

Symantec™ VirtualStore Installation and Configuration Guide

Solaris

6.0.1

Symantec™ VirtualStore Installation and Configuration 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: 6.0.1

Document version: 6.0.1 Rev 0

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec, the Symantec logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec Web site.

<https://sort.symantec.com/documents>

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

Technical Support	4
Section 1 Installation overview and planning	19
Chapter 1 Introducing Symantec VirtualStore	21
About Symantec VirtualStore	21
About Symantec VirtualStore solution for VMware environment	21
About I/O fencing	22
About configuring SVS clusters for data integrity	23
About I/O fencing for Symantec VirtualStore in virtual machines that do not support SCSI-3 PR	24
About I/O fencing components	25
About preferred fencing	26
Chapter 2 System requirements	29
Release notes	29
Hardware compatibility list (HCL)	29
Supported operating systems	30
I/O fencing requirements	30
Coordinator disk requirements for I/O fencing	30
CP server requirements	31
Non-SCSI-3 I/O fencing requirements	34
Veritas File System requirements	35
Database requirements	36
Disk space requirements	36
Discovering product versions and various requirement information	37
Chapter 3 Planning to install Symantec VirtualStore	39
About planning for SVS installation	40
About installation and configuration methods	40
About the Veritas installer	41
Assessing the system for installation readiness	43

	Prechecking your systems using the Veritas installer	44
	Downloading the Symantec VirtualStore software	44
	Setting environment variables	46
	Optimizing LLT media speed settings on private NICs	47
	Guidelines for setting the media speed of the LLT interconnects	47
	Creating the /opt directory	47
	About using ssh or rsh with the Veritas installer	48
	Setting up shared storage	48
	Setting up shared storage: SCSI disks	48
	Setting up shared storage: Fibre Channel	51
	Creating root user	52
	Prerequisites for installing Symantec VirtualStore	53
	Hardware overview and requirements for Symantec	
	VirtualStore	54
	Shared storage	55
	Fibre Channel switch	55
	Cluster platforms	55
Chapter 4	Licensing Symantec VirtualStore	57
	About Veritas product licensing	57
	Setting or changing the product level for keyless licensing	58
	Installing Veritas product license keys	60
Section 2	Preinstallation tasks	61
Chapter 5	Preparing to install SVS	63
	Making the IPS publisher accessible	63
Section 3	Installation using the script-based installer	65
Chapter 6	Installing Symantec VirtualStore using the script-based installer	67
	Installing Symantec VirtualStore using the installer	67
	Configuring Symantec VirtualStore in secure mode	70

Chapter 7	Preparing to configure Symantec VirtualStore	71
	About planning to configure I/O fencing	71
	Typical SVS cluster configuration with server-based I/O fencing	75
	Recommended CP server configurations	76
	Setting up the CP server	79
	Planning your CP server setup	79
	Installing the CP server using the installer	80
	Configuring the CP server cluster in secure mode	81
	Setting up shared storage for the CP server database	82
	Configuring the CP server using the installer program	83
	Configuring the CP server using the Web-based installer	93
	Configuring the CP server manually	94
	Configuring CP server using response files	95
	Verifying the CP server configuration	99
Chapter 8	Configuring Symantec VirtualStore	101
	Overview of tasks to configure Symantec VirtualStore using the script-based installer	101
	Configuring SVS using the script-based installer	102
	Starting the software configuration	102
	Specifying systems for configuration	103
	Configuring the cluster name	104
	Configuring private heartbeat links	104
	Configuring the virtual IP of the cluster	108
	Configuring a secure cluster node by node	110
	Adding VCS users	114
	Configuring SMTP email notification	115
	Configuring SNMP trap notification	116
	Configuring global clusters	118
	Completing the SVS configuration	119
	Verifying and updating licenses on the system	120
Chapter 9	Configuring SVS for data integrity	123
	Setting up disk-based I/O fencing using installsvs	123
	Initializing disks as VxVM disks	123
	Configuring disk-based I/O fencing using installsvs	124
	Checking shared disks for I/O fencing	127
	Setting up disk-based I/O fencing manually	132
	Identifying disks to use as coordinator disks	133
	Setting up coordinator disk groups	133

Creating I/O fencing configuration files	134
Modifying VCS configuration to use I/O fencing	135
Verifying I/O fencing configuration	137
Setting up server-based I/O fencing using installsvs	137
Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsvs	146
Setting up server-based I/O fencing manually	148
Preparing the CP servers manually for use by the SVS cluster	148
Configuring server-based fencing on the SVS cluster manually	151
Configuring CoordPoint agent to monitor coordination points	157
Verifying server-based I/O fencing configuration	159
Setting up non-SCSI-3 fencing in virtual environments manually	160
Sample /etc/vxfenmode file for non-SCSI-3 fencing	162
Enabling or disabling the preferred fencing policy	165

Section 4 Installation using the Web-based installer

169

Chapter 10 Installing Symantec VirtualStore using the Web-based installer	171
About the Web-based installer	171
Before using the Veritas Web-based installer	172
Starting the Veritas Web-based installer	172
Obtaining a security exception on Mozilla Firefox	173
Performing a pre-installation check with the Veritas Web-based installer	174
Setting installer options with the Web-based installer	174
Installing SVS with the Web-based installer	175

Chapter 11 Configuring Symantec VirtualStore	177
Configuring Symantec VirtualStore using the Web-based installer	177
Configuring Symantec VirtualStore for data integrity using the Web-based installer	182

Section 5	Automated installation using response files	191
Chapter 12	Performing an automated Symantec VirtualStore installation	193
	Installing SVS using response files	193
Chapter 13	Performing an automated Symantec VirtualStore configuration	195
	Configuring SVS using response files	195
	Response file variables to configure Symantec VirtualStore	196
Chapter 14	Performing an automated I/O fencing configuration using response files	207
	Configuring I/O fencing using response files	207
	Response file variables to configure disk-based I/O fencing	208
	Sample response file for configuring disk-based I/O fencing	211
	Response file variables to configure server-based I/O fencing	211
	Sample response file for configuring server-based I/O fencing	213
	Response file variables to configure non-SCSI-3 server-based I/O fencing	213
	Sample response file for configuring non-SCSI-3 server-based I/O fencing	214
Section 6	Installation using operating system-specific methods	217
Chapter 15	Installing Symantec VirtualStore using operating system-specific methods	219
	Installing SVS on Solaris 10 using JumpStart	219
	Overview of JumpStart installation tasks	220
	Generating the finish scripts	220
	Preparing installation resources	222
	Adding language pack information to the finish file	222
	Using a Flash archive to install SVS and the operating system	223
	Creating the Veritas post-deployment scripts	224
	Installing SVS on Solaris 11 using Automated Installer	225

	About Automated Installation	225
	Using Automated Installer	226
	Using AI to install the Solaris 11 operating system and SFHA products	227
	Manually installing packages on Oracle Solaris 11 systems	233
	Manually installing packages on Solaris brand non-global zones	233
	Installing SVS using the system command	234
Section 7	Upgrading Symantec VirtualStore	237
Chapter 16	Preparing to upgrade	239
	Upgrade methods for SVS	239
	Supported upgrade paths	240
	About using the installer to upgrade when the root disk is encapsulated	241
	Preparing to upgrade SVS	242
	Getting ready for the upgrade	242
	Creating backups	243
	Determining if the root disk is encapsulated	244
	Pre-upgrade planning for Veritas Volume Replicator	244
	Preparing to upgrade VVR when VCS agents are configured	247
	Verifying that the file systems are clean	251
	Upgrading the array support	252
Chapter 17	Performing a full upgrade using the installer	255
	Performing a full upgrade	255
	Ensuring the file systems are clean	255
	Modifying the main.cf file	256
	Performing the upgrade	259
Chapter 18	Performing a phased upgrade	263
	Performing a phased upgrade of SVS stack from version 5.1 SP1	263
	Prerequisites for a phased upgrade	264
	Planning for a phased upgrade	264
	Phased upgrade limitations	264
	Moving the service groups to the second subcluster	264
	Upgrading the SVS stack on the first subcluster	267
	Preparing the second subcluster	268
	Activating the first subcluster	270
	Upgrading the operating system on the second subcluster	271
	Upgrading the second subcluster	272

	Completing the phased upgrade	272
Chapter 19	Performing a rolling upgrade	273
	Performing a rolling upgrade using the installer	273
	About rolling upgrades	273
	Supported rolling upgrade paths	276
	Performing a rolling upgrade using the script-based installer	276
	Performing a rolling upgrade of SVS using the Web-based installer	278
Chapter 20	Upgrading the operating system	281
	Upgrading the Solaris operating system	281
Section 8	Post-installation tasks	285
Chapter 21	Performing post-upgrade tasks	287
	Changing root user into root role	287
	Re-joining the backup boot disk group into the current disk group	288
	Reverting to the backup boot disk group after an unsuccessful upgrade	288
	Register the new plugin	289
Section 9	Setting up Symantec VirtualStore	291
Chapter 22	Setting up VirtualStore	293
	About setting up VirtualStore	294
	Disabling SMF for NFS daemons	294
	Setting up Clustered NFS	296
	Setting up the VirtualStore vSphere Service Console	299
	Registering the VirtualStore cluster	300
	Verifying the VirtualStore cluster	301
	Virtual machine customization pre-requisites	301
	VMware View Integration pre-requisites	302
	Unregistering the VirtualStore cluster	302
	Displays all the VMware vCenter Servers registered	303
	Useful links from VMware on NFS support and customization while cloning virtual machines	303

Section 10	Using the extensions for Symantec VirtualStore	305
Chapter 23	Using the VirtualStore Plug-in for VMware vSphere	307
	About the VMware vSphere Plug-in for VirtualStore	307
	Adding storage to ESX servers	308
	Creating a virtual machine	309
	Creating virtual machine clones using Symantec FileSnap	309
	Specifying the number of virtual machine clones to be created	311
	Specifying where to create the virtual machine clones	311
	Specifying the guest operating system if customizing for Linux or Windows	312
	Specifying network customization parameters for guest operating systems if using DHCP or Static IP	314
	Configuring the VMware View	315
	Configuring Citrix XenDesktop	316
	Verifying the virtual machine clones	316
Chapter 24	Using the Citrix XenDesktop extension for Symantec VirtualStore	317
	About adding virtual machine clones to Citrix XenDesktop	317
	Connecting Citrix XenDesktop to a vCenter Server	318
	Adding a connection	319
	Creating virtual machine clones using the Citrix XenDesktop extension	322
	Importing virtual machines to Citrix Desktop Studio	323
	Creating a desktop group and testing the deployment	327
Section 11	Adding and removing nodes	331
Chapter 25	Adding a node to a cluster	333
	About adding a node to a cluster	333
	Before adding a node to a cluster	334
	Adding a node to a cluster using the SVS installer	336
	Adding a node using the Web-based installer	340
	Adding the node to a cluster manually	340
	Starting Veritas Volume Manager (VxVM) on the new node	341
	Configuring cluster processes on the new node	342

	Setting up the node to run in secure mode	344
	Configuring server-based fencing on the new node	347
	Starting fencing on the new node	349
	Configuring the ClusterService group for the new node	350
	Starting Cluster Volume Manager (CVM) and Cluster File System (CFS)	350
	After adding the new node	351
Chapter 26	Removing a node from a cluster	353
	Removing a node from a SVS cluster	353
	Verifying the status of nodes and service groups	354
	Deleting the departing node from SVS configuration	355
	Removing security credentials from the leaving node	358
	Removing the node configuration from the CP server	359
	Unloading LLT and GAB and removing VCS on the departing node	359
Section 12	Uninstallation of Symantec VirtualStore	363
Chapter 27	Uninstalling Symantec VirtualStore	365
	About removing Symantec VirtualStore	365
	Preparing to uninstall	365
	Shutting down cluster operations	375
	Disabling the agents on a system	376
	Removing the Replicated Data Set	376
	Uninstalling SVS packages using the script-based installer	378
	Uninstalling SVS with the Veritas Web-based installer	379
	Removing the CP server configuration using the installer program	380
Section 13	Installation reference	383
Appendix A	Tunable files for installation	385
	About setting tunable parameters using the installer or a response file	385
	Setting tunables for an installation, configuration, or upgrade	386
	Setting tunables with no other installer-related operations	387
	Setting tunables with an un-integrated response file	388
	Preparing the tunables file	389

	Setting parameters for the tunables file	389
	Tunables value parameter definitions	390
Appendix B	Installation scripts	395
	Installation script options	395
	Restarting the installer after a failed connection	401
	Starting and stopping processes for the Veritas products	401
	Installation program has improved failure handling	402
Appendix C	Configuration files	403
	About I/O fencing configuration files	403
Appendix D	Response files	407
	About response files	407
	Upgrading SVS using response files	408
	Uninstalling SVS using response files	408
	Syntax in the response file	409
	Response file variables to install, upgrade, or uninstall Symantec VirtualStore	409
	Sample response file for Symantec VirtualStore installation	411
	Sample response file for Symantec VirtualStore configuration	412
Appendix E	Configuring the secure shell or the remote shell for communications	415
	About configuring secure shell or remote shell communication modes before installing products	415
	Manually configuring and passwordless ssh	416
	Restarting the ssh session	421
	Enabling and disabling rsh for Solaris	421
Appendix F	SVS components	423
	Symantec VirtualStore installation packages	423
	Veritas Cluster Server installation packages	426
	Veritas Cluster File System installation packages	426
	Chinese language packages	427
	Japanese language packages	427
	Veritas Storage Foundation obsolete and reorganized installation packages	428

