2008 R2 RTM and SP1 – 32-bit Standard, Enterprise, or Datacenter Edition

- Microsoft SQL Server 2008 R2 RTM and SP1 – 64-bit Standard, Enterprise, or Datacenter Edition

- Microsoft SQL Server 2012 RTM and SP1 – 32-bit / 64-bit Standard, Business Intelligence, Enterprise, or Web Edition

- Microsoft SQL Server 2012 RTM and SP1 – 64-bit Standard, Business Intelligence, Enterprise, or Enterprise Web Edition

- Oracle 10g Release 2 (10.2.0.4) Standard, or Enterprise Edition

- Oracle 11g, Release 1 (11.1.0.7.0)

- Oracle 11g R2

- Microsoft SharePoint Server 2010 (x64) bit Standard, or Enterprise Edition

- Enterprise Vault 8.0 SP1, SP2, and SP3

- Enterprise Vault 9.0

Supported Exchange Server 2007 versions

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

Table 1-5   Microsoft Exchange Server 2007 supported environments

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

Supported Exchange Server 2010 versions

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

Table 1-6   Microsoft Exchange Server 2010 supported environments

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

Supported SQL Server 2008 and 2008 R2 versions

Table 1-7 lists the Microsoft SQL Server 2008 versions supported with this release of SFW HA.

Table 1-7   Supported Microsoft SQL Server 2008 versions

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

Table 1-8 lists the Microsoft SQL Server 2008 R2 versions supported with this release of SFW HA.

Table 1-8   Supported Microsoft SQL Server 2008 R2 versions

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

Table 1-8   Supported Microsoft SQL Server 2008 R2 versions *(continued)*

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

Supported SQL Server 2012 and 2012 R2 versions

Table 1-9 lists the Microsoft SQL Server 2012 versions supported with this release of SFW HA.

Table 1-9   Supported Microsoft SQL Server 2012 versions

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

Table 1-10 lists the Microsoft SQL Server 2012 R2 versions supported with this release of SFW HA.

Table 1-10   Supported Microsoft SQL Server 2012 R2 versions

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

Supported Oracle versions

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

Table 1-11   Supported Oracle environments

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

Table 1-11   Supported Oracle environments *(continued)*

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

Supported SharePoint Server versions

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

Table 1-12   Supported SharePoint versions

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

Supported Enterprise Vault versions

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

■ Enterprise Vault 8.0 SP1, SP2, and SP3

■ Enterprise Vault 9.0

Supported NetApp applications and other applications

The supported versions of NetApp applications and other applications are as follows:

■ NetApp SnapManager for Exchange 4.0, 5.0, 6.0 with Exchange Server 2007

■ NetApp SnapManager for SQL 2.0, 2.1, and 5.0

■ NetApp Data ONTAP 7.3, 7.3.3

■ NetApp SnapDrive 4.1, 4.2.1, 5.0, 6.0, 6.1, and 6.2
  When installing SnapDrive, you must specify a user account in the SnapDrive Service Credentials dialog box. The user account must be a domain user and part of the Administrators group of the local system and the filer.

■ Data ONTAP DSM for Windows MPIO 3.1, 3.2, 3.3, 3.3.1

■ Microsoft iSCSI software initiator version 2.03 or later versions

Verifying the system configuration using the Windows Data Collector

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

Installing the Windows Data Collector

To install and run the Windows Data Collector, your system must be running at a minimum Windows 2000 SP4.

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

■ To download the Data Collector using the product software disc, insert the product software disc into your system drive and double-click **setup.exe**. This launches the CD Browser.
Click **Windows Data Collector** and extract all the files on to your system.

■ To download the Data Collector from the SORT Web site,

■ Go to the Symantec Operations Readiness Tools (SORT) Web site:
https://sort.symantec.com

■ Under the SORT tab, select **My SORT**.

■ On the Custom Reports widget, follow the instructions to download the Data Collector.

Running the verification reports

The Data Collector uses the gathered information to generate the reports that enable you to perform the following:

■ Determine whether a system is ready to install or upgrade to this release of VCS.

■ Analyze the configuration of your current Symantec products and make recommendations about availability, use, performance, and best practices.

■ Get detailed information about your installed Symantec products, versions, and licenses.

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

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

Ensure that the following Windows services are running on all the systems where you wish to run the Windows Data Collector report:

- Windows Management Instrumentation (WMI)

- IP Helper

- Remote Registry

Licensing

VCS for Windows is available in Standard and HA DR editions.

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

Table 1-13 provides the product options available per VCS license edition.

Table 1-13　　　License edition and available product options

License edition	Available features	
	GCO	Hyper-V DR
VCS HA-DR The HA DR edition includes both, the GCO and Hyper-V DR solution. No separate license is available only for the Hyper-V DR solution.	✓	✓
VCS Standard	Not available	Not available

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

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

Table 1-14   Compatibility matrix with the Windows operating system

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

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

■ Keyless

■ User Entered Key

Note: Evaluation licenses are now deprecated.

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

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

- Add the system as a managed host to a Veritas Operations Manager (VOM) Management Server.
  For more details, refer to the VOM documentation.

- Add an appropriate and valid license key on this system using the Symantec product installer from Windows Add or Remove Programs.

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

https://licensing.symantec.com/

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

Licensing notes

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

- If you are installing the product for the first time, the Keyless option is selected by default.

- If you are upgrading the product, the User Entered Key option is available by default. The wizard retrieves all the license keys installed earlier. If you choose to use the 5.x license keys, only the product options available for the entered keys are selected and allowed for installation.
  For example, you cannot install Fast Failover and Hyper-V DR options using the 5.x license keys. To install these options you must specify a 6.0 base license key.

- During the product upgrade, you can choose to change the license option to Keyless. After changing the license option to Keyless, you can install all the available product options.

- You cannot install the 6.0 base license key over the 5.x base license key. However, you can install the 6.0 feature key over the 5.x base key.

- While repairing the product installation, licenses can be managed only if Keyless license option was selected during the installation. You cannot manage the licenses, if the license option selected was User Entered Key.
  To manage the licenses in case of User Entered Key option, you must use the Windows Add or Remove Programs.
  While managing the licenses, you can change the license option from Keyless to User Entered or vice a versa.

- You must configure Veritas Operations Manager (VOM) within two months of product installation. Failing this, a warning message for non-compliance is displayed periodically.
  For more details on configuring VOM, refer to VOM product documentation.

- You can install new licenses or remove the existing licenses using the product installer.

vxlicrep command

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

To use the vxlicrep command to display a license report

1 Open a command prompt window.

2 Enter the `vxlicrep` command without any options to generate a default report.

3 Enter the `vxlicrep` command with any of the following options to produce the type of report required:

-g	default report
-s	short report
-e	enhanced/detailed report
-l	print report for valid keys only
-k <key1, key2, ----	print report for input keys key1, key2, ----
-v	print version
-h	display this help

Planning a VCS installation

Review the following pre-installation tasks that you must perform, if you plan to install VCS.

Installing Microsoft .NET Framework 4.5 on your system

Before installing the product on either a local or remote system, install Microsoft .NET Framework 4.5 on the system.

Note the following points before installing the Microsoft .NET Framework:

- If you are installing the product on Windows Server 2008 R2 Server Core SP1 system, then enable Microsoft .NET Framework 2.0 SP2 before installing Microsoft .NET Framework 4.5.

  To enable Microsoft .NET Framework 2.0 SP2 on the system, run the following command:

  ```
  DISM.exe /online /enable-feature
  /featurename:NetFx2-ServerCore-WOW64
  ```

- If you are installing the product on a Windows XP SP3 system, install Microsoft .NET Framework 4.0 on the system instead of Microsoft .NET Framework 4.5.

Enabling the Computer Browser service for Windows Server

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

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

Enable the Computer Browser Service on your Windows Server systems before installing VCS.

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

Activating Microsoft Windows on your server

Symantec recommends that you activate Microsoft Windows before proceeding with your product installation.

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

Upgrading the Microsoft Windows operating system

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

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

If you install VCS before upgrading your Windows Server 2008 operating system, you must repair your installation, after you complete the Windows Server 2008 R2 or SP2 upgrade.

See "Repairing the VCS installation" on page 52.

Installing VCS

This chapter includes the following topics:

- About installing VCS
- Installing the VCS server components using the product installer
- Installing the VCS client components using the product installer
- Performing an automated installation for VCS server or client components

About installing VCS

This section describes the process for a new installation of VCS.