Appendix G	Sample SVS cluster setup diagrams for CP server-based I/O fencing	433
	Configuration diagrams for setting up server-based I/O fencing	433
	Two unique client clusters served by 3 CP servers	433
	Client cluster served by highly available CPS and 2 SCSI-3 disks	434
	Two node campus cluster served by remote CP server and 2 SCSI-3 disks	436
	Multiple client clusters served by highly available CP server and 2 SCSI-3 disks	438
Appendix H	Configuring LLT over UDP using IPv6	441
	Using the UDP layer of IPv6 for LLT	441
	When to use LLT over UDP	441
	Manually configuring LLT over UDP using IPv6	441
	The link command in the /etc/llttab file	442
	The set-addr command in the /etc/llttab file	443
	Selecting UDP ports	443
	Sample configuration: direct-attached links	444
	Sample configuration: links crossing IP routers	446
Appendix I	Configuring LLT over UDP using IPv4	449
	Using the UDP layer for LLT	449
	When to use LLT over UDP	449
	Manually configuring LLT over UDP using IPv4	449
	Broadcast address in the /etc/llttab file	450
	The link command in the /etc/llttab file	450
	The set-addr command in the /etc/llttab file	451
	Selecting UDP ports	452
	Configuring the netmask for LLT	453
	Configuring the broadcast address for LLT	453
	Sample configuration: direct-attached links	454
	Sample configuration: links crossing IP routers	455
Appendix J	Compatibility issues when installing Symantec VirtualStore with other products	459
	Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present	459
	Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present	460

Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present	460
Index	461

Installation overview and planning

- [Chapter 1. Introducing Symantec VirtualStore](#)
- [Chapter 2. System requirements](#)
- [Chapter 3. Planning to install Symantec VirtualStore](#)
- [Chapter 4. Licensing Symantec VirtualStore](#)

Introducing Symantec VirtualStore

This chapter includes the following topics:

- [About Symantec VirtualStore](#)
- [About Symantec VirtualStore solution for VMware environment](#)
- [About I/O fencing](#)
- [About configuring SVS clusters for data integrity](#)
- [About preferred fencing](#)

About Symantec VirtualStore

Symantec VirtualStore (SVS) powered by Veritas Storage Foundation Cluster File System High Availability (SFCFSHA) serves as a highly scalable, highly available NAS solution optimized for deploying and hosting virtual machine. VirtualStore is built on top of Cluster File System (CFS), which provides high availability and linear scalability across the cluster.

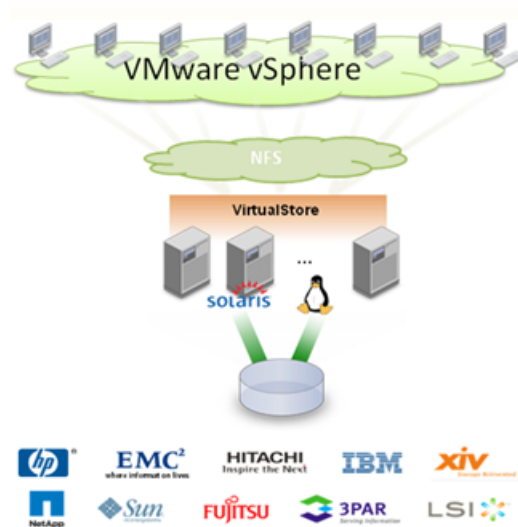
About Symantec VirtualStore solution for VMware environment

Symantec VirtualStore powered by Veritas Storage Foundation Cluster File System High Availability (SFCFSHA) is an optimized and customized NAS solution for your VMware environments. It provides the benefits of a highly scalable NAS and NFS solution for the VMware ESX workloads. With seamless integration with VMware Virtual Center, VirtualStore gives you a complete solution to efficiently

manage the VMware ESX NAS storage and leverage some of the key underlying benefits of the SFCFSHA.

- Provide standard NAS/NFS interfaces to interact with the VMware Virtual Infrastructure.
- Compatibility with VMotion (and storage VMotion).
- Balance datastore based on SVS Cluster Virtual IP addresses for optimized IO.
- Leverage key capabilities within the SFCFSHA (export same file system through multiple NAS heads, SmartTier, and high availability plus others...).
- Leverage SFCFSHA File snapshot technology that would let you take multiple copies of a large file.
- Page file caching for optimized read-IO access to shared pages for virtual machine disk access.

Figure 1-1 VirtualStore VMware Vsphere environment



About I/O fencing

I/O fencing protects the data on shared disks when nodes in a cluster detect a change in the cluster membership that indicates a split-brain condition.

The fencing operation determines the following:

- The nodes that must retain access to the shared storage
- The nodes that must be ejected from the cluster

This decision prevents possible data corruption. The installer installs the I/O fencing driver, VRTSvxfen package, when you install Symantec VirtualStore. To protect data on shared disks, you must configure I/O fencing after you install and configure Symantec VirtualStore.

I/O fencing technology uses coordination points for arbitration in the event of a network partition.

I/O fencing coordination points can be coordinator disks or coordination point servers (CP servers) or both. You can configure disk-based or server-based I/O fencing:

Disk-based I/O fencing	<p>I/O fencing that uses coordinator disks is referred to as disk-based I/O fencing.</p> <p>Disk-based I/O fencing ensures data integrity in a single cluster.</p>
Server-based I/O fencing	<p>I/O fencing that uses at least one CP server system is referred to as server-based I/O fencing.</p> <p>Server-based fencing can include only CP servers, or a mix of CP servers and coordinator disks.</p> <p>Server-based I/O fencing ensures data integrity in clusters.</p> <p>In virtualized environments that do not support SCSI-3 PR, Symantec VirtualStore supports non-SCSI-3 server-based I/O fencing.</p>

See [“About planning to configure I/O fencing”](#) on page 71.

Note: Symantec recommends that you use I/O fencing to protect your cluster against split-brain situations.

See the *Symantec VirtualStore Administrator's Guide*.

About configuring SVS clusters for data integrity

When a node fails, SVS takes corrective action and configures its components to reflect the altered membership. If an actual node failure did not occur and if the symptoms were identical to those of a failed node, then such corrective action would cause a split-brain situation.

Some example scenarios that can cause such split-brain situations are as follows:

- Broken set of private networks

If a system in a two-node cluster fails, the system stops sending heartbeats over the private interconnects. The remaining node then takes corrective action. The failure of the private interconnects, instead of the actual nodes, presents identical symptoms and causes each node to determine its peer has departed. This situation typically results in data corruption because both nodes try to take control of data storage in an uncoordinated manner.

- System that appears to have a system-hang
If a system is so busy that it appears to stop responding, the other nodes could declare it as dead. This declaration may also occur for the nodes that use the hardware that supports a "break" and "resume" function. When a node drops to PROM level with a break and subsequently resumes operations, the other nodes may declare the system dead. They can declare it dead even if the system later returns and begins write operations.

I/O fencing is a feature that prevents data corruption in the event of a communication breakdown in a cluster. SVS uses I/O fencing to remove the risk that is associated with split-brain. I/O fencing allows write access for members of the active cluster. It blocks access to storage from non-members so that even a node that is alive is unable to cause damage.

After you install and configure SVS, you must configure I/O fencing in SVS to ensure data integrity.

See [“About planning to configure I/O fencing”](#) on page 71.

About I/O fencing for Symantec VirtualStore in virtual machines that do not support SCSI-3 PR

In a traditional I/O fencing implementation, where the coordination points are coordination point servers (CP servers) or coordinator disks, Veritas Clustered Volume Manager and Veritas I/O fencing modules provide SCSI-3 persistent reservation (SCSI-3 PR) based protection on the data disks. This SCSI-3 PR protection ensures that the I/O operations from the losing node cannot reach a disk that the surviving sub-cluster has already taken over.

See the *Veritas Cluster Server Administrator's Guide* for more information on how I/O fencing works.

In virtualized environments that do not support SCSI-3 PR, Symantec VirtualStore attempts to provide reasonable safety for the data disks. Symantec VirtualStore requires you to configure non-SCSI-3 server-based I/O fencing in such environments. Non-SCSI-3 fencing uses CP servers as coordination points with some additional configuration changes to support I/O fencing in such environments.

See [“Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsvs”](#) on page 146.

See [“Setting up non-SCSI-3 fencing in virtual environments manually”](#) on page 160.

About I/O fencing components

The shared storage for SVS must support SCSI-3 persistent reservations to enable I/O fencing. SVS involves two types of shared storage:

- Data disks—Store shared data
See [“About data disks”](#) on page 25.
- Coordination points—Act as a global lock during membership changes
See [“About coordination points”](#) on page 25.

About data disks

Data disks are standard disk devices for data storage and are either physical disks or RAID Logical Units (LUNs).

These disks must support SCSI-3 PR and must be part of standard VxVM or CVM disk groups. CVM is responsible for fencing data disks on a disk group basis. Disks that are added to a disk group and new paths that are discovered for a device are automatically fenced.

About coordination points

Coordination points provide a lock mechanism to determine which nodes get to fence off data drives from other nodes. A node must eject a peer from the coordination points before it can fence the peer from the data drives. SVS prevents split-brain when vxfen races for control of the coordination points and the winner partition fences the ejected nodes from accessing the data disks.

Note: Typically, a fencing configuration for a cluster must have three coordination points. Symantec also supports server-based fencing with a single CP server as its only coordination point with a caveat that this CP server becomes a single point of failure.

The coordination points can either be disks or servers or both.

- Coordinator disks
Disks that act as coordination points are called coordinator disks. Coordinator disks are three standard disks or LUNs set aside for I/O fencing during cluster reconfiguration. Coordinator disks do not serve any other storage purpose in the SVS configuration.

You can configure coordinator disks to use Veritas Volume Manager Dynamic Multi-pathing (DMP) feature. Dynamic Multi-pathing (DMP) allows coordinator disks to take advantage of the path failover and the dynamic adding and removal capabilities of DMP. So, you can configure I/O fencing to use either DMP devices or the underlying raw character devices. I/O fencing uses SCSI-3 disk policy that is either raw or dmp based on the disk device that you use. The disk policy is dmp by default.

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

■ Coordination point servers

The coordination point server (CP server) is a software solution which runs on a remote system or cluster. CP server provides arbitration functionality by allowing the SVS cluster nodes to perform the following tasks:

- Self-register to become a member of an active SVS cluster (registered with CP server) with access to the data drives
- Check which other nodes are registered as members of this active SVS cluster
- Self-unregister from this active SVS cluster
- Forcefully unregister other nodes (preempt) as members of this active SVS cluster

In short, the CP server functions as another arbitration mechanism that integrates within the existing I/O fencing module.

Note: With the CP server, the fencing arbitration logic still remains on the SVS cluster.

Multiple SVS clusters running different operating systems can simultaneously access the CP server. TCP/IP based communication is used between the CP server and the SVS clusters.

About preferred fencing

The I/O fencing driver uses coordination points to prevent split-brain in a VCS cluster. By default, the fencing driver favors the subcluster with maximum number of nodes during the race for coordination points. With the preferred fencing feature, you can specify how the fencing driver must determine the surviving subcluster.

You can configure the preferred fencing policy using the cluster-level attribute PreferredFencingPolicy for the following:

- Enable system-based preferred fencing policy to give preference to high capacity systems.
- Enable group-based preferred fencing policy to give preference to service groups for high priority applications.
- Disable preferred fencing policy to use the default node count-based race policy.

See the *Symantec VirtualStore Administrator's Guide* for more details.

See [“Enabling or disabling the preferred fencing policy”](#) on page 165.

System requirements

This chapter includes the following topics:

- [Release notes](#)
- [Hardware compatibility list \(HCL\)](#)
- [Supported operating systems](#)
- [I/O fencing requirements](#)
- [Veritas File System requirements](#)
- [Database requirements](#)
- [Disk space requirements](#)
- [Discovering product versions and various requirement information](#)

Release notes

The *Release Notes* for each Veritas product contains last minute news and important details for each product, including updates to system requirements and supported software. Review the Release Notes for the latest information before you start installing the product.

The product documentation is available on the Web at the following location:

<https://sort.symantec.com/documents>

Hardware compatibility list (HCL)

The hardware compatibility list contains information about supported hardware and is updated regularly. Before installing or upgrading Storage Foundation and

High Availability Solutions products, review the current compatibility list to confirm the compatibility of your hardware and software.

For the latest information on supported hardware, visit the following URL:

<http://www.symantec.com/docs/TECH170013>

For information on specific High Availability setup requirements, see the *Veritas Cluster Server Installation Guide*.

Supported operating systems

For information on supported operating systems, see the *Symantec VirtualStore Release Notes*.

I/O fencing requirements

Depending on whether you plan to configure disk-based fencing or server-based fencing, make sure that you meet the requirements for coordination points:

- Coordinator disks
See “[Coordinator disk requirements for I/O fencing](#)” on page 30.
- CP servers
See “[CP server requirements](#)” on page 31.

If you have installed Symantec VirtualStore in a virtual environment that is not SCSI-3 PR compliant, review the requirements to configure non-SCSI-3 server-based fencing.

See “[Non-SCSI-3 I/O fencing requirements](#)” on page 34.

Coordinator disk requirements for I/O fencing

Make sure that the I/O fencing coordinator disks meet the following requirements:

- For disk-based I/O fencing, you must have at least three coordinator disks or there must be odd number of coordinator disks.
- The coordinator disks can be raw devices, DMP devices, or iSCSI devices.
- Each of the coordinator disks must use a physically separate disk or LUN. Symantec recommends using the smallest possible LUNs for coordinator disks.
- Each of the coordinator disks should exist on a different disk array, if possible.
- The coordinator disks must support SCSI-3 persistent reservations.
- Symantec recommends using hardware-based mirroring for coordinator disks.

- Coordinator disks must not be used to store data or must not be included in disk groups that store user data.
- Coordinator disks cannot be the special devices that array vendors use. For example, you cannot use EMC gatekeeper devices as coordinator disks.

CP server requirements

Symantec VirtualStore 6.0.1 clusters (application clusters) support coordination point servers (CP servers) which are hosted on the following VCS and SFHA versions:

- VCS 6.0.1, VCS 6.0, VCS 6.0 PR1, VCS 6.0 RP1, VCS 5.1SP1, or VCS 5.1 single-node cluster
Single-node VCS clusters with VCS 5.1 SP1 RP1 and later or VCS 6.0 and later that hosts CP server does not require LLT and GAB to be configured.
- SFHA 6.0.1, SFHA 6.0, SFHA 6.0 PR1, SFHA 6.0 RP1, 5.1SP1, or 5.1 cluster

Warning: Before you upgrade 5.1 CP server nodes to use VCS or SFHA 6.0.1, you must upgrade all the application clusters that use this CP server to version 6.0.1. Application clusters at version 5.1 cannot communicate with CP server that runs VCS or SFHA 5.1 SP1 or later.

Make sure that you meet the basic hardware requirements for the VCS/SFHA cluster to host the CP server.

See the *Veritas Cluster Server Installation Guide* or the *Veritas Storage Foundation High Availability Installation Guide*.

Note: While Symantec recommends at least three coordination points for fencing, a single CP server as coordination point is a supported server-based fencing configuration. Such single CP server fencing configuration requires that the coordination point be a highly available CP server that is hosted on an SFHA cluster.

Make sure you meet the following additional CP server requirements which are covered in this section before you install and configure CP server:

- Hardware requirements
- Operating system requirements
- Networking requirements (and recommendations)
- Security requirements

[Table 2-1](#) lists additional requirements for hosting the CP server.

Table 2-1 CP server hardware requirements

Hardware required	Description
Disk space	<p>To host the CP server on a VCS cluster or SFHA cluster, each host requires the following file system space:</p> <ul style="list-style-type: none"> ■ 550 MB in the /opt directory (additionally, the language pack requires another 15 MB) ■ 300 MB in /usr ■ 20 MB in /var ■ 10 MB in /etc (for the CP server database) <p>See “Disk space requirements” on page 36.</p>
Storage	<p>When CP server is hosted on an SFHA cluster, there must be shared storage between the nodes of this SFHA cluster.</p>
RAM	<p>Each CP server requires at least 512 MB.</p>
Network	<p>Network hardware capable of providing TCP/IP connection between CP servers and SVS clusters (application clusters).</p>

[Table 2-2](#) displays the CP server supported operating systems and versions. An application cluster can use a CP server that runs any of the following supported operating systems.

Table 2-2 CP server supported operating systems and versions

CP server	Operating system and version
CP server hosted on a VCS single-node cluster or on an SFHA cluster	<p>CP server supports any of the following operating systems:</p> <ul style="list-style-type: none"> ■ AIX 6.1 and 7.1 ■ HP-UX 11i v3 ■ Linux: <ul style="list-style-type: none"> ■ RHEL 5 ■ RHEL 6 ■ SLES 10 ■ SLES 11 ■ Oracle Solaris 10 ■ Oracle Solaris 11 <p>Review other details such as supported operating system levels and architecture for the supported operating systems.</p> <p>See the <i>Veritas Cluster Server Release Notes</i> or the <i>Veritas Storage Foundation High Availability Release Notes</i> for that platform.</p>

Following are the CP server networking requirements and recommendations:

- Symantec recommends that network access from the application clusters to the CP servers should be made highly-available and redundant. The network connections require either a secure LAN or VPN.
- The CP server uses the TCP/IP protocol to connect to and communicate with the application clusters by these network paths. The CP server listens for messages from the application clusters using TCP port 14250. This is the default port that can be changed during a CP server configuration. Symantec recommends that you configure multiple network paths to access a CP server. If a network path fails, CP server does not require a restart and continues to listen on all the other available virtual IP addresses.
- The CP server supports either Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with the application clusters. If the CP server is configured to use an IPv6 virtual IP address, then the application clusters should also be on the IPv6 network where the CP server is hosted.
- When placing the CP servers within a specific network configuration, you must take into consideration the number of hops from the different application cluster nodes to the CP servers. As a best practice, Symantec recommends that the number of hops and network latency from the different application cluster nodes to the CP servers should be equal. This ensures that if an event occurs that results in an I/O fencing scenario, there is no bias in the race due to

difference in number of hops or network latency between the CPS and various nodes.

For secure communication between the SVS cluster (application cluster) and the CP server, review the following support matrix:

Communication mode	CP server in secure mode	CP server in non-secure mode
SVS cluster in secure mode	Yes	Yes
SVS cluster in non-secure mode	Yes	Yes

For secure communications between the SVS and CP server, consider the following requirements and suggestions:

- In a secure communication environment, all CP servers that are used by the application cluster must be configured with security enabled. A configuration where the application cluster uses some CP servers running with security enabled and other CP servers running with security disabled is not supported.
- For non-secure communication between CP server and application clusters, there is no need to configure Symantec Product Authentication Service. In non-secure mode, authorization is still provided by CP server for the application cluster users. The authorization that is performed only ensures that authorized users can perform appropriate actions as per their user privileges on the CP server.

For information about establishing secure communications between the application cluster and CP server, see the *Symantec VirtualStore Administrator's Guide*.

Non-SCSI-3 I/O fencing requirements

Supported virtual environment for non-SCSI-3 fencing:

- Solaris 10 Update 7 and later, Oracle Solaris 11
Oracle VM Server for SPARC 2.0 and 2.1
Guest operating system: Oracle Solaris 10, Oracle Solaris 11

Make sure that you also meet the following requirements to configure non-SCSI-3 fencing in the virtual environments that do not support SCSI-3 PR:

- Symantec VirtualStore must be configured with Cluster attribute UseFence set to SCSI3
- All coordination points must be CP servers

Veritas File System requirements

Veritas File System requires that the values of the Solaris variables `lwp_default_stksize` and `svc_default_stksize` are at least 0x6000 (for Solaris 10) and 0x8000 (for Solaris 11). When you install the Veritas File System package, `VRTSvxfs`, the `VRTSvxfs` packaging scripts check the values of these variables in the kernel. If the values are less than the required values, `VRTSvxfs` increases the values and modifies the `/etc/system` file with the required values. If the `VRTSvxfs` scripts increase the values, the installation proceeds as usual except that you must reboot and restart the installation program. A message displays if a reboot is required.

To avoid an unexpected need for a reboot, verify the values of the variables before installing Veritas File System. Use the following commands to check the values of the variables:

```
For Solaris 10: # echo "lwp_default_stksize/X" | mdb -k
                lwp_default_stksize:
                lwp_default_stksize:          6000

                # echo "svc_default_stksize/X" | mdb -k
                svc_default_stksize:
                svc_default_stksize:          6000

For Solaris 11: # echo "lwp_default_stksize/X" | mdb -k
                lwp_default_stksize:
                lwp_default_stksize:          8000

                # echo "svc_default_stksize/X" | mdb -k
                svc_default_stksize:
                svc_default_stksize:          8000
```

If the values shown are less than 6000 (for Solaris 10) and less than 8000 (for Solaris 11), you can expect a reboot after installation.

Note: The default value of the `svc_default_stksize` variable is 0 (zero), which indicates that the value is set to the value of the `lwp_default_stksize` variable. In this case, no reboot is required, unless the value of the `lwp_default_stksize` variable is too small.

To avoid a reboot after installation, you can modify the `/etc/system` file with the appropriate values. Reboot the system prior to installing the packages. Add the following lines to the `/etc/system` file:

```
For Solaris 10:  set lwp_default_stksize=0x6000
                 set rpcmod:svc_default_stksize=0x6000
```

```
For Solaris 11:  set lwp_default_stksize=0x8000
                 set rpcmod:svc_default_stksize=0x8000
```

Database requirements

The following TechNote identifies the most current information on supported database and operating system combinations:

<http://www.symantec.com/docs/DOC4039>

Note: SVS supports running Oracle, DB2, and Sybase on VxFS and VxVM.

SVS does not support running SFDB tools with DB2 and Oracle.

Disk space requirements

Before installing your products, confirm that your system has enough free disk space.

Use the "Perform a Pre-installation Check" (P) menu for the Web-based installer or the `-precheck` option of the script-based installer to determine whether there is sufficient space.

Go to the installation directory and run the installer with the `-precheck` option.

```
# ./installer -precheck
```

If you have downloaded SVS, you must use the following command:

```
# ./installsvs -precheck<version>
```

Where `<version>` is the specific release version.

See ["About the Veritas installer"](#) on page 41.

Discovering product versions and various requirement information

Symantec provides several methods to check the Veritas product you have installed, plus various requirement information.

You can check the existing product versions using the `installer` command with the `-version` option before or after you install. After you have installed the current version of the product, you can use the `showversion` script in the `/opt/VRTS/install` directory to find version information.

Information the `version` option or the `showversion` script discovers on systems includes the following:

- The installed version of all released Storage Foundation and High Availability Suite of products
- The required packages or patches (if applicable) that are missing
- The available updates (including patches or hotfixes) from Symantec Operations Readiness Tools (SORT) for the installed products

To run the version checker

- 1 Mount the media.
- 2 Start the installer with the `-version` option.

```
# ./installer -version system1 system2
```


Planning to install Symantec VirtualStore

This chapter includes the following topics:

- [About planning for SVS installation](#)
- [About installation and configuration methods](#)
- [About the Veritas installer](#)
- [Assessing the system for installation readiness](#)
- [Downloading the Symantec VirtualStore software](#)
- [Setting environment variables](#)
- [Optimizing LLT media speed settings on private NICs](#)
- [Guidelines for setting the media speed of the LLT interconnects](#)
- [Creating the /opt directory](#)
- [About using ssh or rsh with the Veritas installer](#)
- [Setting up shared storage](#)
- [Creating root user](#)
- [Prerequisites for installing Symantec VirtualStore](#)
- [Hardware overview and requirements for Symantec VirtualStore](#)

About planning for SVS installation

Before you continue, make sure that you are using the current version of this guide. The latest documentation is available on the Symantec Symantec Operations Readiness Tools (SORT) website.

<https://sort.symantec.com/documents>

Document version: 6.0.1 Rev 0.

This installation guide is designed for system administrators who already have a knowledge of basic UNIX system and network administration. Basic knowledge includes commands such as `tar`, `mkdir`, and simple shell scripting. Also required is basic familiarity with the specific platform and operating system where SVS will be installed.

Follow the preinstallation instructions if you are installing Symantec VirtualStore. The following Symantec VirtualStore is installed with these instructions:

- Symantec VirtualStore

About installation and configuration methods

You can use one of the following methods to install and configure SVS.

Table 3-1 Installation and configuration methods

Method	Description
Interactive installation and configuration using the script-based installer Note: If you obtained SVS from an electronic download site, you must use the <code>installsvs</code> script instead of the <code>installer</code> script.	You can use one of the following script-based installers: <ul style="list-style-type: none">■ Common product installer script: <code>installer</code> The common product installer script provides a menu that simplifies the selection of installation and configuration options.■ Product-specific installation script: <code>installsvs</code>■ The product-specific installation script provides command-line interface options. Installing and configuring with the <code>installsvs</code> script is identical to specifying SVS from the <code>installer</code> script. Use this method to install or configure only SVS.

Table 3-1 Installation and configuration methods (*continued*)

Method	Description
Silent installation using the response file	The response file automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. You can use the script-based installers with the response file to install silently on one or more systems. See “About response files” on page 407.
Web-based installer	The Web-based installer provides an interface to manage the installation and configuration from a remote site using a standard Web browser. <code>webinstaller</code> See “About the Web-based installer” on page 171.
JumpStart (For Solaris 10 systems)	You can use the Veritas product installer of the product-specific installation script to generate a JumpStart script file. Use the generated script to install Veritas packages from your JumpStart server. See “Installing SVS on Solaris 10 using JumpStart” on page 219.
Manual installation and configuration	Manual installation uses the Solaris commands to install SVS. To retrieve a list of all packages and patches required for all products in the correct installation order, enter: <code># installsvs -allpkgs</code> Use the Solaris commands to install SVS. Then use a manual or an interactive method with <code>installsvs</code> or <code>installer</code> script to configure the SVS stack.
Automated Installer (For Solaris 11 systems)	You can use the Oracle Solaris Automated Installer (AI) to install the Solaris operating system on multiple client systems in a network. AI performs a hands-free installation (automated installation without manual interactions) of both x86 and SPARC systems.

About the Veritas installer

To install your Veritas product, use one of the following methods:

- The general product installer. The general product installer enables you to install and configure the product, verify preinstallation requirements, and

view the product’s description. You perform the installation from a disc, and you are prompted to choose a product to install.

See “[Installing Symantec VirtualStore using the installer](#)” on page 67.

- **Product-specific installation scripts.** If you obtained a standalone Veritas product from an electronic download site, the single product download files do not contain the general product installer. Use the product installation script to install the individual products. You can find these scripts at the root of the product media in the scripts directory. These scripts are also installed with the product.