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

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

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

- Menu to install the Symantec High Availability guest components

- Symantec High Availability home page

- Symantec High Availability tab

- Symantec High Availability dashboard

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

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

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

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

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

Client components	This installs the VCS Java Console on the same nodes where the server components are installed.
High Availability Hardware Replication Agents	Symantec Cluster Server Hardware Replication Agent for NetApp
High Availability Application Agents	■ Symantec Cluster Server Application Agent for Exchange 2007 ■ Symantec Cluster Server Database Agent for Exchange 2010 ■ Symantec Cluster Server Application Agent for SharePoint Server 2013
High Availability Database Agents	■ Symantec Cluster Server Database Agent for SQL ■ Symantec Cluster Server Database Agent for Oracle
VRTSvbs package	Enables you to add the system as a managed host to the Virtual Business Services. For more details about configuring Virtual Business Services, refer to the *Virtual Business Service–Availability User's Guide*.

> **Note:** The high availability agents that are installed with the product software are also available in the form of an agent pack. The agent pack is released on a quarterly basis. The agent pack includes support for new applications as well as fixes and enhancements to existing agents. You can install the agent pack on an existing VCS installation.
>
> Refer to the Symantec Operations Readiness Tools (SORT) Web site for information on the latest agent pack availability.
>
> https://sort.symantec.com
>
> Refer to the agent-specific configuration guide for more details about the application agents.

To install the server or client components using the product installation wizard,

See "Installing the VCS server components using the product installer" on page 32.

See "Installing the VCS client components using the product installer" on page 38.

See "Performing an automated installation for VCS server or client components" on page 42.

Installing the VCS server components using the product installer

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

- Symantec Storage Foundation for Windows (SFW)

- Symantec Storage Foundation and High Availability Solutions for Windows (SFW HA)

- Symantec Dynamic Multi-Pathing for Windows

- Symantec Cluster Server for Windows

For installing SFW, SFW HA, or DMP refer to the respective installation guide.

Perform the following steps to install SFW HA server components

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

https://fileconnect.symantec.com

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

The CD browser appears.

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

---

3   Click to download the required contents.

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

Symantec Cluster Server 6.1	Click to install the server components for Symantec Cluster Server for Windows.
Late Breaking News	Click to access the latest information about updates, patches, and software issues regarding this release.
Windows Data Collector	Click to verify that your configuration meets all pertinent software and hardware requirements.
SORT	Click to access the Symantec Operations Readiness Tools site.
	In addition to the product download you can also download the custom reports about your computer and Symantec enterprise products, a checklist providing configuration recommendations, and system and patch requirements to install or upgrade your software.
Browse Contents	Click to view the software disc contents.
Technical Support	Click to contact Symantec Technical Support.

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

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

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

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

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

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

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

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

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

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

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

   The local host is populated by default.

- Alternatively, browse to select the systems.

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

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

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

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

See "Applying the selected installation and product options to multiple systems" on page 38.

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

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

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

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

  Note: The default license type is "Keyless".

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

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

  - The client components, high availability hardware replication agents, high availability application agents, and the high availability database agents are installed by default.
    For details, See "About installing VCS" on page 30.

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

Global Cluster Option (GCO)	Global Cluster Option (GCO) enables you to link clusters to provide wide-area failover and disaster recovery.

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

This completes the product installation. For configuring application service groups refer to the application implementation guide. For any administrative tasks to be performed, refer to the *Symantec Cluster Server Administrator's Guide*.

Applying the selected installation and product options to multiple systems

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

1   Click on any one of the selected systems and select the desired installation and product options.

2   Click **Apply to multiple systems**.

3   On the Apply Installation Options panel, select the installation options to be applied and then select the desired systems. Click **OK**.

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

Installing the VCS client components using the product installer

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

■   Symantec Storage Foundation for Windows (SFW)

■   Symantec Storage Foundation and High Availability Solutions for Windows (SFW HA)

■   Symantec Dynamic Multi-Pathing for Windows

■   Symantec Cluster Server for Windows

For installing SFW, SFW HA or DMP refer to the respective installation guide.

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

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

Perform the following steps to install Symantec Cluster Server client components

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

    https://fileconnect.symantec.com

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

    The CD browser appears.

3   Click to download the required contents.

Symantec Cluster Server 6.1	Click to install the server or client components for Symantec Cluster Server for Windows.
Late Breaking News	Click to access the latest information about updates, patches, and software issues regarding this release.
Windows Data Collector	Click to verify that your configuration meets all pertinent software and hardware requirements.
SORT	Click to access the Symantec Operations Readiness Tools site.
	In addition to the product download you can also download the custom reports about your computer and Symantec enterprise products, a checklist providing configuration recommendations, and system and patch requirements to install or upgrade your software.
Browse Contents	Click to view the software disc contents.
Technical Support	Click to contact Symantec Technical Support.

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

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

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

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

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

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

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

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

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

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

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

Local host is populated by default.

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

This completes the installation of the client components.

Performing an automated installation for VCS server or client components

You can perform an automated or unattended installation using the command line interface at the command prompt with the Setup.exe command. With an unattended installation, you can only install on one system at a time.

During the installation, ensure that you verify the following points:

■ There are no parallel installations, live updates, or Microsoft Windows updates in progress.

■ All CLI commands must run in the command window in the "run as administrator" mode.

To perform an automated installation

1 If you are installing the package from the software disc, insert the product
   software disc into your system's drive.

2 Log into a console session.

3 Open a command window by clicking **Start** > **Run**.

4 Enter cmd in the Open field and click **OK**.

5 Navigate to the root directory of your software disc.

   If you are downloading the installation software from the Symantec web site,
   then navigate to the download path where the setup.exe is located.

6 Use the following command syntax to install the product software.

   For example,

   ```
   Setup.exe /s Solutions="SolutionID"
   Install_mode=InstallMode
   Telemetry=Telemetry
   Installdir="InstallDirPath" Reboot=RebootMode
   NODE="SysA" Licensekey="LicenseKey"
   options="a,b,c,..."
   NoOptionDiscovery=NoOptionDiscovery
   GetPatchInfo=GetPatchInfo
   ```

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

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

Parameters for setup.exe

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

Table 2-1   Parameters for setup.exe

Parameter	Use
/s	Set for unattended mode. If not set, boots the product installation wizard.

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

Parameter	Use
INSTALL_MODE	Set to indicate an installation or uninstallation.
	1 = To install
	4 = To repair
	5 = To uninstall
	Example: INSTALL_MODE=1
	Note: The parameter, INSTALL_MODE=1 is used for both a new installation, as well as an upgrade. The installer switches to the correct mode (installation or upgrade) depending upon what has already been installed on the selected system.
SOLUTIONS	Set to the type of installation.
	6 = VCS Server Components (includes client components)
	7 = VCS Client Components only
	Example: SOLUTIONS="6"
Telemetry	Set this parameter to participate in the Symantec Product Improvement Program by submitting system and usage information anonymously.
	The Product Improvement Program allows the product installer to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the Product Improvement Program, set this parameter to 0.
INSTALLDIR	Set the installation directory path. The path must start and end with a quotation mark.
	The default setting is SystemDrive: \Program files\Veritas
	Example: INSTALLDIR="C:\InstallationDirectory"
	This is an optional parameter.
	Note: If you plan to configure the cluster for single sign-on authentication and your system runs a non-English locale operating system, ensure that the installation directory contains only English characters.

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

Parameter	Use
Reboot	Set for the automatic reboot of the system at the completion of the installation. 0 = No reboot 1 = Reboot The default setting is 0 for no system reboot. Example: Reboot=1 **Note:** This is an optional parameter.
Node	Set the node name. Specify only one node at a time. The local node is the default setting when the node is unspecified. The machine name of the node must start and end with a quotation mark ("). Example: Node="PC177VM-3"
LICENSEKEY	Set the license key for the installation. Enter multiple keys by separating them with a comma (e.g. 123-345-567-789-123, 321-543-765-789-321, etc.) The license key must start and end with a quotation mark ("). LicenseKey has no default setting. Example: LICENSEKEY="123-234-123-234-345" **Note:** This parameter is applicable only if you plan to use the "User entered license key" as your license type. You need not specify this parameter for "Keyless" license type.

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

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

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

Parameter	Use
GetPatchInfo	Set this parameter to search for available product updates.

1 = Lists available updates

0 = Does not list available updates

Default value is 1.