[Table 3-2](#) lists all the SFHA Solutions product installation scripts. The list of product installation scripts that you find on your system depends on the product that you install on your system.

Note: The name of the script is different depending on whether you run the script from the install media or from a system on which the product software is installed.

Table 3-2 Product installation scripts

Veritas product name	Product installation script (When running the script from the install media)	Product installation script (When running the script from a system on which the SFHA Solutions product is installed)
Veritas Cluster Server (VCS)	installvcs	installvcs<version>
Veritas Storage Foundation (SF)	installsf	installsf<version>
Veritas Storage Foundation and High Availability (SFHA)	installsfha	installsfha<version>
Veritas Storage Foundation Cluster File System High Availability (SFCFSHA)	installsfcfsha	installsfcfsha<version>
Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)	installsfrac	installsfrac<version>
Veritas Storage Foundation for Sybase ASE CE (SF Sybase CE)	installsfsybasece	installsfsybasece<version>

Table 3-2 Product installation scripts (*continued*)

Veritas product name	Product installation script (When running the script from the install media)	Product installation script (When running the script from a system on which the SFHA Solutions product is installed)
Veritas Dynamic Multi-Pathing	installdmp	installdmp<version>
Symantec VirtualStore	installsvs	installsvs<version>

The scripts that are installed on the system include the product version in the script name. For example, to install the SVS script from the install media, run the `installsvs` command. However, to run the script from the installed binaries, run the `installsvs<version>` command.

For example, for the 6.0.1 version:

```
# /opt/VRTS/install/installsvs601 -configure
```

Note: Do not include the release version if you use the general product installer to install the product.

At most points during the installation you can type the following characters for different actions:

- Use `b` (back) to return to a previous section of the installation procedure. The back feature of the installation scripts is context-sensitive, so it returns to the beginning of a grouped section of questions.
- Use `Control+c` to stop and exit the program if an installation procedure hangs. After a short delay, the script exits.
- Use `q` to quit the installer.
- Use `?` to display help information.
- Use the Enter button to accept a default response.

See [“Installation script options”](#) on page 395.

Assessing the system for installation readiness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing 6.0.1.

Prechecking your systems using the installer Performs a pre-installation check on the specified systems. The Veritas product installer reports whether the specified systems meet the minimum requirements for installing 6.0.1.

See [“Prechecking your systems using the Veritas installer”](#) on page 44.

Prechecking your systems using the Veritas installer

The script-based and Web-based installer's precheck option checks for the following:

- Recommended swap space for installation
- Recommended memory sizes on target systems for Veritas programs for best performance
- Required operating system versions

To use the precheck option

- 1 Start the script-based or Web-based installer.
See [“Installing SVS with the Web-based installer”](#) on page 175.
- 2 Select the precheck option:
 - From the Web-based installer, select the **Perform a Pre-Installation Check** from the Task pull-down menu.
 - In the script-based installer, from root on the system where you want to perform the check, start the installer.

```
# ./installer
```

In the Task Menu, press the p key to start the precheck.

- 3 Review the output and make the changes that the installer recommends.

Downloading the Symantec VirtualStore software

One method of obtaining the Symantec VirtualStore software is to download it to your local system from the Symantec Web site.

For a Trialware download, perform the following. Contact your Veritas representative for more information.

To download the trialware version of the software

- 1 Open the following link in your browser:
<http://www.symantec.com/index.jsp>
- 2 In Products and Solutions section, click the **Trialware & Downloads** link.
- 3 On the next page near the bottom of the page, click **Business Continuity**.
- 4 Under Cluster Server, click **Download Now**.
- 5 In the new window, click **Download Now**.
- 6 Review the terms and conditions, and click **I agree**.
- 7 You can use existing credentials to log in or create new credentials.
- 8 Find the product that you want to download and select it. Continue with the installation.

If you download a standalone Veritas product, the single product download files do not contain the product installer. Use the installation script for the specific product to install the product.

Note: Trialware is the full product version. The enabled licensing places the product in a demo or a trial state.

See “[About the Veritas installer](#)” on page 41.

To download the software

- 1 Verify that you have enough space on your filesystem to store the downloaded software.

The estimated space for download, gunzip, and tar extract is 2 GB for SPARC and 1.5 GB for Opteron.

If you plan to install the software on the same system, make sure that you also have enough space for the installed software.

See “[Disk space requirements](#)” on page 36.

- 2 To see the space available, you can use the `df` command with the name of the local file system where you intend to download the software.

```
# /usr/bin/df -l filesystem
```

Caution: When you select a location to download files, do not select a directory that contains Veritas products from a previous release or maintenance pack. Make sure that different versions exist in different directories.

- 3 Download the software, specifying the file system with sufficient space for the file.

Setting environment variables

Most of the commands used in the installation are in the `/sbin` or `/usr/sbin` directory. Add these directories to your `PATH` environment variable as necessary.

After installation, SVS commands are in `/opt/VRTS/bin`. SVS manual pages are stored in `/opt/VRTS/man`.

Add the following directories to your `PATH` and `MANPATH` environment variable:

- If you are using Bourne or Korn shell (`sh` or `ksh`), enter the following:

```
$ PATH=$PATH:/usr/sbin:/opt/VRTS/bin
$ MANPATH=/usr/share/man:/opt/VRTS/man:$MANPATH
$ export PATH MANPATH
```

- If you are using a C shell (`csh` or `tcsh`), enter the following:

```
% set path = ( $path /usr/sbin /opt/VRTS/bin )
% setenv MANPATH /usr/share/man:/opt/VRTS/man:$MANPATH
```

Optimizing LLT media speed settings on private NICs

For optimal LLT communication among the cluster nodes, the interface cards on each node must use the same media speed settings. Also, the settings for the switches or the hubs that are used for the LLT interconnections must match that of the interface cards. Incorrect settings can cause poor network performance or even network failure.

If you use different media speed for the private NICs, Symantec recommends that you configure the NICs with lesser speed as low-priority links to enhance LLT performance.

Guidelines for setting the media speed of the LLT interconnects

Review the following guidelines for setting the media speed of the LLT interconnects:

- Symantec recommends that you manually set the same media speed setting on each Ethernet card on each node.
If you use different media speed for the private NICs, Symantec recommends that you configure the NICs with lesser speed as low-priority links to enhance LLT performance.
- If you have hubs or switches for LLT interconnects, then set the hub or switch port to the same setting as used on the cards on each node.
- If you use directly connected Ethernet links (using crossover cables), Symantec recommends that you set the media speed to the highest value common to both cards, typically 1000_Full_Duplex.

Details for setting the media speeds for specific devices are outside of the scope of this manual. Consult the device's documentation or the operating system manual for more information.

Creating the /opt directory

The directory `/opt` must exist, be writable and must not be a symbolic link.

If you are upgrading, you cannot have a symbolic link from `/opt` to an unconverted volume. If you do have a symbolic link to an unconverted volume, the symbolic link will not function during the upgrade and items in `/opt` will not be installed.

About using ssh or rsh with the Veritas installer

The installer uses passwordless secure shell (ssh) or remote shell (rsh) communications among systems. The installer uses the ssh or rsh daemon that comes bundled with the operating system. During an installation, you choose the communication method that you want to use. You then provide the installer with the superuser passwords for the systems where you plan to install. The ssh or rsh communication among the systems is removed when the installation process completes, unless the installation abruptly terminates. If installation terminated abruptly, use the installation script's `-comcleanup` option to remove the ssh or rsh configuration from the systems.

See [“Installation script options”](#) on page 395.

In most installation, configuration, upgrade (where necessary), and uninstallation scenarios, the installer can configure ssh or rsh on the target systems. In the following scenarios, you need to set up ssh or rsh manually:

- When you perform installer sessions using a response file.

See [“About configuring secure shell or remote shell communication modes before installing products”](#) on page 415.

Setting up shared storage

The following sections describe how to set up the SCSI and the Fibre Channel devices that the cluster systems share.

For I/O fencing, the data disks must support SCSI-3 persistent reservations. You need to configure a coordinator disk group that supports SCSI-3 PR and verify that it works.

See [“About planning to configure I/O fencing”](#) on page 71.

See also the *Symantec VirtualStore Administrator's Guide* for a description of I/O fencing.

Setting up shared storage: SCSI disks

When SCSI devices are used for shared storage, the SCSI address or SCSI initiator ID of each node must be unique. Since each node typically has the default SCSI address of "7," the addresses of one or more nodes must be changed to avoid a conflict. In the following example, two nodes share SCSI devices. The SCSI address of one node is changed to "5" by using `nvedit` commands to edit the `nvrarc` script.

If you have more than two systems that share the SCSI bus, do the following:

- Use the same procedure to set up shared storage.
- Make sure to meet the following requirements:
 - The storage devices have power before any of the systems
 - Only one node runs at one time until each node's address is set to a unique value

To set up shared storage

- 1 Install the required SCSI host adapters on each node that connects to the storage, and make cable connections to the storage.
 Refer to the documentation that is shipped with the host adapters, the storage, and the systems.
- 2 With both nodes powered off, power on the storage devices.
- 3 Power on one system, but do not allow it to boot. If necessary, halt the system so that you can use the ok prompt.

Note that only one system must run at a time to avoid address conflicts.

- 4 Find the paths to the host adapters:

```
{0} ok show-disks
...b) /sbus@6,0/QLGC,isp@2,10000/sd
```

The example output shows the path to one host adapter. You must include the path information without the "/sd" directory, in the `nvrामrc` script. The path information varies from system to system.

- 5 Edit the `nvrामrc` script on to change the `scsi-initiator-id` to 5. (The *Solaris OpenBoot 3.x Command Reference Manual* contains a full list of `nvedit` commands and keystrokes.) For example:

```
{0} ok nvedit
```

As you edit the script, note the following points:

- Each line is numbered, 0:, 1:, 2:, and so on, as you enter the `nvedit` commands.
- On the line where the `scsi-initiator-id` is set, insert exactly one space after the first quotation mark and before `scsi-initiator-id`.

In this example, edit the `nvrामrc` script as follows:

```
0: probe-all
1: cd /sbus@6,0/QLGC,isp@2,10000
2: 5 " scsi-initiator-id" integer-property
```

```
3: device-end  
4: install-console  
5: banner  
6: <CTRL-C>
```

- 6 Store the changes you make to the `nvrामrc` script. The changes you make are temporary until you store them.

```
{0} ok nvstore
```

If you are not sure of the changes you made, you can re-edit the script without risk before you store it. You can display the contents of the `nvrामrc` script by entering:

```
{0} ok printenv nvrामrc
```

You can re-edit the file to make corrections:

```
{0} ok nvedit
```

Or, discard the changes if necessary by entering:

```
{0} ok nvquit
```

- 7 Instruct the OpenBoot PROM Monitor to use the `nvrामrc` script on the node.

```
{0} ok setenv use-nvrामrc? true
```

- 8 Reboot the node. If necessary, halt the system so that you can use the `ok` prompt.

- 9 Verify that the `scsi-initiator-id` has changed. Go to the `ok` prompt. Use the output of the `show-disks` command to find the paths for the host adapters. Then, display the properties for the paths. For example:

```
{0} ok show-disks
...b) /sbus@6,0/QLGC,isp@2,10000/sd
{0} ok cd /sbus@6,0/QLGC,isp@2,10000
{0} ok .properties
scsi-initiator-id      00000005
```

Permit the system to continue booting.

- 10 Boot the second node. If necessary, halt the system to use the `ok` prompt. Verify that the `scsi-initiator-id` is 7. Use the output of the `show-disks` command to find the paths for the host adapters. Then, display the properties for that paths. For example:

```
{0} ok show-disks
...b) /sbus@6,0/QLGC,isp@2,10000/sd
{0} ok cd /sbus@6,0/QLGC,isp@2,10000
{0} ok .properties
scsi-initiator-id      00000007
```

Permit the system to continue booting.

Setting up shared storage: Fibre Channel

Perform the following steps to set up Fibre Channel.

To set up shared storage

- 1 Install the required FC-AL controllers.
- 2 Connect the FC-AL controllers and the shared storage devices to the same hub or switch.

All systems must see all the shared devices that are required to run the critical application. If you want to implement zoning for a fibre switch, make sure that no zoning prevents all systems from seeing all these shared devices.

- 3 Boot each system with the reconfigure devices option:

```
ok boot -r
```

- 4 After all systems have booted, use the `format (1m)` command to verify that each system can see all shared devices.

If Volume Manager is used, the same number of external disk devices must appear, but device names (c#t#d#s#) may differ.

If Volume Manager is not used, then you must meet the following requirements:

- The same number of external disk devices must appear.
- The device names must be identical for all devices on all systems.

Creating root user

On Oracle Solaris 11, you need to change the root role into a user as you cannot directly log in as root user.

To change root role into a user

- 1 Log in as local user and assume the root role.

```
% su - root
```

- 2 Remove the root role from local users who have been assigned the role.

```
# roles admin  
  
root  
  
# usermod -R " " admin
```

- 3 Change the root role into a user.

```
# rolemod -K type=normal root
```

- 4 Verify the change.

- # getent user_attr root

```
root:::auths=solaris.*;profiles=All;audit_flags=lo\  
:no;lock_after_retries=no;min_label=admin_low;clearance=admin_high
```

If the `type` keyword is missing in the output or is equal to `normal`, the account is not a role.

- # userattr type root

If the output is empty or lists `normal`, the account is not a role.

Note: For more information, see the Oracle documentation on Oracle Solaris 11 operating system.

Note: After installation, you may want to change root user into root role to allow local users to assume the root role.

See [“Changing root user into root role”](#) on page 287.

Prerequisites for installing Symantec VirtualStore

Each cluster node must be connected to the public network and each must have a unique host name by which it can be addressed on the public network. The local node from which you install does not have to be part of the cluster.

Provide the following information when installing SVS:

- The cluster name, beginning with a letter (a-z, A-Z).
- A unique ID from 0-65535 for the cluster. Within the public subnet, a new cluster using a duplicate cluster ID can cause existing clusters to fail.
- The host names of the cluster nodes.
- The device names of the network interface cards (NICs) used for the private networks among nodes.
- Establishing communication between nodes is required to install Veritas software from a remote system, or to install and configure a cluster. The node from which the installation utility is run must have permissions to run `rsh` (remote shell) or `ssh` (secure shell) utilities as root on all cluster nodes or remote systems.
- Symantec recommends configuring the cluster with I/O fencing enabled. I/O fencing requires shared devices to support SCSI-3 Persistent Reservations (PR). Enabling I/O fencing prevents data corruption caused by a split brain scenario.

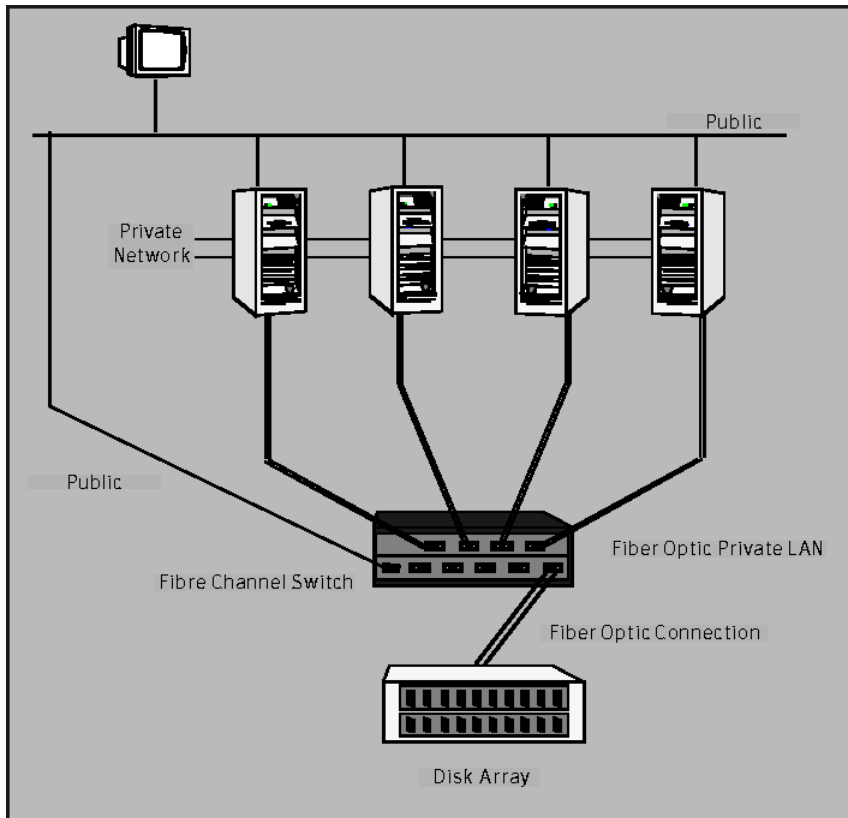
The Symantec VirtualStore is supported without I/O fencing enabled. However, without I/O fencing enabled, split brain scenarios can result in data corruption.

Hardware overview and requirements for Symantec VirtualStore

VxFS cluster functionality runs optimally on a Fibre Channel fabric. Fibre Channel technology provides the fastest, most reliable, and highest bandwidth connectivity currently available. By employing Fibre Channel technology, SVS can be used in conjunction with the latest Veritas Storage Area Network (SAN) applications to provide a complete data storage and retrieval solution.

Figure 3-1 shows the configuration of a cluster file system on a Fibre Channel fabric with a disk array.

Figure 3-1 Four Node SVS Cluster Built on Fibre Channel Fabric



Shared storage

Shared storage can be one or more shared disks or a disk array connected either directly to the nodes of the cluster or through a Fibre Channel Switch. Nodes can also have non-shared or local devices on a local I/O channel. It is advisable to have `/`, `/usr`, `/var` and other system partitions on local devices.

Fibre Channel switch

Each node in the cluster must have a Fibre Channel I/O channel to access shared storage devices. The primary component of the Fibre Channel fabric is the Fibre Channel switch.

Cluster platforms

There are several hardware platforms that can function as nodes in a Symantec VirtualStore (SVS) cluster.

See the *Symantec VirtualStore Release Notes*.

Note: For a cluster to work correctly, all nodes must have the same time. If you are not running the Network Time Protocol (NTP) daemon, make sure the time on all the systems comprising your cluster is synchronized.

Licensing Symantec VirtualStore

This chapter includes the following topics:

- [About Veritas product licensing](#)
- [Setting or changing the product level for keyless licensing](#)
- [Installing Veritas product license keys](#)

About Veritas product licensing

You have the option to install Veritas products without a license key. Installation without a license does not eliminate the need to obtain a license. A software license is a legal instrument governing the usage or redistribution of copyright protected software. The administrator and company representatives must ensure that a server or cluster is entitled to the license level for the products installed. Symantec reserves the right to ensure entitlement and compliance through auditing.

If you encounter problems while licensing this product, visit the Symantec licensing support website.

www.symantec.com/techsupp/

The Veritas product installer prompts you to select one of the following licensing methods:

- Install a license key for the product and features that you want to install.
When you purchase a Symantec product, you receive a License Key certificate. The certificate specifies the product keys and the number of product licenses purchased.
- Continue to install without a license key.

The installer prompts for the product modes and options that you want to install, and then sets the required product level.

Within 60 days of choosing this option, you must install a valid license key corresponding to the license level entitled. If you do not comply with the above terms, continuing to use the Symantec product is a violation of your end user license agreement, and results in warning messages.

For more information about keyless licensing, see the following URL:

<http://go.symantec.com/sfhakeyless>

If you upgrade to this release from a prior release of the Veritas software, the installer asks whether you want to upgrade the key to the new version. The existing license keys may not activate new features in this release.

If you upgrade with the product installer, or if you install or upgrade with a method other than the product installer, you must do one of the following to license the products:

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
See “[Setting or changing the product level for keyless licensing](#)” on page 58.
See the `vxkeyless (1m)` manual page.
- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.
See “[Installing Veritas product license keys](#)” on page 60.
See the `vxlicinst (1m)` manual page.

You can also use the above options to change the product levels to another level that you are authorized to use. For example, you can add the replication option to the installed product. You must ensure that you have the appropriate license for the product level and options in use.

Note: In order to change from one product group to another, you may need to perform additional steps.

Setting or changing the product level for keyless licensing

The keyless licensing method uses product levels to determine the Veritas products and functionality that are licensed.

For more information to use keyless licensing and to download the management server, see the following URL:

<http://go.symantec.com/vom>

When you set the product license level for the first time, you enable keyless licensing for that system. If you install with the product installer and select the keyless option, you are prompted to select the product and feature level that you want to license.

After you install, you can change product license levels at any time to reflect the products and functionality that you want to license. When you set a product level, you agree that you have the license for that functionality.

To set or change the product level

- 1 Change your current working directory:

```
# cd /opt/VRTSvlic/bin
```

- 2 View the current setting for the product level.

```
# ./vxkeyless -v display
```

- 3 View the possible settings for the product level.

```
# ./vxkeyless displayall
```

- 4 Set the desired product level.

```
# ./vxkeyless set prod_levels
```

where *prod_levels* is a comma-separated list of keywords. The keywords are the product levels as shown by the output of step 3.

If you want to remove keyless licensing and enter a key, you must clear the keyless licenses. Use the NONE keyword to clear all keys from the system.

Warning: Clearing the keys disables the Veritas products until you install a new key or set a new product level.

To clear the product license level

- 1 View the current setting for the product license level.

```
# ./vxkeyless [-v] display
```

- 2 If there are keyless licenses installed, remove all keyless licenses:

```
# ./vxkeyless [-q] set NONE
```

For more details on using the `vxkeyless` utility, see the `vxkeyless(1m)` manual page.

Installing Veritas product license keys

The `VRTSvlic` package enables product licensing. After the `VRTSvlic` is installed, the following commands and their manual pages are available on the system:

<code>vxlicinst</code>	Installs a license key for a Symantec product
<code>vxlicrep</code>	Displays currently installed licenses
<code>vxlictest</code>	Retrieves features and their descriptions encoded in a license key

Even though other products are included on the enclosed software discs, you can only use the Symantec software products for which you have purchased a license.

To install a new license

- ◆ Run the following commands. In a cluster environment, run the commands on each node in the cluster:

```
# cd /opt/VRTS/bin  
  
# ./vxlicinst -k license key
```

To see a list of your `vxkeyless` keys, enter the following command:

```
# ./vxkeyless display
```

After you upgrade from a previous release, the output you see when you run the `vxkeyless display` command includes the previous release's `vxkeyless` keys. Each `vxkeyless` key name includes the suffix `_<previous_release_version>`. For example, `DMP_6.0`, or `SFENT_VR_5.1SP1`, or `VCS_GCO_5.1`. During the upgrade process, the CPI installer prompts you to update the `vxkeyless` keys to the current release level. If you update the `vxkeyless` keys during the upgrade process, you no longer see the `_<previous_release_number>` suffix after the keys are updated.

Preinstallation tasks

- [Chapter 5. Preparing to install SVS](#)

Preparing to install SVS

This chapter includes the following topics:

- [Making the IPS publisher accessible](#)

Making the IPS publisher accessible

The installation of SVS 6.0.1 fails on Solaris 11 if the Image Packaging System (IPS) publisher is inaccessible. The following error message is displayed:

```
CPIERROR V-9-20-1273 Unable to contact configured publishers on <node_name>.
```

Solaris 11 introduces the new Image Packaging System (IPS) and sets a default publisher (solaris) during Solaris installation. When additional packages are being installed, the set publisher must be accessible for the installation to succeed. If the publisher is inaccessible, as in the case of a private network, then package installation will fail. The following commands can be used to display the set publishers:

```
# pkg publisher
```

Example:

```
root@sol11-03:~# pkg publisher
PUBLISHER      TYPE      STATUS  URI
solaris        origin   online  http://pkg.oracle.com/solaris/release/
root@sol11-03:~# pkg publisher solaris          Publisher: solaris
Alias:
Origin URI: http://pkg.oracle.com/solaris/release/
SSL Key: None
SSL Cert: None
Client UUID: 00000000-3f24-fe2e-0000-000068120608
Catalog Updated: October 09:53:00 PM
```

```
Enabled: Yes  
Signature Policy: verify
```

To make the IPS publisher accessible

- 1 Enter the following to disable the publisher (in this case, solaris):

```
# pkg set-publisher --disable solaris
```

- 2 Repeat the installation of SVS 6.0.1.

- 3 Re-enable the original publisher. If the publisher is still inaccessible (private network), then the `no-refresh` option can be used to re-enable it.

```
# pkg set-publisher --enable solaris
```

or

```
# pkg set-publisher --enable --no-refresh solaris
```

Note: Unsetting the publisher will have a similar effect, except that the publisher can only be re-set if it is accessible. See `pkg(1)` for further information on the `pkg` utility.

Installation using the script-based installer

- [Chapter 6. Installing Symantec VirtualStore using the script-based installer](#)
- [Chapter 7. Preparing to configure Symantec VirtualStore](#)
- [Chapter 8. Configuring Symantec VirtualStore](#)
- [Chapter 9. Configuring SVS for data integrity](#)

Installing Symantec VirtualStore using the script-based installer

This chapter includes the following topics:

- [Installing Symantec VirtualStore using the installer](#)
- [Configuring Symantec VirtualStore in secure mode](#)

Installing Symantec VirtualStore using the installer

The following walkthrough is to install Symantec VirtualStore on two systems: "host1" and "host2".

To install Symantec VirtualStore

- 1 To install on multiple systems, set up the systems so that commands between systems execute without prompting for passwords or confirmations.

Note: The `installer` program can configure both SSH and RSH communications.

See [“About configuring secure shell or remote shell communication modes before installing products”](#) on page 415.

- 2 Load and mount the software disc.
- 3 Move to the top-level directory on the disc.

```
# cd /cdrom/cdrom0
```

- 4 From this directory, type the following command to install on the local system. Also use this command to install on remote systems provided that the secure shell (ssh) or remote shell (rsh) utilities are configured:

```
# ./installer
```

- 5 Enter `I` to install and press Return.
- 6 When the list of available products appears, select Symantec VirtualStore (SVS). Enter the corresponding number, and press Return.
- 7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA).

```
Do you agree with the terms of the End User License Agreement as
specified in the
virtualstore/EULA/en/EULA_productname_Ux_version.pdf file present
on media? [y,n,q,?] y
```

- 8 Choose the mode you want to install:

```
1) Typical
2) Custom
```

```
Choose the mode you would like to install SVS: [1-2,q,?] (1)
```

If you chose the **Typical** install mode, the recommended packages will be installed by default. Skip to step [10](#).

If you chose the **Custom** install mode, proceed to step [9](#).

- 9 Select from one of the following installation options:
 - Minimal packages: installs only the basic functionality for the selected product.
 - Recommended packages: installs the full feature set without optional packages.
 - All packages: installs all available packages.
- 10 You are prompted to enter the system names (in the following example, "host1" and "host2") where you plan to install the software. Enter the system name or names and then press Return.

```
Enter the platform system names separated by spaces: host1 host2
```

where *platform* indicates the operating system.