The product updates comprise of the pre-installation patches, post-installation patches, High Availability Agents, and Array-Specific Modules. If you set this parameter to 1, then the available pre-installation patches and post-installation patches are listed. If any pre-installation patches are available, then the setup exits to let you download and apply the pre-installation patches. Apply the pre-installation patches in the sequence displayed and rerun the setup with GetPatchInfo = 0. After the successful installation of the product, apply the post-installation patches. Also download and install the High-Availability Agents and Array-Specific Modules from the SORT website. |

Automated installation example: VCS client

This sample command installs the client components at the specified installation path and tells the system not to reboot at the end of the installation.

```
Setup.exe /s Solutions=7 Install_mode=1
Installdir="C:\InstallationDirectory"
```

Automated installation: VCS server and client

This sample command installs the server components in the directory C:\InstallationDirectory and tells the system to reboot at the end of the installation. It also installs with a license key of 123-234-123-234-345, and with the GCO option.

```
Setup.exe /s Solutions=6 Install_mode=1
INSTALLDIR="C:\InstallationDirectory" REBOOT=1
licensekey="123-234-123-234-345" options="GCO"
```

Administering VCS installation

This chapter includes the following topics:

- Adding or removing product options
- Managing VCS licenses
- Repairing the VCS installation
- About reinstalling VCS

Adding or removing product options

After you have installed VCS, you may need to add or remove the product options.

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

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

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

To add or remove features

1   Open the Windows Control Panel and click **Programs and Features**.

2   Select **Veritas Cluster Server 6.1 for Windows** and click **Change**.

3 On the Mode Selection panel, select **Add or Remove** and then click **Next**.

4 On the System Selection panel, the wizard performs the verification checks and displays the applicable installation and product options. In case the verification checks have failed, review the details and rectify the issue. Before you choose to proceed with the installation, click **Re-verify** to re-initiate the verification checks.

Note that the wizard proceeds only if the system passes the validation checks.

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

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

For details on managing your licenses, See "Managing VCS licenses" on page 50.

---

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

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

Note that the wizard proceeds only if the system passes the validation checks.

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

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

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

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

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

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

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

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

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

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

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

For details, refer to *Symantec Cluster Server Administrator's Guide*.

Managing VCS licenses

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

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

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

- Adding or removing the license keys.
  You can add or remove the license keys only if the license type selected is "User entered license key".

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

- You cannot manage licenses on a system that runs Server Core operating system. To manage licenses on these systems, you must uninstall the product and then install it again using the new licenses.

- You can manage the licenses on the local system only.

- You can manage the licenses only if you have installed the server components.

To manage licenses

1   Open the Windows Control Panel and click **Programs and Features**.

2   Select **Veritas Cluster Server 6.1 for Windows** and click **Change**.

3   On the Mode Selection panel, select **Add or Remove** and then click **Next**.

4   On the System Selection panel, the wizard performs the verification checks
    and displays the applicable installation and product options. In case the
    verification checks have failed, review the details and rectify the issue. Before
    you choose to proceed with the installation click **Re-verify** to re-initiate the
    verification checks.

    Note that the wizard proceeds only if the system passes the validation checks.

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

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

    ■   To add or remove the licenses, click **Edit**.

5   On the License Details panel, enter the license key and then click **Add**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Note: If you make any changes to the licenses, you must restart VCS High Availability Engine service for the changes to take effect. If you remove all the licenses, VCS High Availability Engine service fails to start. To start the VCS High Availability Engine service you must enter the required licenses and then run the `hastart` command or manually start VCS High Availability Engine service.

Repairing the VCS installation

The product installer can repair an existing installation of the VCS client and server components.

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

You can repair the installation only on the local system.

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

To repair the installation

1   Open the Windows Control Panel and click **Programs and Features**.

2   Select **Veritas Cluster Server 6.1 for Windows**.

    If you have installed the client components, select **Veritas Cluster Server 6.1 for Windows (Client Components)**.

3   Click **Change**.

4   On the Mode Selection panel, select **Repair**. Click **Next**.

5   On the System Selection panel, installer performs the verification checks. Click **Next** once the status is "Ready for repair".

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

    Note: You cannot select the installation and product options.

    ---

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

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

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

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

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

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

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

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

About reinstalling VCS

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

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

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

See "Installing the VCS server components using the product installer" on page 32.

See "Installing the VCS client components using the product installer" on page 38.

See "Performing an automated installation for VCS server or client components"
on page 42.

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

Uninstalling VCS

This chapter includes the following topics:

- About uninstalling VCS
- Uninstalling VCS using the product installer
- Performing an automated uninstallation of VCS

About uninstalling VCS

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

Before you uninstall VCS, you must unconfigure the cluster. Use the Veritas Cluster Configuration Wizard (VCW) to unconfigure the cluster. See the *Symantec Cluster Server Administrator's Guide* for more information.

Uninstalling VCS using the product installer

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

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

To uninstall using the product installer

1   In the Windows Control Panel, select **Programs and Features**.

2   Select **Veritas Cluster Server 6.1 for Windows**.

    If you had installed the client components, click **Veritas Cluster Server 6.1 for Windows (Client Components)**.

3   Click **Uninstall**.

4   Review the information on the Welcome panel and then click **Next**.

5   On the System Selection panel, add the nodes from which you want to uninstall the product.

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

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

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

        > **Note:** The wizard does not support the Internet Protocol version 6. To add the systems having Internet Protocol version 6, you must type the system name.

    ■   Alternatively, browse to select the nodes.
        The nodes that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more nodes and click the right arrow to move them to the Selected Systems list. Click **OK**. Once you add or select a node, wizard performs the verification checks and notes the verification details.

6   Click **Next**.

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

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

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

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

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

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

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

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

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

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

Performing an automated uninstallation of VCS

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

The VPI.exe command syntax is as follows:

```
%Installation Directory%\Veritas Shared\VPI\
{F834E070-8D71-4c4b-B688-06964B88F3E8}\{6.1.xxx}\VPI.exe install_mode=5
solutions=1 telemetry=1 reboot=1
```

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

Table 4-1   Parameters for uninstalling the product

Parameter	Use
`/s`	Set for automated mode.
`INSTALL_MODE`	Set to indicate an install or uninstall.
	1 = To install
	4 = To repair
	5 = To uninstall
	The default setting is *1* to install. Set this parameter to 5 for uninstall.
	Example: `INSTALL_MODE=`*5*
`SOLUTIONS`	Set to the type of uninstallation.
	6 - VCS Server Components (includes client components)
	7 - VCS Client Components only
	Example: Solutions="6"
	Example: SOLUTIONS=1
`TELEMETRY`	Set this parameter to participate in the Symantec Product Improvement Program by submitting system and usage information anonymously.
	The Product Improvement Program allows the product installation wizard to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the Product Improvement Program, set this parameter to 0.
`REBOOT`	Set for the automatic reboot of the system at the completion of the uninstallation.
	0 = No reboot
	1 = Reboot
	The default setting is *0* for no system reboot.
	Example: `REBOOT=`*1*

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

Parameter	Use
NODE	Set the node name.
	You can enter only one node at a time.
	The local node is the default setting when the node is unspecified.
	The system name of the node must start and end with a quotation mark (").
	Example: `Node="SysA"`
	Note: Reboot the system at the end of uninstallation to ensure that all components are uninstalled correctly. You do not have to reboot after uninstalling the client.

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

To perform an automated uninstallation

1   Open a command window by clicking **Start > Run**.

2   Enter `cmd` in the Open field and click **OK**.

3   In the command window, navigate to the root directory of the product software disk.

4   Use the following command syntax to uninstall VCS:

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

Uninstall command examples

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

```
VPI.exe /s Solutions=7 Install_mode=5 Telemetry=1 Reboot=0
```

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

```
VPI.exe /s Solutions=6 Install_mode=5 Telemetry=1 Reboot=1
```

Upgrading VCS

This chapter includes the following topics:

- Preparing the VCS cluster nodes for upgrade
- Upgrading VCS

Preparing the VCS cluster nodes for upgrade

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

Checking the supported minimum product versions

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

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

Table 5-1 lists the supported upgrade paths.

Table 5-1   Supported upgrade paths

Upgrade from	Upgrade to
VCS for Windows 6.0 VCS for Windows 6.0.1 VCS for Windows 6.0.2	VCS for Windows 6.1

Note: If you had selected Microsoft failover cluster option while installing SFW 6.1, then upgrading from SFW 6.1 to SFW HA 6.1 is not supported.

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

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

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

General preparations

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

- Back up the configuration and application data.

- Review the licensing details
  See "Licensing" on page 24.

- Ensure that you have reviewed the list of installation requirements and the supported hardware and software details.
  See "Installation requirements" on page 11.

- Ensure that you have performed the applicable pre-installation and planning tasks.
  See "Planning a VCS installation" on page 27.

- Ensure that there are no parallel scheduled snapshots in progress.

- Run the Windows Data Collector or access the SORT website to verify whether the systems in your environment meet the requirements to upgrade the cluster.

- Ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.

- If you are running Symantec NetBackup™ version 6.0 or 6.5 on systems where you are upgrading to VCS 6.1, then you must shut down the OpsCenterServer service prior to the upgrade. Both NetBackup and VCS share the same AT broker and client, and for this reason the OpsCenterServer service must by shut down prior to an upgrade.