- 11 You have the option to let the installer configure SSH or RSH communications between the systems. If you choose to allow this configuration, select the shell and provide the root passwords for each system.
- 12 After the system checks complete, the installer displays a list of the patches and packages that will be installed. For **Custom** install mode, press Enter to continue with the installation.
- 13 After installation completes, choose your licensing method.

To comply with the terms of Symantec's End User License Agreement, you have 60 days to either:

- * Enter a valid license key matching the functionality in use on the systems
- * Enable keyless licensing and manage the systems with a Management Server. For more details visit <http://go.symantec.com/sfhakeyless>. The product is fully functional during these 60 days.

- 1) Enter a valid license key
- 2) Enable keyless licensing and complete system licensing later

How would you like to license the systems? [1-2,q] (2)

If you have a valid license key, select 1 and enter the license key at the prompt. Skip to step 17.

To install using keyless licensing, select 2. You are prompted for the product modes and the options that you want to install and license.

Note: The keyless license option enables you to install without entering a key. However, you must still have a valid license to install and use Veritas products.

Keyless licensing requires that you manage the systems with a Management Server.

If you chose the **Custom** install mode, proceed to step 14.

If you chose the **Typical** install mode, the installer takes you directly to the configuration.

- 14 If you are going to use the Veritas Volume Replicator, enter **y** at the following prompt:

Would you like to enable Veritas Volume Replicator [y,n,q] (n) **y**

15 For typical install mode, SVS is automatically configured and started.

16 At the prompt, specify whether you want to send your installation information to Symantec.

```
Would you like to send the information about this installation
to Symantec to help improve installation in the future? [y,n,q,?]
y
```

17 View the log file, if needed, to confirm the installation.

Installation log files, summary file, and response file are saved at:

```
/opt/VRTS/install/logs/installer-****
```

Configuring Symantec VirtualStore in secure mode

Configuring SVS in secure mode ensures that all the communication between the systems is encrypted and users are verified against security credentials. SVS user names and passwords are not used when a cluster is running in secure mode. You can select the secure mode to be FIPS compliant while configuring the secure mode.

To configure SVS in secure mode

1 Enter appropriate choices when the installer prompts you:

```
Would you like to configure the VCS cluster in
secure mode [y,n,q] (n) y
1. Configure the cluster in secure mode without FIPS
2. Configure the cluster in secure mode with FIPS
3. Back to previous menu
Select the option you would like to perform [1-2,b,q] (1) 2
```

2 To verify the cluster is in secure mode after configuration, run the command:

```
# haclus -<value> SecureClus
```

The command returns 1 if cluster is in secure mode, else returns 0.

Preparing to configure Symantec VirtualStore

This chapter includes the following topics:

- [About planning to configure I/O fencing](#)
- [Setting up the CP server](#)

About planning to configure I/O fencing

After you configure SVS with the installer, you must configure I/O fencing in the cluster for data integrity.

You can configure disk-based I/O fencing or server-based I/O fencing. If your enterprise setup has multiple clusters that use VCS for clustering, Symantec recommends you to configure server-based I/O fencing.

The coordination points in server-based fencing can include only CP servers or a mix of CP servers and coordinator disks. Symantec also supports server-based fencing with a single coordination point which is a single highly available CP server that is hosted on an SFHA cluster.

Warning: For server-based fencing configurations that use a single coordination point (CP server), the coordination point becomes a single point of failure. In such configurations, the arbitration facility is not available during a failover of the CP server in the SFHA cluster. So, if a network partition occurs on any application cluster during the CP server failover, the application cluster is brought down. Symantec recommends the use of single CP server-based fencing only in test environments.

If you have installed Symantec VirtualStore in a virtual environment that is not SCSI-3 PR compliant, you can configure non-SCSI-3 server-based fencing.

See [Figure 7-2](#) on page 74.

[Figure 7-1](#) illustrates a high-level flowchart to configure I/O fencing for the Symantec VirtualStore cluster.

Figure 7-1 Workflow to configure I/O fencing

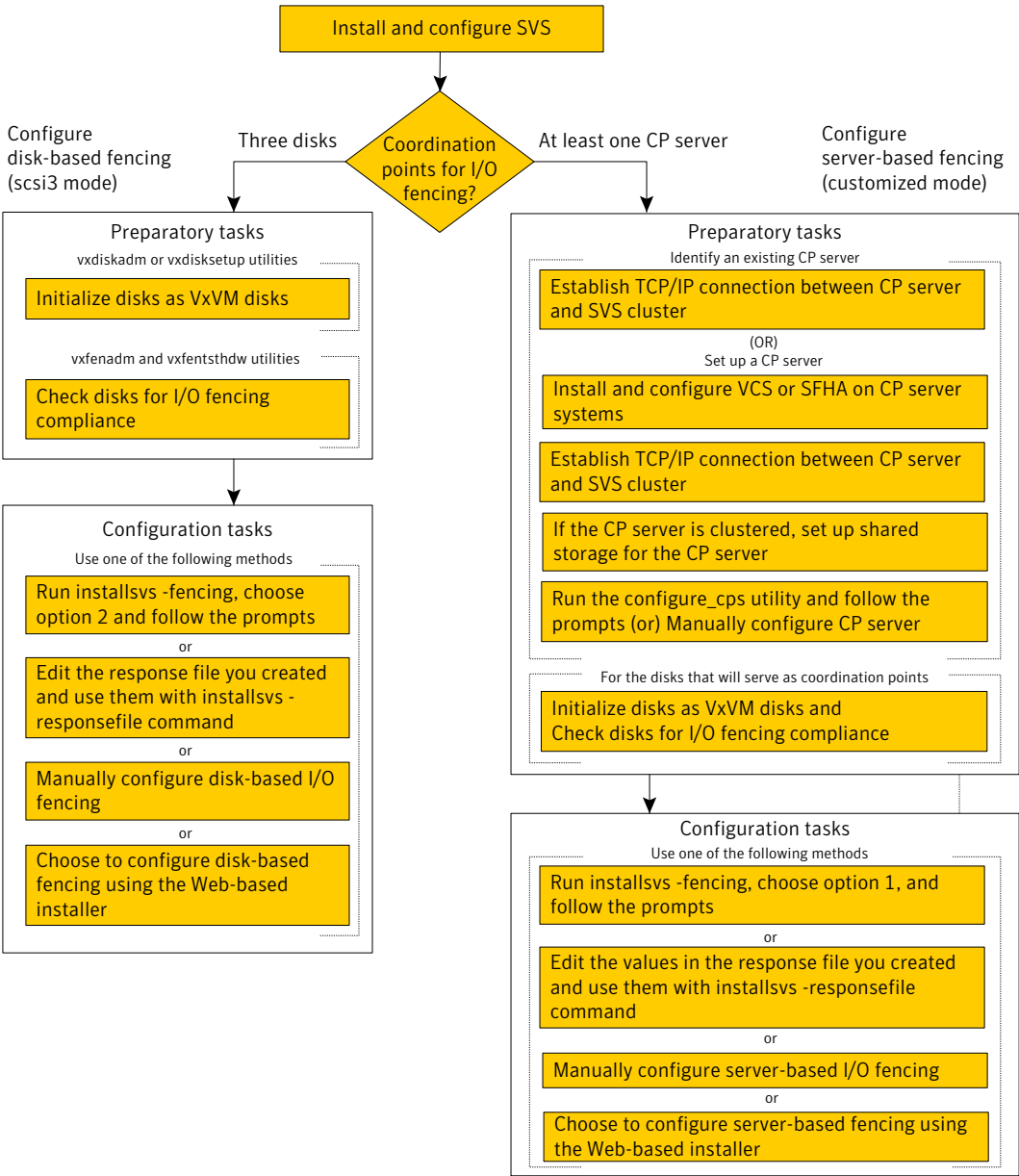
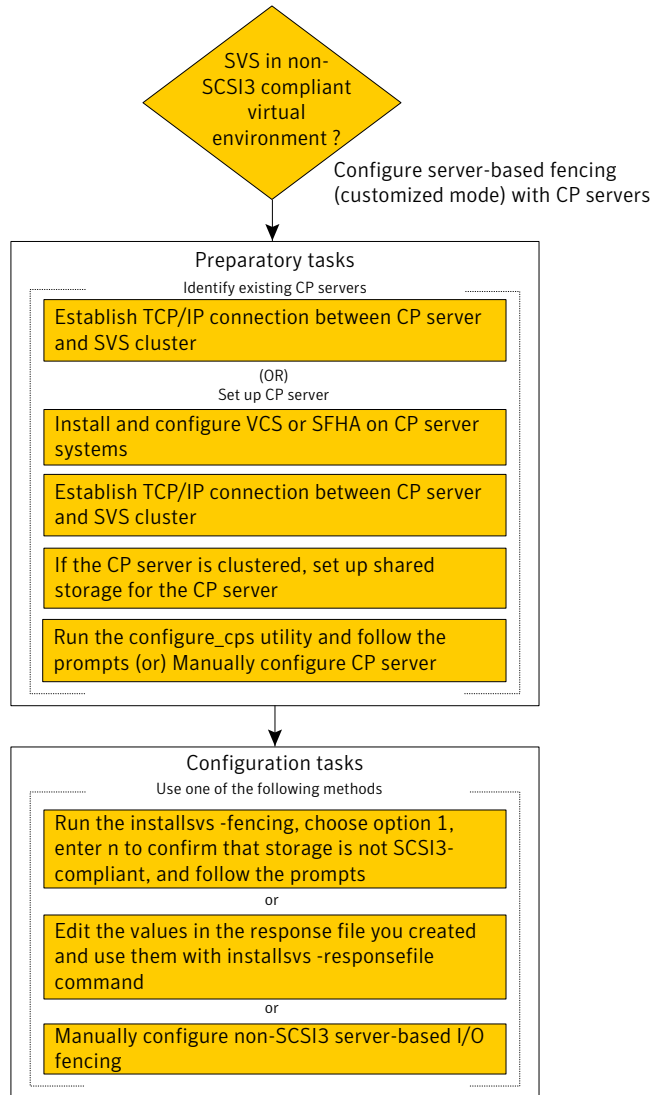


Figure 7-2 illustrates a high-level flowchart to configure non-SCSI-3 server-based I/O fencing for the Symantec VirtualStore cluster in virtual environments that do not support SCSI-3 PR.

Figure 7-2 Workflow to configure non-SCSI-3 server-based I/O fencing



After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:

Using the installsvs	See “Setting up disk-based I/O fencing using installsvs” on page 123. See “Setting up server-based I/O fencing using installsvs” on page 137. See “Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsvs” on page 146.
Using the Web-based installer	See “Configuring Symantec VirtualStore for data integrity using the Web-based installer” on page 182.
Using response files	See “Response file variables to configure disk-based I/O fencing” on page 208. See “Response file variables to configure server-based I/O fencing” on page 211. See “Response file variables to configure non-SCSI-3 server-based I/O fencing” on page 213. See “Configuring I/O fencing using response files” on page 207.
Manually editing configuration files	See “Setting up disk-based I/O fencing manually” on page 132. See “Setting up server-based I/O fencing manually” on page 148. See “Setting up non-SCSI-3 fencing in virtual environments manually” on page 160.

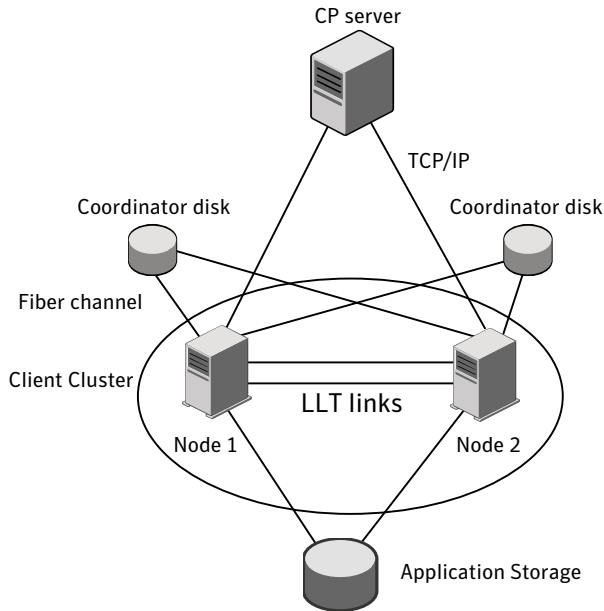
You can also migrate from one I/O fencing configuration to another.

See the *Veritas Storage foundation High Availability Administrator's Guide* for more details.

Typical SVS cluster configuration with server-based I/O fencing

[Figure 7-3](#) displays a configuration using a SVS cluster (with two nodes), a single CP server, and two coordinator disks. The nodes within the SVS cluster are connected to and communicate with each other using LLT links.

Figure 7-3 CP server, SVS cluster, and coordinator disks



Recommended CP server configurations

Following are the recommended CP server configurations:

- Multiple application clusters use three CP servers as their coordination points
See [Figure 7-4](#) on page 77.
- Multiple application clusters use a single CP server and single or multiple pairs of coordinator disks (two) as their coordination points
See [Figure 7-5](#) on page 78.
- Multiple application clusters use a single CP server as their coordination point
This single coordination point fencing configuration must use a highly available CP server that is configured on an SFHA cluster as its coordination point.
See [Figure 7-6](#) on page 78.