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

Saving and closing the cluster configuration

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

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

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

- From the command prompt, type the following command.

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

Taking the backup of custom agent binaries

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

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

Taking the service groups offline

This task is applicable only in case of parallel upgrade.

To take the service groups offline

1   From the command prompt, type:

    ```
    C:\>hagrp -offline group_name -sys system_name
    ```

    where 'group_name' is the name of the service group and system_name is the node on which the group is online.

2   Repeat this command for all service groups that are online.

Closing client applications

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

- Cluster Manager (Java Console)

- Solutions Configuration Center (SCC)

Upgrading VCS

This section describes the tasks to be performed while upgrading VCS.

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

- Parallel upgrade
  See "About the parallel upgrade" on page 64.

- Rolling upgrade
  See "About the rolling upgrades" on page 64.

About the parallel upgrade

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

To perform the steps for a parallel upgrade,

See "Installing the VCS server components using the product installer" on page 32.

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

About the rolling upgrades

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

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

See "Installing the VCS client components using the product installer" on page 38.

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

passive nodes. After the service groups failover, the wizard upgrades the new passive nodes.

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

Upgrading VCS using the Rolling Upgrade wizard

Perform the following steps to upgrade the server components using the Rolling Upgrade wizard.

To upgrade the server components using the Rolling Upgrade wizard.

1 On any of the systems that does not belong to the cluster you want to upgrade, insert the product software disk containing the installation package into your system's disc drive.

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

   The CD browser appears.

3 Click **Veritas Cluster Server 6.1 for Windows**

4 Click **Upgrade Server Components (Rolling Upgrade)**.

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

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

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

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

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

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

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

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

- In the **Cluster Node host name or IP** text box, specify the node name or IP address of a node that belongs to the cluster you want to upgrade.

- Enter the cluster user account details or select **log-on user credentials** to log-on with the user account credentials of the system on which you are running the wizard.

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

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

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

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

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

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

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

If you select the "Keyless" license type, all the available product options are displayed and are selected by default.

If you select "User entered license key" as your license type, the License Details panel appears by default. On the License Details panel, enter the license key and then click **Add**. You can add multiple licenses for the various product options you want to use.

The wizard validates the entered license keys and displays the relevant error if the validation fails. After the validation is complete, click **OK**.

- The installed product options are selected by default. Select the additional options to be installed, if any. These options are available depending on your product license.

  You can also choose to clear the default selection for any of the installed option. If you clear the selection, the option is uninstalled.

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

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

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

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

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

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

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

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

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

In case the rolling upgrade operation fails and the the existing cluster is configured for single sign-on authentication, then you cannot sign on to the existing cluster configuration. This issue may also occur if you exit the Rolling Upgrade wizard before successfully upgrading the product.

In such a scenario, add a user to the cluster by typing the following command on any cluster node:

```
hauser -add <name> [-priv <Administrator|Operator|Guest> [-group
<group(s)>]]
```

Use these user credentials to sign on to the existing cluster configuration.

Performing the post-upgrade tasks

This chapter includes the following topics:

- Including custom resources in the upgraded VCS cluster
- Removing the VRTSWebApp resource from the VCS cluster configuration
- Reinstalling the custom agents

Including custom resources in the upgraded VCS cluster

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

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

1   Make sure that the agent binaries for the custom agent are available under `%VCS_HOME%\bin` where the variable *%VCS_HOME%* represents the VCS installation directory, typically `C:\Program Files\Veritas\cluster server`.

2   Stop the VCS engine (HAD) on all the nodes in the cluster.

From the command prompt, type:

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

3   During the VCS installation, the installer copies previous configuration files to a backup location. Locate the backed up types.cf and main.cf files:

    ```
    C:\Documents and Settings\All Users\Application
    Data\Veritas\cluster server\vpibackup.
    ```

4   Copy the resource type definition for the custom resource from the backed up types.cf and add it to the types.cf file for the VCS cluster.

5   If resources for a custom resource type are dependent on resources for agents bundled with VCS, you must update the resource definition of the VCS bundled agent to include the new attributes or remove the deprecated attributes.

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

6   Verify the configuration.

    From the command prompt, type:

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

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

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

    ```
    C:\> hastart
    ```

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

Removing the VRTSWebApp resource from the VCS cluster configuration

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

If VRTSWebApp resource is configured in ClusterService group, after upgrading to 6.1 the resource fails to get probed and the ClusterService group fails to come online in the cluster. You must manually delete the VRTSWebApp resource from the ClusterService group. Use the Cluster Manager (Java Console), the command line (hares -delete), or the Veritas Operations Manager (VOM) to remove the resource.

Reinstalling the custom agents

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

Application upgrades

This chapter includes the following topics:

- About the application upgrades in a VCS cluster
- Upgrading SQL Server
- Upgrading Oracle in a VCS cluster
- Upgrading application service packs in a VCS cluster

About the application upgrades in a VCS cluster

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

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

See "Supported applications" on page 17.

For application upgrade,

See "Upgrading Oracle in a VCS cluster" on page 82.

For service pack upgrade,

See "Upgrading application service packs in a VCS cluster" on page 88.

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

See "Upgrading VCS" on page 64.

Upgrading SQL Server

This section describes the following Microsoft SQL Server upgrade scenarios, in VCS environment:

SQL Server upgrade scenarios	Refer to
Upgrading Microsoft SQL Server 2008 to Microsoft SQL Server 2008 R2	See "Upgrading Microsoft SQL Server 2008 to SQL Server 2008 R2" on page 73.
Upgrading Microsoft SQL Server 2008 or 2008 SP1 to Microsoft SQL Server 2012	See "Upgrading from Microsoft SQL Server 2008 or SQL Server 2008 R2 to SQL Server 2012" on page 79.

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

Upgrading Microsoft SQL Server 2008 to SQL Server 2008 R2

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

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

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

- Ensure that you have installed VCS on all the SQL service group cluster nodes that you wish to upgrade.

- Take a backup of the SQL databases.

- Upgrade SQL Server on the first cluster node.

- Upgrade SQL Server on each additional failover node.

- In case of a Disaster Recovery configuration, ensure that the databases on the primary and secondary sites are synchronized and then proceed to upgrade the cluster.
  You can upgrade the cluster using one of the following method:

  - Adding a temporary disk and creating the volumes similar to that on the primary site.

To upgrade the cluster using this method, perform the set of pre-upgrade tasks and then proceed to upgrade the cluster on both the sites. You must follow the same upgrade sequence simultaneously at both sites, upgrade first node and then the additional nodes, as described in the procedures.

See "Preupgrade tasks for upgrading SQL Server 2008 to 2008 R2 in a disaster recovery environment" on page 74.

■ Deleting the SQL Server 2008 and then creating the service group for SQL Server 2008 R2.

Follow this method only if the data size is small. After you re-create the service groups and setup replication across the two sites, the entire data will be replicated. This involves a considerable amount of time.

See "Deleting the SQL Server 2008 service group and creating the service group SQL Server 2008 R2" on page 78.

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

To configure a new HA and DR environment for SQL Server, refer to the *Symantec Cluster Server Implementation Guide for Microsoft SQL Server* .

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

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

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

■ Obtain the drive letter on which the system database and the analysis service reside, using the following command:

```
hadiscover -discover SQLServer2008 StartUpParams:INSTANCE2K8
```

The sample output is similar to the following:

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

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

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

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

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

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

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

Upgrading SQL Server 2008 to 2008 R2 on the first cluster node

These steps assume a single SQL Server instance configured in a two-node cluster configuration.

To upgrade SQL Server on the first cluster node

1   On the node on which the SQL service group is online, take all the resources (excluding the storage resources) offline.

    From the VCS Cluster Manager (Java Console), right-click the resource and select Offline. Click Yes in the confirmation pop-up box to take the resource offline.

2   Take a backup of the SQL Server 2008 directories from the shared disk and store them in a temporary location.

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

3   Delete the RegRep resource.

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

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

5   Launch the Microsoft SQL Server installer for SQL Server 2008 R2, and install SQL Server on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so. Also, ensure that the instance name or id is the same on all the cluster nodes.

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

    Refer to the Microsoft SQL Server documentation for instructions.

6   Unfreeze and then take the SQL Server service group offline. From the VCS Cluster Manager (Java Console), right-click the SQL Server service group in tree view on the left pane and click **Unfreeze**, and then take the entire service group offline on the node.

    This completes the upgrade steps on the first cluster node. Proceed to upgrading SQL on the additional failover nodes.

Upgrading SQL Server 2008 to 2008 R2 on additional failover nodes

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

To upgrade SQL Server on the additional node

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

2 Delete the original RegRep folder and rename the SQL Server data directories on the shared disks. These directories are updated when the SQL Server 2008 R2 is installed on the first node. You can also delete these directories, if desired.

3 Copy the backed-up SQL Server 2008 databases from the temporary location to the shared disks. The backup directories are the same that you had backed up earlier while upgrading SQL on the first cluster node.

4 Freeze the SQL service group.

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

5 Launch the Microsoft SQL Server 2008 R2 installer and install SQL Server on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so. The SQL Server installer then automatically places the SQL data files in the appropriate location.

   Refer to the Microsoft SQL Server documentation for instructions.

6 From the VCS Cluster Manager (Java Console), right-click the SQL Server service group in tree view on the left pane and click **Unfreeze**, and then take the entire service group offline on the node.

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

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

Modifying the SQL Server 2008 service group configuration

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

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

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

To modify the SQL Server configuration

1   Rename the Registry (RegRep) directory on the shared disk.

2   On the first cluster node, bring the storage resources of the SQL service group, online.

3   Run the SQL Server 2008 wizard in the modify mode and follow the wizard steps.

    When asked for, provide the location for the RegRep resource. This creates a new RegRep for the version of SQL Server 2008 R2.

    Refer to the *VCS Implementation Guide for Microsoft SQL Server 2008* for detailed instructions on how to create the service group using the SQL Server 2008 Configuration Wizard.

4   After modifying the SQL Server service group, verify the configuration by switching the service group to another node in the cluster.

5   Delete the RegRep directory that you renamed in the first step.

Deleting the SQL Server 2008 service group and creating the service group SQL Server 2008 R2

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

- The VCS cluster is set up in a disaster recovery environment.

- You have chosen to follow the upgrade by deleting the SQL Server 2008 service group and then creating the service group for SQL Server 2008 R2.

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

- Using the VCS Cluster Manager (Java Console), offline and delete the service group for the instance you want to upgrade, on both the sites.

- Stop the replication between the primary and the secondary site.

- For the selected instance mount the created volumes and LUNs on any one of the cluster node, on both the sites.

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

- Launch the Microsoft SQL Server 2008 R2 installer and install SQL Server 2008 R2 on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so.

- To upgrade the additional nodes, dismount the volumes on the upgraded node and mount them on the node to be upgraded. Launch the SQL Server 2008 R2 installer to install SQL Server 2008 R2.

  Repeat this task for each additional node.

- Create the SQL Service group, reconfigure the DR components and then set the required resource dependency.

  For details, refer to *Symantec Cluster Server Implementation Guide for Microsoft SQL Server* .

Upgrading from Microsoft SQL Server 2008 or SQL Server 2008 R2 to SQL Server 2012

The following steps describe how to upgrade your existing clustered SQL Server 2008 or SQL Server 2008 R2 setup to SQL Server 2012, in a VCS cluster. Complete these steps on all the cluster nodes that are part of the SQL service group, one node at a time.

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

At a high level, upgrading to SQL Server 2012 involves the following tasks:

- Upgrade SQL Server on the first cluster node.

- Upgrade SQL Server on each additional failover node.

- In case of a Disaster Recovery configuration, repeat the SQL upgrade procedures on the nodes at the secondary site. First upgrade the first cluster node at the DR site, and then the additional failover nodes.

- Delete the existing SQL Server 2008 or SQL Server 2008 R2 service group, including the service group at the DR site, if applicable.

- Create a SQL Server 2012 service group, using the SQL Server 2012 Configuration Wizard. In case of a DR setup, create a service group at the secondary site also.

To configure a new HA and DR environment for SQL Server 2008 or SQL Server 2008 R2, refer to the *Symantec Cluster Server Implementation Guide for Microsoft SQL*.

To configure a new HA and DR environment for SQL Server 2012, refer to the*Symantec Cluster Server Implementation Guide for Microsoft SQL Server 2012*.

Note: In case of a Disaster Recovery setup, you must first upgrade SQL on the cluster nodes at the primary site and then proceed with the nodes at the secondary site. You must follow the same upgrade sequence at both sites, upgrade first node and then the additional nodes, as described in the procedures in this section.

Ensure that you perform the following before the upgrade:

- Take a backup of the SQL databases.

- In case of a Disaster Recovery environment, ensure that the databases on the primary and secondary sites are synchronized and then stop the replication between the sites.

- Ensure that you have installed VCS on all the SQL service group cluster nodes that you wish to upgrade.

- Make a note of the SQL virtual server name and all the IP addresses configured at both the primary and the secondary site, for the SQL setup in the DR environment. You will need these details later.

Upgrading SQL on the first cluster node

These steps assume a single SQL Server instance configured in a two-node cluster configuration.

To upgrade SQL Server on the first cluster node

1   On any one of the cluster node on which you want to upgrade SQL Server, take all the SQL Server 2008 or 2008 R2 service group resources (excluding the storage resources) offline and delete the same.

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

2   Take a backup of the SQL Server 2008 or 2008 R2 database from the shared disk and store them in a temporary location.

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

3 Launch the Microsoft SQL Server 2012 installer and install SQL Server 2012 on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so. The SQL Server 2012 installer then automatically places the SQL data files in the appropriate location.

Refer to the Microsoft SQL Server 2012 documentation for instructions.

4 Take the entire service group offline on the node.

This completes the upgrade steps on the first cluster node. Proceed to upgrading SQL on the additional failover nodes.

Upgrading SQL on the additional failover node

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

To upgrade SQL Server on the additional node

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

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

3 Copy the backed-up SQL Server 2008 or 2008 R2 data directories from the temporary location to the shared disks.

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

4 Launch the Microsoft SQL Server 2012 installer and install SQL Server 2012 on the node. Make sure that you select the option to upgrade the existing SQL Server instance(s), when prompted to do so. The SQL Server 2012 installer then automatically places the SQL data files in the appropriate location.

Refer to the Microsoft SQL Server 2012 documentation for instructions.

5 Take the entire service group offline on the node.

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

This completes the upgrade steps on the additional failover node. Delete the existing SQL Server 2008 or 2008 R2 service group and proceed to create SQL Server 2012 service group in the cluster.

Create SQL Server 2012 service group in a VCS cluster

To configure the SQL Server 2012 service group, run the SQL Server 2012 Configuration Wizard, from the last upgraded node.

Refer to *Symantec Cluster Server Implementation Guide for Microsoft SQL Server 2012* for instructions.

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

Refer to the *Symantec Cluster Server Implementation Guide for Microsoft SQL Server 2012* for instructions.

To create the SQL Server 2012 service group

1   Rename the Registry (RegRep) directory, if present, on the shared disk.

2   Create the SQL Server 2012 service group using the SQL Server 2012 Configuration Wizard.

    Refer to *Symantec Cluster Server Implementation Guide for Microsoft SQL Server 2012* for detailed instructions on how to create the service group using the SQL Server 2012 Configuration Wizard.

3   After creating the SQL Server service group, verify the configuration by switching the service group to another node in the cluster.

4   Delete the RegRep directory that you renamed in the first step.

Upgrading Oracle in a VCS cluster

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

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

Upgrading the Oracle application in a VCS cluster

Upgrading Oracle involves the following steps:

- Upgrading the Oracle binaries.

- Upgrading the Oracle database.

  Perform the following tasks before upgrading the Oracle database:

  - Bring the Oracle service group online.

■ Stop HAD using the `hastop -local -force` command.

For details, refer to the Oracle product documentation.

Additional tasks after upgrading Oracle in a VCS cluster

Perform the following tasks to configure Oracle in a VCS environment:

■ Associate the updated database with the listener for Oracle 10g and 11g.
See "Associating the updated Oracle database with the listener" on page 83.

■ Configure the database and listener to use the virtual IP address.
See "Configuring the Oracle database and listener to use the virtual IP address"
on page 84.

■ Configure Oracle and listener services.
See "Configuring Oracle and listener services" on page 87.

■ Modify the ServiceName attribute for the Netlsnr resource.
See "Modifying the ServiceName attribute for the netlsnr resource" on page 88.

Associating the updated Oracle database with the listener

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

Prerequisites to associate Oracle databases with listeners

Ensure that the initialization parameter file contains the following entries:

■ SERVICE_NAMES (the name of the database service)

■ INSTANCE_NAME (the name of the database instance)

These parameters are created during installation or database creation.

Associate the Oracle database with the listener

The following procedure associates the database with the listener.

To associate the database with the listener

1   Use one of the following procedures to configure the new attribute listener_alias:

Run the following SQL command:

```
SQL> ALTER SYSTEM SET LOCAL_LISTENER='<listener_alias>' scope=spfile;
```

OR

Add the following entry to the initialization parameter file (pfile or spfile):

```
LOCAL_LISTENER = <listener_alias>
```

2   Define the parameter listener_alias. If your Oracle configuration uses the file `tnsnames.ora`, edit the file as instructed below. The default location of `tnsnames.ora` is `%ORACLE_HOME%\NETWORK\ADMIN`.