Warning: In a single CP server fencing configuration, arbitration facility is not available during a failover of the CP server in the SFHA cluster. So, if a network partition occurs on any application cluster during the CP server failover, the application cluster is brought down.

Although the recommended CP server configurations use three coordination points, you can use more than three coordination points for I/O fencing. Ensure that the total number of coordination points you use is an odd number. In a configuration where multiple application clusters share a common set of CP server coordination points, the application cluster as well as the CP server use a Universally Unique Identifier (UUID) to uniquely identify an application cluster.

Figure 7-4 displays a configuration using three CP servers that are connected to multiple application clusters.

Figure 7-4 Three CP servers connecting to multiple application clusters

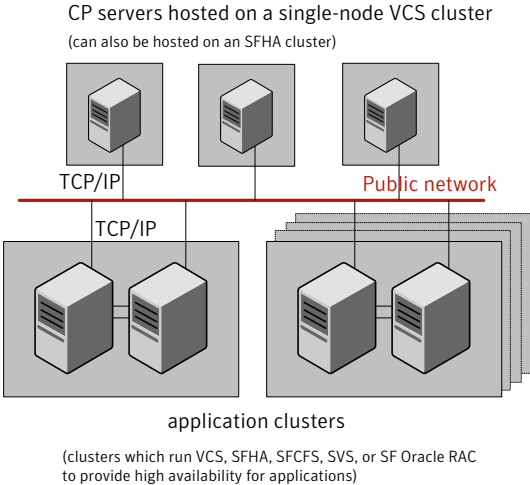


Figure 7-5 displays a configuration using a single CP server that is connected to multiple application clusters with each application cluster also using two coordinator disks.

Figure 7-5 Single CP server with two coordinator disks for each application cluster

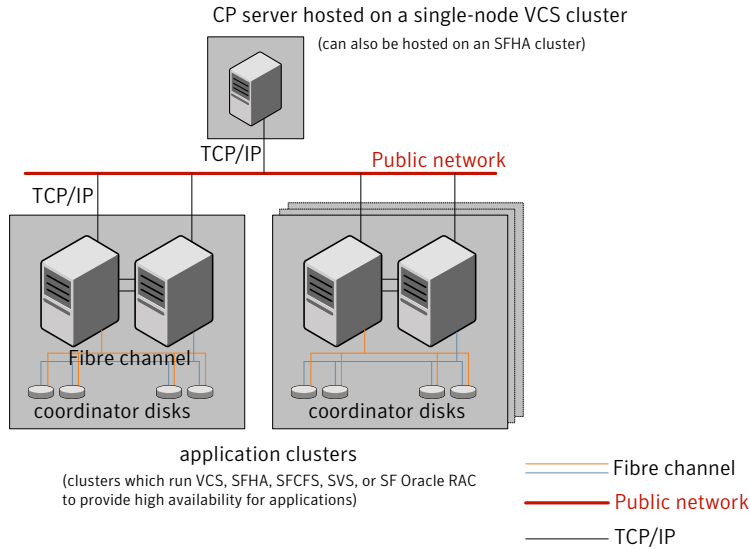
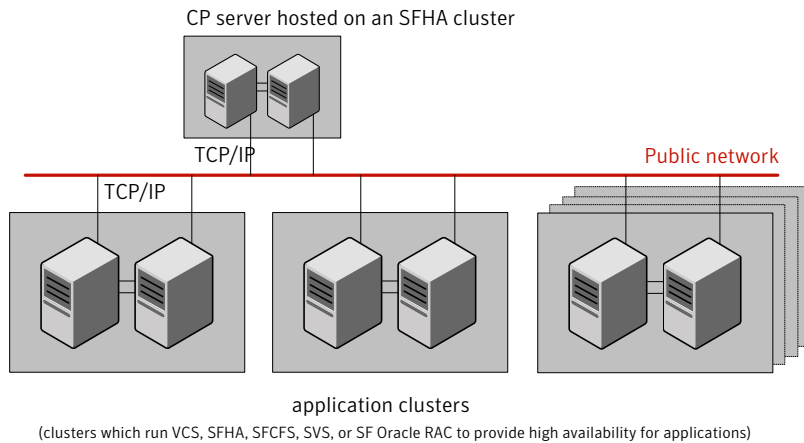


Figure 7-6 displays a configuration using a single CP server that is connected to multiple application clusters.

Figure 7-6 Single CP server connecting to multiple application clusters



See "Configuration diagrams for setting up server-based I/O fencing" on page 433.

Setting up the CP server

Table 7-1 lists the tasks to set up the CP server for server-based I/O fencing.

Table 7-1 Tasks to set up CP server for server-based I/O fencing

Task	Reference
Plan your CP server setup	See “Planning your CP server setup” on page 79.
Install the CP server	See “Installing the CP server using the installer” on page 80.
Configure the CP server cluster in secure mode	See “Configuring the CP server cluster in secure mode” on page 81.
Set up shared storage for the CP server database	See “Setting up shared storage for the CP server database” on page 82.
Configure the CP server	See “Configuring the CP server using the installer program” on page 83. See “Configuring the CP server using the Web-based installer” on page 93. See “Configuring the CP server manually” on page 94. See “Configuring CP server using response files” on page 95.
Verify the CP server configuration	See “Verifying the CP server configuration” on page 99.

Planning your CP server setup

Follow the planning instructions to set up CP server for server-based I/O fencing.

To plan your CP server setup

- 1 Decide whether you want to host the CP server on a single-node VCS cluster, or on an SFHA cluster.
Symantec recommends hosting the CP server on an SFHA cluster to make the CP server highly available.
- 2 If you host the CP server on an SFHA cluster, review the following information. Make sure you make the decisions and meet these prerequisites when you set up the CP server:

- You must set up shared storage for the CP server database during your CP server setup.
 - Decide whether you want to configure server-based fencing for the SVS cluster (application cluster) with a single CP server as coordination point or with at least three coordination points.
Symantec recommends using at least three coordination points.
- 3 Decide whether you want to configure the CP server cluster in secure mode.
Symantec recommends configuring the CP server cluster in secure mode to secure the communication between the CP server and its clients (SVS clusters). It also secures the HAD communication on the CP server cluster.
 - 4 Set up the hardware and network for your CP server.
See “[CP server requirements](#)” on page 31.
 - 5 Have the following information handy for CP server configuration:
 - Name for the CP server
The CP server name should not contain any special characters. CP server name can include alphanumeric characters, underscore, and hyphen.
 - Port number for the CP server
Allocate a TCP/IP port for use by the CP server.
Valid port range is between 49152 and 65535. The default port number is 14250.
 - Virtual IP address, network interface, netmask, and networkhosts for the CP server
You can configure multiple virtual IP addresses for the CP server.

Installing the CP server using the installer

Perform the following procedure to install and configure VCS or SFHA on CP server systems.

To install and configure VCS or SFHA on the CP server systems

- ◆ Depending on whether your CP server uses a single system or multiple systems, perform the following tasks:

CP server setup uses a single system	<p>Install and configure VCS to create a single-node VCS cluster.</p> <p>During installation, make sure to select all packages for installation. The VRTScps package is installed only if you select to install all packages.</p> <p>See the <i>Veritas Cluster Server Installation Guide</i> for instructions on installing and configuring VCS.</p> <p>Proceed to configure the CP server.</p> <p>See “Configuring the CP server using the installer program” on page 83.</p> <p>See “Configuring the CP server manually” on page 94.</p>
CP server setup uses multiple systems	<p>Install and configure SFHA to create an SFHA cluster. This makes the CP server highly available.</p> <p>Meet the following requirements for CP server:</p> <ul style="list-style-type: none"> ■ During installation, make sure to select all packages for installation. The VRTScps package is installed only if you select to install all packages. ■ During configuration, configure disk-based fencing (scsi3 mode). <p>See the <i>Veritas Storage Foundation and High Availability Installation Guide</i> for instructions on installing and configuring SFHA.</p> <p>Proceed to set up shared storage for the CP server database.</p>

Configuring the CP server cluster in secure mode

You must configure security on the CP server only if you want to secure the communication between the CP server and the SVS cluster (CP client).

This step secures the HAD communication on the CP server cluster.

Note: If you already configured the CP server cluster in secure mode during the VCS configuration, then skip this section.

To configure the CP server cluster in secure mode

- ◆ Run the installer as follows to configure the CP server cluster in secure mode.

If you have VCS installed on the CP server, run the following command:

```
# /opt/VRTS/install/installvcs<version> -security
```

Where *<version>* is the specific release version.

See “[About the Veritas installer](#)” on page 41.

If you have SFHA installed on the CP server, run the following command:

```
# /opt/VRTS/install/installsfha<version> -security
```

Where *<version>* is the specific release version.

See “[About the Veritas installer](#)” on page 41.

Setting up shared storage for the CP server database

If you configured SFHA on the CP server cluster, perform the following procedure to set up shared storage for the CP server database.

Symantec recommends that you create a mirrored volume for the CP server database and that you use the VxFS file system type.

To set up shared storage for the CP server database

- 1 Create a disk group containing the disks. You require two disks to create a mirrored volume.

For example:

```
# vxdg init cps_dg disk1 disk2
```

- 2 Create a mirrored volume over the disk group.

For example:

```
# vxassist -g cps_dg make cps_vol volume_size layout=mirror
```

- 3 Create a file system over the volume.

The CP server configuration utility only supports vxfs file system type. If you use an alternate file system, then you must configure CP server manually.

Depending on the operating system that your CP server runs, enter the following command:

```
AIX # mkfs -V vxfs /dev/vx/rdsk/cps_dg/cps_volume
```

```
HP-UX # mkfs -F vxfs /dev/vx/rdsk/cps_dg/cps_volume
```

```
Linux # mkfs -t vxfs /dev/vx/rdsk/cps_dg/cps_volume
```

```
Solaris # mkfs -F vxfs /dev/vx/rdsk/cps_dg/cps_volume
```

Configuring the CP server using the installer program

Use the `configcps` option available in the installer program to configure the CP server.

Perform one of the following procedures:

For CP servers on single-node VCS cluster: See [“To configure the CP server on a single-node VCS cluster”](#) on page 84.

For CP servers on an SFHA cluster: See [“To configure the CP server on an SFHA cluster”](#) on page 88.

To configure the CP server on a single-node VCS cluster

- 1 Verify that the `VRTScps` package is installed on the node.
- 2 Run the `installvcs<version>` program with the `configcps` option.

```
# /opt/VRTS/install/installvcs<version> -configcps
```

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

- 3 Installer checks the cluster information and prompts if you want to configure CP Server on the cluster.

Enter `y` to confirm.

- 4 Select an option based on how you want to configure Coordination Point server.

```
1) Configure Coordination Point Server on single node VCS system
2) Configure Coordination Point Server on SFHA cluster
3) Unconfigure Coordination Point Server
```

- 5 Enter the option: `[1-3,q] 1`.

The installer then runs the following preconfiguration checks:

- Checks to see if a single-node VCS cluster is running with the supported platform.

The CP server requires VCS to be installed and configured before its configuration.

- Checks to see if the CP server is already configured on the system.

If the CP server is already configured, then the installer informs the user and requests that the user unconfigure the CP server before trying to configure it.

- 6 Enter the name of the CP Server.

```
Enter the name of the CP Server: [b] mycpserver1
```

- 7 Enter valid virtual IP addresses for the CP Server. A CP Server can be configured with more than one virtual IP address. You can also use IPv6 address.

Enter valid IP addresses for Virtual IPs for the CP Server, separated by space [b] **10.200.58.231 10.200.58.232**

Note: Ensure that the virtual IP address of the CP server and the IP address of the NIC interface on the CP server belongs to the same subnet of the IP network. This is required for communication to happen between client nodes and CP server.

- 8 Enter the corresponding CP server port number for each virtual IP address or press Enter to accept the default value (14250).

Enter corresponding port number for each Virtual IP address in the range [49152, 65535], separated by space, or simply accept the default port suggested: [b] **(14250) 65535**

- 9 Choose whether the communication between the CP server and the VCS clusters has to be made secure. If you have not configured the CP server cluster in secure mode, enter **n** at the prompt.

Warning: If the CP server cluster is not configured in secure mode, and if you enter **y**, then the script immediately exits. You must configure the CP server cluster in secure mode and rerun the CP server configuration script.

Symantec recommends secure communication between the CP server and application clusters. Enabling security requires Symantec Product Authentication Service to be installed and configured on the cluster. Do you want to enable Security for the communications? [y,n,q,b] (y) **n**

- 10 Enter the absolute path of the CP server database or press **Enter** to accept the default value (/etc/VRTScps/db).

Enter absolute path of the database: [b] **(/etc/VRTScps/db)**

11 Verify and confirm the CP server configuration information.

```
CP Server configuration verification:
-----
CP Server Name: mycpserver1
CP Server Virtual IP(s): 10.200.58.231, 10.200.58.232
CP Server Port(s): 65535, 14250
CP Server Security: 0
CP Server Database Dir: /etc/VRTScps/db
-----
```

Is this information correct? [y,n,q,?] (y)

12 The installer proceeds with the configuration process, and creates a vxcps.conf configuration file.

```
Successfully generated the /etc/vxcps.conf configuration file
Successfully created directory /etc/VRTScps/db on node
```

13 Configure the CP Server Service Group (CPSSG) for this cluster.

```
Enter the number of NIC resources that you want to configure.
You must use a public NIC.
Enter how many NIC resources you want to configure (1 to 2): 2
```

Answer the following questions for each NIC resource that you want to configure.