Add the following to `tnsnames.ora` file:

```
<listener_alias>=
(DESCRIPTION =
(ADDRESS=(Protocol=TCP)(HOST=virtual_IP_address)(Port=1521))
)
```

3   Stop and restart the database.

The listener_alias parameter gets appended by the default domain name that is specified in the file `sqlnet.ora`.

Configuring the Oracle database and listener to use the virtual IP address

All databases and listeners configured must use the same virtual IP. Update the Oracle files to set the virtual IP address.

Setting the virtual IP address involves the following tasks:

■   Creating a virtual IP address.

■   Verifying the initialization file settings.

■   Updating the Oracle configuration files.

Use the following procedures to configure the Oracle database and listener.

To create a virtual IP address

1   Open the **Network Connections**.

2   Right-click the public network connection to be used and click **Properties**.

3   Select **Internet Protocol (TCP/IP)** and click **Properties**.

4   Click **Advanced**.

5   In the **IP Settings** tab, click **Add** to add a virtual IP address and subnet mask.

To verify the initialization file settings, if a PFILE is used

1   Open the Registry Editor.

    From the **Start** menu, choose **Run**. In the **Open** field, enter `regedit` and click **OK**.

2   Double-click the ORA_*SID*_PFILE registry key at HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME_*ID*\.

    The variable *SID* represents the database instance.

3   Verify that the Value data field specifies the correct path at which the initialization file, `init.ora`, is located.

To verify the initialization file settings, if an SPFILE is used

1   Run sqlplus.exe.

2   Connect to the database.

3   Verify the following query returns the correct path of the SPFILE.

    ```
    select value from v$parameter where name = 'spfile'
    ```

To update the Oracle configuration files

1   In the `listener.ora` and `tnsnames.ora` files, change the host name for all the TCP protocol address databases to the virtual IP address that you created.

    Replace

    ```
    HOSTNAME=machine_name
    ```

    with

    ```
    HOSTNAME=virtual_IP_address
    ```

2 In the initialization file, change the dispatchers parameter.

Oracle requires an initialization file, a PFILE or an SPFILE, to start database instances. Choose the appropriate reference depending on the initialization file you use.

See "Setting the dispatchers parameter in PFILE" on page 86.

See "Setting the dispatchers parameter in SPFILE" on page 86.

3 Restart the Oracle and listener services.

Setting the dispatchers parameter in PFILE

In the PFILE, set the host name for all TCP protocol address dispatchers to the virtual IP address that you created.

Edit the dispatchers parameter only for the host name and leave the rest of the configuration as it is. Set the value as:

```
dispatchers = '(ADDRESS = (Protocol=TCP)
(HOST=virtual_IP_address)
(any other previously existing entry))'
```

The variable *virtual_IP_address* represents the virtual IP address that you created.

For example:

```
dispatchers = '(ADDRESS = (Protocol=TCP)(HOST=10.210.100.110)
(SERVICE=Data1XDB)'
```

Setting the dispatchers parameter in SPFILE

Use the following steps to set the dispatchers parameter in SPFILE.

To set the dispatchers parameter in SPFILE

1 Convert the SPFILE to PFILE.

2 Modify the PFILE.

See "Setting the dispatchers parameter in PFILE" on page 86.

3 Convert the PFILE to SPFILE.

4 Save the SPFILE to the original location on the shared disk.

Refer to the Oracle documentation for specific information on converting a PFILE or an SPFILE.

Configuring Oracle and listener services

Configuring the Oracle and Listener services involves the following tasks:

- Making the Oracle and Netlsnr services manual.

- Configuring log on properties for Oracle services.

Use the following procedures to configure Oracle and listener services.

To make services manual

1   Open the **Services** applet from **Start > All Programs > Administrative Tools > Services** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.

2   Double-click the Oracle service. In the SCM, the following appears:

- Oracle services appear as OracleService*SID*, where *SID* represents the database instance.

- Listener services appear as Oracle*Ora_Home*TNS*ListenerName*, where *Ora_Home* represents the Oracle home directory and *ListenerName* is the name of the listener set during the installation.

3   In the **Properties** window, click the **General** tab.

4   From the **Startup Type** drop-down list, select **Manual**.

5   Click **OK**.

To configure the log on properties for oracle services

1   Open the **Services** applet from **Start > All Programs > Administrative Tools > Services** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.

2   Double-click the Oracle service. In the SCM, the names of Oracle services appear as OracleService*SID*, where *SID* represents the database instance.

3   In the **General** tab of the **Properties** window, click **Stop** to stop the service.

4   Click the **Log On** tab.

5   Choose **This Account**.

6   Enter the credentials of the user in whose context Oracle was installed.

7   Click the **General** tab and click **Start** to start the service with the new Log On properties. Click **OK**.

Modifying the ServiceName attribute for the netlsnr resource

Perform the following steps to modify the ServiceName attribute for the Netlsnr resource.

To modify the ServiceName attribute

1   Start HAD. Type the following on the command prompt:

    ```
    C:\> hastart
    ```

2   Offline the Netlsnr resource. Type the following on the command prompt:

    ```
    C:\> hares -offline resource_name -sys system_name
    ```

3   Modify the ServiceName attribute for the Netlsnr resource. Type the following on the command prompt:

    ```
    C:\> hares -modify resource_name attribute_name attribute_value
    ```

    For example, to modify the ServiceName attribute of the Netlsnr resource, Netlsnr_res, type:

    ```
    C:\> hares -modify Netlsnr_res ServiceName attribute_value
    ```

    where, *attribute_value* is the name of the listener service in Oracle 9i or 10g versions.

4   Online the Netlsnr resource. Type the following on the command prompt:

    ```
    C:\> hares -online resource_name -sys system_name
    ```

Upgrading application service packs in a VCS cluster

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

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

See "Upgrading the SharePoint Server service packs " on page 98.

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

See "Upgrading VCS" on page 64.

Upgrading the Exchange Server service packs

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

Exchange Server service pack upgrade scenarios	Refer to
Microsoft Exchange 2007 to 2007 SP3	See " Upgrading Exchange Server 2007 to a service pack" on page 89.
Microsoft Exchange 2010 to 2010 SP1, SP2 or SP3	See "Upgrading Exchange Server 2010 to a service pack" on page 93.

Upgrading Exchange Server 2007 to a service pack

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

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

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

Symantec Cluster Server Implementation Guide for Microsoft Exchange 2007

Before you proceed to upgrade the Exchange Server service pack, note the following:

- Ensure that the Exchange 2007 service group is offline in the cluster.

- While performing the upgrade the Exchange 2007 Upgrade Wizard renames and then restarts the cluster node. Exit all the other programs before you run the wizard on a cluster node.

- Ensure that the Exchange database and registry replication files are configured on separate volumes. Configuring the Exchange database and the registry replication files on the same volume may cause data corruption, after you upgrade Exchange with the latest service pack.

  If you fail to configure the Exchange database and the registry replication files on separate volumes, and the data gets corrupt after upgrading Exchange with the latest service pack, perform the following steps as a workaround:

  - Delete or rename the file that could not be restored. Refer to the agent logs for the list of files that could not be restored.

  - Bring the Regrep resource online.

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

To upgrade Exchange 2007 to Exchange 2007 SP3

1 Launch the Exchange 2007 Upgrade wizard on one of the cluster nodes from **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange 2007 Upgrade Wizard** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.

2 Review the information on the Welcome panel and click **Next**.

3 On the Exchange Virtual Server Selection panel, select the Exchange virtual server that you want to upgrade and then click **Next**.

The Summary table provides the details of the Exchange virtual servers in the cluster and their upgrade status on each cluster node.
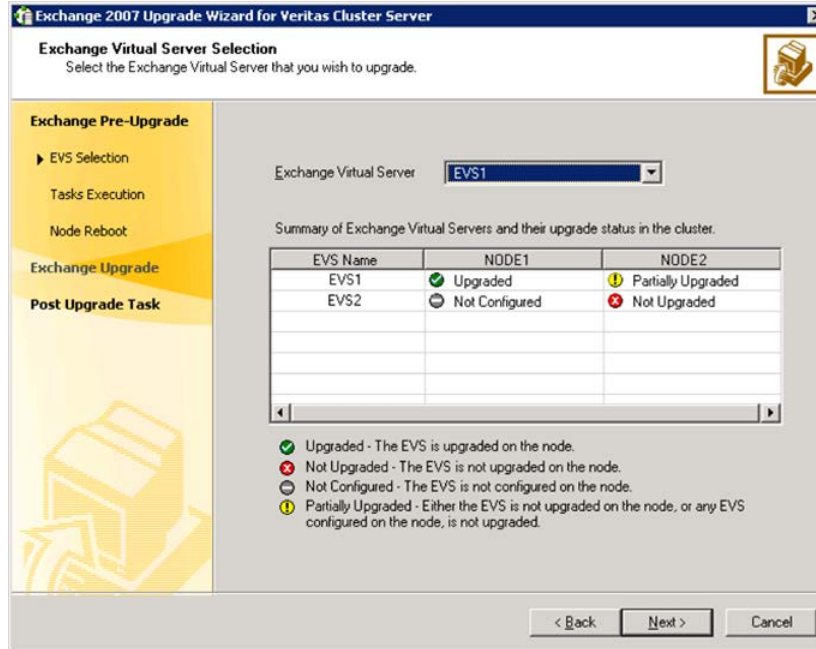
4 The wizard performs the tasks required to set up the VCS environment for the Exchange upgrade. The Tasks table displays the progress of the various tasks. After all the tasks are completed, click **Next**.

5 Review the information on the Cluster Node Reboot panel and then click **Reboot**. The wizard prompts you to reboot the node. Click **Yes** to reboot the node.

The Exchange virtual server name is temporarily assigned to the cluster node. On rebooting the node, the Exchange 2007 Upgrade Wizard is launched automatically with a message that the Exchange pre-upgrade tasks are complete. Do not click **Continue** at this time. Wait until after the Exchange upgrade is complete.

6 Run the Exchange 2007 SP1 installer to upgrade Exchange 2007 on the node. Type the following at the command prompt:

```
<drive letter>:\setup.com /mode:Upgrade
```

Here `<drive letter>` is the drive where the Exchange SP1 installer is located.

Note: You can also run Setup.exe to launch the installer GUI for upgrading Exchange. If using the installer GUI, ensure that you do not select any other Exchange 2007 server role. Only the Mailbox server role must be upgraded.

Verify that the upgrade has completed successfully. In case there are errors or if the upgrade has partially succeeded or has failed, resolve the errors and ensure that the upgrade is successful.

Refer to the Microsoft Exchange documentation for more information.

7 Return to the Exchange 2007 Upgrade Wizard and click **Continue**.

If the wizard is not running, start the wizard from **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange 2007 Upgrade Wizard** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.

8 The wizard performs the tasks required to set up the VCS environment after the Exchange upgrade. The Tasks table displays the progress of the various tasks. After all the tasks are completed, click **Next**.

9 Review the information on the completion panel and then click **Finish**.

The wizard displays the status of the Exchange virtual server upgrade. The Summary table provides the details of the Exchange virtual servers in the cluster and their upgrade status on each cluster node.

10 Repeat these steps on the remaining cluster nodes. After you have upgraded all the cluster nodes that are configured to host the Exchange virtual server, bring the Exchange 2007 service group online in the cluster.

Note: Do not bring the Exchange 2007 service group online until you have completed the upgrade on all the cluster nodes that are part of the service group.

---

11 For a disaster recovery environment, repeat this procedure at the secondary (DR) site.

Upgrading Exchange Server 2010 to a service pack

This section describes how to upgrade Exchange Server 2010 to any 2010 service pack. It is applicable only if you already have Exchange 2010 setup in a VCS cluster environment.

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

- You have met all the necessary pre-requisites for installing the service pack on all the cluster nodes where you are upgrading Exchange.
  For details refer to Microsoft documentation.

- Ensure that you have upgraded VCS on all the cluster nodes.

To upgrade Exchange 2010 to a service pack

1 Using the VCS Cluster Manager (Java Console), bring the Exchange service group online.

2 Stop HAD on all the cluster nodes where you want to upgrade the Exchange installation. At the command prompt, type:

   ```
   hastop -local -force
   ```

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

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

Upgrading the SQL Server service packs

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

SQL Server service pack upgrade scenarios	Refer to
Microsoft SQL Server 2008 or 2008 R2 to its latest service packs	See "Upgrading SQL Server 2008 or 2008 R2 to a service pack " on page 93.
Microsoft SQL Server 2012 to SQL Server 2012 SP1	See "Upgrading SQL Server 2012 to a service pack " on page 95.

Upgrading SQL Server 2008 or 2008 R2 to a service pack

Use this procedure to perform the following upgrades:

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

- SQL Server 2008 R2 to SQL Server 2008 R2 SP1

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

- You must have administrative privileges to the SQL instance that you want to upgrade.

- Make sure that you have a recent backup of your system and user databases.

- Make sure that the VCS version installed is 5.1 SP2 or later.

- Refer to the Microsoft documentation for prerequisites related to SQL Server 2008 Service Pack installation.

Consider a two node cluster, Node A and Node B. The SQL service group is ONLINE on Node A, and Node B is the passive node.

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

- Upgrade SQL Server on all the nodes parallely

- Upgrade SQL Server on the passive node first and then upgrade the active nodes

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

To parallely upgrade SQL Server on all the cluster nodes

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

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

3   Reboot the nodes.

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

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

To upgrade SQL Server on the passive nodes first

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

2   Confirm all SQL services are stopped on Node B.

3   Upgrade the SQL Server 2008 instance on Node B.

4   Reboot node B.

5   Unfreeze the service group on node A.

6   Fail over the service group to Node B.

7   After the service group comes online, freeze the service group on Node B.

8   Confirm all SQL services are stopped on Node A.

9   Upgrade the SQL Server 2008 instance on Node A.

10 Reboot Node A.

11 Unfreeze the service group on node B.

12 Fail back the service group to Node A.

Upgrading SQL Server 2012 to a service pack

This section describes the tasks to upgrade SQL Server 2012 to SQL Server 2012 SP1 in a VCS cluster, that is configured in a disaster recovery environment.

Note: This procedure is applicable only if you have already configured SQL Server in a VCS cluster environment.

Before upgrading SQL Server 2012 to SQL Server 2012 SP1

Consider the following points before you proceed:

■   Ensure that you have installed and configured VCS 6.1.

■   Ensure that you have installed and configured SQL Server 2012 in a VCS environment.

■   Ensure that the logged on user has administrative privileges to the SQL instance that you want to upgrade.

■   Ensure that you have taken a recent backup of your system, user databases and the SQL Server directories from the shared storage.

■   Refer to the Microsoft documentation for prerequisites related to SQL Server 2012 Service Pack installation.

Upgrading SQL Server 2012

Consider a three node disaster recovery cluster set up; Node A, Node B and Node C. Node A and Node B are on the primary site and Node C is on the secondary site. The SQL service group is Online on Node A.

The upgrade involves upgrading SQL Server on the nodes at the primary site first and then on the nodes at the secondary site. Symantec recommends that you perform the upgrade in the specified order, one node at a time.

To upgrade SQL Server 2012 to 2012 SP1, perform the following steps:

1   Stop the replication between the primary and the secondary site.

   If using VVR for replication, from the VEA Console right-click the Secondary RVG and select **Stop Replication** from the menu that appears.

2   On Node A where the SQL Server service group is Online bring the SQLServer, MSOlap and SQLServer-Agent resources offline.

   Using the VCS Cluster Manager (Java Console), on the Service Groups tab, right-click the resource and then click **Offline**.

3   From Services.msc ensure that all the SQL services and the SQL services for which VCS resources are configured are stopped.

4   Use the VCS Cluster Manager (Java Console) and perform the following steps on the SQL Server 2012 service group on Node A (active node):

   ■   Bring the RegRep resource offline.
       On the Service Groups tab, right-click the RegRep resource and then click **Offline** from the menu that appears. Click Yes in the confirmation pop-up box to take the RegRep resource offline.

   ■   Disable the RegRep resource.
       On the Service Groups tab, right-click the RegRep resource and then click **Disabled** from the menu that appears.

   ■   Except the storage resources (MountV and VMDg) bring all the resources offline.

   ■   Freeze the service group.
       On the Service Groups tab, right-click the service group and then click **Freeze** > **Persistent**.

5   Install the Microsoft SQL Server 2012 Service Pack 1 on Node A.

6   Using VCS Java Console, right-click the SQL Server service group and select **Unfreeze**.

7   Fail over the service group to Node B and perform the following steps on Node B, in the given order:

   ■   Except the storage resources (MountV and VMDg) bring all the resources offline.

   ■   From Services.msc ensure that all the SQL services and the SQL services for which VCS resources are configured are stopped.

   ■   Freeze the service group.

8 Rename the SQL folders on the shared storage and copy the backed up SQL Server directories on the shared storage.

The SQL data files available on the shared storage are upgraded during the SQL upgrade on Node A. Before you begin to upgrade SQL on Node B, you must rename the folders containing the upgraded SQL data files and restore the initially backed up SQL Server directories. If you do not restore the initially backed up SQL Server directories, then the SQL upgrade on Node B may fail indicating that the SQL data files are already upgraded.

9 Install the Microsoft SQL Server 2012 Service Pack 1 on Node B.

10 Unfreeze the service group on Node B and enable the RegRep resource.

11 Bring the service group Online on Node B.

12 Start the replication between the primary and the secondary site.

13 Switch the service group to the DR site (Node C).

On the Service Groups tab, right-click the service group and then click **Switch To** > **Remote Switch**.

14 Stop the replication between the primary and the secondary site again.

15 Perform the following steps on Node C, in the given order:

- Except the storage resources (MountV and VMDg) bring all the resources offline.

- Disable the RegRep resource and freeze the service group.

- Rename the SQL folders from the shared storage and copy the backed up directories on the shared storage.

- Install the Microsoft SQL Server 2012 Service Pack 1.

- Unfreeze the service group and enable the RegRep resource.

16 Start replication between the primary and secondary site.

17 Switch the service group back to Node B (last upgraded node) on the primary site.

This completes the SQL Server 2012 upgrade.

Note: You must bring the SQL service group online on Node B first. This is because the replication service group is online on Node B. You can then switch the SQL service group on any node on the primary site.

Upgrading the SharePoint Server service packs

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

SharePoint Server service pack upgrade scenarios	Refer to
Microsoft SharePointServer 2010 to SharePoint Server 2010 SP1 or SharePoint Server 2010 SP2	See "Upgrading SharePoint Server 2010 to a service pack" on page 98.

Upgrading SharePoint Server 2010 to a service pack

This section describes how to upgrade SharePoint Server 2010 to SharePoint Server 2010 SP1 or SharePoint Server 2010 SP2.

It is applicable only if you already have SharePoint Server 2010 setup in a VCS cluster environment.

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

- You have met all the necessary pre-requisites for installing SharePoint Server 2010 SP1 or SharePoint Server 2010 SP2 on all the cluster nodes where you are upgrading SharePoint Server.
  For details, refer to Microsoft documentation.

- Ensure that you have upgraded VCS on all the cluster nodes.

To upgrade SharePoint Server 2010 to SharePoint Server 2010 SP1 or SharePoint Server 2010 SP2

1   Using the VCS Cluster Manager (Java Console), bring all the service groups corresponding to Share Point application online.

2   Stop HAD on all the cluster nodes where you want to upgrade the SharePoint Server installation. At the command prompt, type:

    ```
    hastop -all –force
    ```

3   Upgrade SharePoint Server 2010 to SharePoint Server 2010 SP1 or SharePoint Server 2010 SP2.

    For details, refer to Microsoft documentation.

4   At the command prompt, type:

    ```
    hastart -all
    ```

Services and ports

This appendix includes the following topics:

- VCS ports and services

- Symantec ApplicationHA ports and firewall settings

- Services and ports used during the installation and configuration of the Symantec High Availability Console

VCS ports and services

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

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

Ensure that you enable the ports and services for both, inbound and outbound communication.

Note: The port numbers marked with an asterisk are mandatory for configuring VCS.

Table A-1   VCS services and ports

Component Name/Process	Port/Protocol	Description
CmdServer.exe	14150*/TCP	Veritas Command Server

Table A-1   VCS services and ports *(continued)*

Component Name/Process	Port/Protocol	Description
had.exe	14141*/TCP	Veritas High Availability Engine
		Veritas Cluster Manager (Java console) (ClusterManager.exe)
		VCS Agent driver (VCSAgDriver.exe)
pluginHost.exe	7419*/TCP	Symantec Plugin Host Service
		Solutions Configuration Center (SFWConfigPanel.exe)
		CCF Engine (CEngineDriver.exe)
vcsauthserver.exe	14149/TCP/UDP	VCS Authentication Service
vras.dll	8199/TCP	Volume Replicator Administrative Service
vxio.sys	4145/UDP	VCS Cluster Heartbeats
VxSchedService.exe	4888/TCP	Veritas Scheduler Service
		Use to launch the configured schedule.
User configurable ports created at kernel level by vxio .sys file	49152-65535/TCP/UDP	Volume Replicator Packets
Notifier.exe	14144/TCP/UDP	VCS Notification
hasim.exe	14153, 15550 - 15558/TCP/UDP	VCS Cluster Simulator
wac.exe	14155/TCP/UDP	VCS Global Cluster Option (GCO)

Symantec ApplicationHA ports and firewall settings

uses certain ports and services during installation and configuration. If you have configured a firewall, ensure that the firewall settings allow access to these ports and services.

displays the services and ports used by .

Table A-2   Services and ports used by ApplicationHA

Component Name/Process	Port/Protocol	Description
File and Printer Sharing		Used by ApplicationHA installer while installing ApplicationHA. The installer uses this to copy the installation files to the machine.
Windows Management Instrumentation (WMI) service		Used by ApplicationHA installer while installing ApplicationHA. The installer uses this service to discover virtual machines.
Veritas Storage Foundation Messaging Service (xprtld)	5634 / TCP	Used for communications between the Symantec High Availability Console host machine and the virtual machines.

Services and ports used during the installation and configuration of the Symantec High Availability Console

Table A-3 displays the services and ports used during the installation and configuration of the Symantec High Availability Console.

Table A-3   Services and ports used during the installation and configuration of the Symantec High Availability Console

Component Name/Process	Port/Protocol	Description
File and Printer Sharing		Used by the installer during the Console server installation. The installer uses this to copy the installation files to the machine.
Windows Management Instrumentation (WMI) service		Used by the installer during the Console server installation, to discover the virtual machines.

Table A-3   Services and ports used during the installation and configuration
of the Symantec High Availability Console *(continued)*

Component Name/Process	Port/Protocol	Description
VMware Web Service	443/ https (Default port)	Used by the installer during the Console server installation, to register High Availability plugin and add High Availability privileges to the vCenter Server.
Symantec ApplicationHA Service	14151, 14152/ TCP	Used by the High Availability Console host to run Java Servlets that fetch the application monitoring status from the virtual machines and display the information on the High Availability tab in the vSphere Client.
Symantec ApplicationHA Authentication Service	14153/ TCP	Used by the High Availability Console to authenticate the single sign-on account configured for a virtual machine.
Symantec ApplicationHA Database Service	14154/ TCP	Used by the High Availability Console to read and update the Sybase database.
Veritas Storage Foundation Messaging Service (xprtld)	5634 / TCP	Used for communications between the High Availability Console host machine and the virtual machines.
VMwareDisksAgent	443/https	Used for communication between virtual machines and the ESX hosts.

Appendix B

About SORT

This appendix includes the following topics:

- About Symantec Operations Readiness Tools

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a website that automates and simplifies some of the most time-consuming administrative tasks. It helps you identify risks in your datacenters and improve operational efficiency, enabling you to manage the complexity that is associated with datacenter architectures and scale.

Table B-1 lists three major datacenter tasks and the SORT tools that can help you accomplish them.

Table B-1 Datacenter tasks and the SORT tools

Task	SORT tools
Prepare for installations and upgrades	- Installation and Upgrade checklists Display system requirements including memory, disk space, and architecture. - Installation and Upgrade custom reports Create reports that determine if you're ready to install or upgrade a Symantec enterprise product. - Array-specific Module Finder List the latest Array Support Libraries (ASLs) and Array Policy Modules (APMs) for UNIX servers, and Device Driver Installers (DDIs) and Device Discovery Layers (DDLs) for Windows servers. - High Availability Agents table Find and download the agents for applications, databases, replication, and Symantec partners.

Table B-1   Datacenter tasks and the SORT tools *(continued)*

Task	SORT tools
Identify risks and get server-specific recommendations	■ Patch notifications Receive automatic email notifications about patch updates. (Sign in required.) ■ Risk Assessment check lists Display configuration recommendations based on your Symantec product and platform. ■ Risk Assessment custom reports Create reports that analyze your system and give you recommendations about system availability, storage use, performance, and best practices. ■ Error code descriptions and solutions Display detailed information on thousands of Symantec error codes.
Improve efficiency	■ Patch Finder List and download patches for your Symantec enterprise products. ■ License/Deployment custom reports Create custom reports that list your installed Symantec products and license keys. Display licenses by product, platform, server tier, and system. ■ Symantec Performance Value Unit (SPVU) Calculator Use the calculator to assist you with the pricing meter transition. ■ Documentation List and download Symantec product documentation, including manual pages, product guides, and support articles. ■ Related links Display links to Symantec product support, forums, customer care, and vendor information on a single page.

SORT is available at no additional charge.

To access SORT, go to:

https://sort.symantec.com

Index