14 Enter a valid network interface for the virtual IP address for the CP server process.

```
Enter a valid network interface on sol92216 for NIC resource - 1: e1000g0
Enter a valid network interface on sol92216 for NIC resource - 2: e1000g1
```

15 Enter the NIC resource you want to associate with the virtual IP addresses.

```
Enter the NIC resource you want to associate with the virtual IP 10.200.58.231 (1 to 2): 1
Enter the NIC resource you want to associate with the virtual IP 10.200.58.232 (1 to 2): 2
```

16 Enter the networkhosts information for each NIC resource.

Symantec recommends configuring NetworkHosts attribute to ensure NIC resource to be always online

```
Do you want to add NetworkHosts attribute for the NIC device e1000g0
on system sol92216? [y,n,q] y
Enter a valid IP address to configure NetworkHosts for NIC e1000g0
on system sol92216: 10.200.56.22
```

```
Do you want to add another Network Host? [y,n,q] n
```

17 Enter the netmask for virtual IP addresses. If you entered an IPv6 address, enter the prefix details at the prompt.

```
Enter the netmask for virtual IP 10.200.58.231: (255.255.252.0)
Enter the netmask for virtual IP 10.200.58.232: (255.255.252.0)
```

18 Installer displays the status of the Coordination Point Server configuration. After the configuration process has completed, a success message appears.

```
For example:
Updating main.cf with CPSSG service group.. Done
Successfully added the CPSSG service group to VCS configuration.
Trying to bring CPSSG service group
ONLINE and will wait for upto 120 seconds
```

```
The Veritas Coordination Point Server is ONLINE
```

```
The Veritas Coordination Point Server has been
configured on your system.
```

19 Run the hagr -state command to ensure that the CPSSG service group has been added.

```
For example:
# hagr -state CPSSG
#Group Attribute System Value
CPSSG State.... |ONLINE|
```

It also generates the configuration file for CP server (/etc/vxcps.conf). The vxcpserv process and other resources are added to the VCS configuration in the CP server service group (CPSSG).

For information about the CPSSG, refer to the *Veritas Cluster Server Administrator's Guide*.

To configure the CP server on an SFHA cluster

- 1 Verify that the `VRTScps` package is installed on each node.
- 2 Ensure that you have configured passwordless ssh or rsh on the CP server cluster nodes.
- 3 Run the `installsfha<version>` program with the `configcps` option.

```
# ./installsfha<version> -configcps
```

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

- 4 Installer checks the cluster information and prompts if you want to configure CP Server on the cluster.

Enter `y` to confirm.

- 5 Select an option based on how you want to configure Coordination Point server.

```
1) Configure Coordination Point Server on single node VCS system
2) Configure Coordination Point Server on SFHA cluster
3) Unconfigure Coordination Point Server
```

- 6 Enter `2` at the prompt to configure CP server on an SFHA cluster.

The installer then runs the following preconfiguration checks:

- Checks to see if an SFHA cluster is running with the supported platform. The CP server requires SFHA to be installed and configured before its configuration.
- Checks to see if the CP server is already configured on the system. If the CP server is already configured, then the installer informs the user and requests that the user unconfigure the CP server before trying to configure it.

- 7 Enter the name of the CP server.

```
Enter the name of the CP Server: [b] cps1
```


- 8** Enter valid virtual IP addresses for the CP Server. A CP Server can be configured with more than one virtual IP address. You can also use IPv6 address.

Enter valid IP addresses for Virtual IPs for the CP Server, separated by space [b] **10.200.58.231 10.200.58.232**

- 9** Enter the corresponding CP server port number for each virtual IP address or press Enter to accept the default value (14250).

Enter corresponding port number for each Virtual IP address in the range [49152, 65535], separated by space, or simply accept the default port suggested: [b] **(14250) 65535**

- 10** Choose whether the communication between the CP server and the VCS clusters has to be made secure. If you have not configured the CP server cluster in secure mode, enter **n** at the prompt.

Warning: If the CP server cluster is not configured in secure mode, and if you enter **y**, then the script immediately exits. You must configure the CP server cluster in secure mode and rerun the CP server configuration script.

Symantec recommends secure communication between the CP server and application clusters. Enabling security requires Symantec Product Authentication Service to be installed and configured on the cluster.

Do you want to enable Security for the communications? [y,n,q,b] **(y)**

- 11** Enter absolute path of the database.

CP Server uses an internal database to store the client information. As the CP Server is being configured on SFHA cluster, the database should reside on shared storage with vxfs file system. Please refer to documentation for information on setting up of shared storage for CP server database.

Enter absolute path of the database: [b] **/cpsdb**

12 Verify and confirm the CP server configuration information.

CP Server configuration verification:

```
CP Server Name: cps1
CP Server Virtual IP(s): 10.200.58.231, 10.200.58.232
CP Server Port(s): 65535, 14250
CP Server Security: 1
CP Server Database Dir: /cpsdb
```

Is this information correct? [y,n,q,?] **(y)**

13 The installer proceeds with the configuration process, and creates a vxcps.conf configuration file.

```
Successfully generated the /etc/vxcps.conf configuration file
Copying configuration file /etc/vxcps.conf to sys0...Done
Creating mount point /cps_mount_data on sys0. ... Done
Copying configuration file /etc/vxcps.conf to sys0. ... Done
Press Enter to continue.
```

14 Configure CP Server Service Group (CPSSG) for this cluster.

Enter the number of NIC resources that you want to configure. You must use a public NIC.

Enter how many NIC resources you want to configure (1 to 2): **2**

Answer the following questions for each NIC resource that you want to configure.

15 Enter a valid network interface for the virtual IP address for the CP server process.

Enter a valid network interface on sol92216 for NIC resource - 1: e1000g0

Enter a valid network interface on sol92216 for NIC resource - 2: e1000g1

16 Enter the NIC resource you want to associate with the virtual IP addresses.

Enter the NIC resource you want to associate with the virtual IP 10.200.58.231 (1 to 2): 1

Enter the NIC resource you want to associate with the virtual IP 10.200.58.232 (1 to 2): 2

17 Enter the networkhosts information for each NIC resource.

Symantec recommends configuring NetworkHosts attribute to ensure NIC resource to be always online

```
Do you want to add NetworkHosts attribute for the NIC device e1000g0
on system sol92216? [y,n,q] y
Enter a valid IP address to configure NetworkHosts for NIC e1000g0
on system sol92216: 10.200.56.22
```

```
Do you want to add another Network Host? [y,n,q] n
Do you want to apply the same NetworkHosts for all systems? [y,n,q] (y)
```

18 Enter the netmask for virtual IP addresses. If you entered an IPv6 address, enter the prefix details at the prompt.

```
Enter the netmask for virtual IP 10.200.58.231: (255.255.252.0)
Enter the netmask for virtual IP 10.200.58.232: (255.255.252.0)
```

19 Configure a disk group for CP server database. You can choose an existing disk group or create a new disk group.

Symantec recommends to use the disk group that has at least two disks on which mirrored volume can be created.
 Select one of the options below for CP Server database disk group:

- 1) Create a new disk group
- 2) Using an existing disk group

```
Enter the choice for a disk group: [1-2,q] 2
```

20 Select one disk group as the CP Server database disk group.

```
Select one disk group as CP Server database disk group: [1-3,q] 3
1) mycpsdg
2) cpsdgl
3) newcpsdg
```

21 Select the CP Server database volume.

You can choose to use an existing volume or create new volume for CP Server database. If you chose newly created disk group, you can only choose to create new volume for CP Server database.

Select one of the options below for CP Server database volume:

- 1) Create a new volume on disk group newcpsdg
- 2) Using an existing volume on disk group newcpsdg

22 Enter the choice for a volume: [1-2,q] **2**.

23 Select one volume as CP Server database volume [1-1,q] **1**

- 1) newcpsvol

24 After the VCS configuration files are updated, a success message appears.

For example:

```
Updating main.cf with CPSSG service group .... Done
Successfully added the CPSSG service group to VCS configuration.
```

25 If the cluster is secure, installer creates the softlink /var/VRTSvc/vcsauth/data/CPSEVER to /cpsdb/CPSEVER and check if credentials are already present at /cpsdb/CPSEVER. If not, installer creates credentials in the directory, otherwise, installer asks if you want to reuse existing credentials.

Do you want to reuse these credentials? [y,n,q] **(y)**

26 After the configuration process has completed, a success message appears.

For example:

```
Trying to bring CPSSG service group ONLINE and will wait for upto 120 seconds
The Veritas Coordination Point Server is ONLINE
The Veritas Coordination Point Server has been configured on your system.
```

27 Run the `hagrp -state` command to ensure that the CPSSG service group has been added.

For example:

```
# hagrp -state CPSSG
#Group Attribute System Value
CPSSG State cps1 |ONLINE|
CPSSG State cps2 |OFFLINE|
```

It also generates the configuration file for CP server (`/etc/vxcps.conf`). The `vxcpserv` process and other resources are added to the VCS configuration in the CP server service group (CPSSG).

For information about the CPSSG, refer to the *Veritas Cluster Server Administrator's Guide*.

Configuring the CP server using the Web-based installer

Perform the following steps to configure the CP server using the Web-based installer.

To configure Symantec VirtualStore on a cluster

- 1 Start the Web-based installer.
See [“Starting the Veritas Web-based installer”](#) on page 172.
- 2 On the Select a task and a product page, select the task and the product as follows:

Task	I/O fencing configuration
Product	Symantec VirtualStore

Click **Next**.

- 3 On the Select Cluster page, enter the system names where you want to configure Symantec VirtualStore and click **Next**.

- 4 In the Confirmation dialog box, verify cluster information is correct and choose whether or not to configure I/O fencing.
 - To configure I/O fencing, click **Yes**.
 - To configure I/O fencing later, click **No**.
- 5 On the Select Option page, select Configure CP Server on VCS and click **Next**.
- 6 On the Configure CP Server page, provide CP server information, such as, name, virtual IPs, port numbers, and absolute path of the database to store the configuration details.
Click **Next**.
- 7 Configure the CP Server Service Group (CPSSG), select the number of NIC resources, and associate NIC resources to virtual IPs that are going to be used to configure the CP Server.
Click **Next**.
- 8 Configure network hosts for the CP server.
Click **Next**.
- 9 Configure disk group for the CP server.
Click **Next**.

Note: This step is not applicable for a single node cluster.

- 10 Configure volume for the disk group associated to the CP server.
Click **Next**.

Note: This step is not applicable for a single node cluster.

- 11 Click **Finish** to complete configuring the CP server.

Configuring the CP server manually

Perform the following steps to manually configure the CP server.

To manually configure the CP server

- 1 Stop VCS on each node in the CP server cluster using the following command:

```
# hstop -local
```

- 2 Edit the `main.cf` file to add the CPSSG service group on any node. Use the CPSSG service group in the sample `main.cf` as an example:

Customize the resources under the CPSSG service group as per your configuration.

- 3 Verify the `main.cf` file using the following command:

```
# hacf -verify /etc/VRTSvcs/conf/config
```

If successfully verified, copy this `main.cf` to all other cluster nodes.

- 4 Create the `/etc/vxcps.conf` file using the sample configuration file provided at `/etc/vxcps/vxcps.conf.sample`.

Based on whether you have configured the CP server cluster in secure mode or not, do the following:

- For a CP server cluster which is configured in secure mode, edit the `/etc/vxcps.conf` file to set `security=1`.
- For a CP server cluster which is not configured in secure mode, edit the `/etc/vxcps.conf` file to set `security=0`.

Symantec recommends enabling security for communication between CP server and the application clusters.

- 5 Start VCS on all the cluster nodes.

```
# hstart
```

- 6 Verify that the CP server service group (CPSSG) is online.

```
# hagr -state CPSSG
```

Output similar to the following appears:

```
# Group Attribute System Value
CPSSG State cps1.symantecexample.com |ONLINE|
```

Configuring CP server using response files

You can configure a CP server using a generated responsefile.

On a single node VCS cluster:

- ◆ Run the `installvcs<version>` command with the `responsefile` option to configure the CP server on a single node VCS cluster.

```
# /opt/VRTS/install/installvcs<version> -responsefile
'/tmp/sample1.res'
```

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

On a SFHA cluster:

- ◆ Run the `installsfha<version>` command with the `responsefile` option to configure the CP server on a SFHA cluster.

```
# /opt/VRTS/install/installsfha<version> -responsefile
'/tmp/sample1.res'
```

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

Response file variables to configure CP server

[Table 7-2](#)

Table 7-2 describes response file variables to configure CP server

Variable	List or Scalar	Description
CFG{opt}{configcps}	Scalar	This variable performs CP server configuration task
CFG{cps_singlenode_config}	Scalar	This variable describes if the CP server will be configured on a singlenode VCS cluster
CFG{cps_sfha_config}	Scalar	This variable describes if the CP server will be configured on a SFHA cluster
CFG{cps_unconfig}	Scalar	This variable describes if the CP server will be unconfigured
CFG{cpsname}	Scalar	This variable describes the name of the CP server
CFG{cps_db_dir}	Scalar	This variable describes the absolute path of CP server database

Table 7-2 describes response file variables to configure CP server (*continued*)

Variable	List or Scalar	Description
CFG{cps_security}	Scalar	This variable describes if security is configured for the CP server
CFG{cps_reuse_cred}	Scalar	This variable describes if reusing the existing credentials for the CP server
CFG{cps_vips}	List	This variable describes the virtual IP addresses for the CP server
CFG{cps_ports}	List	This variable describes the port number for the virtual IP addresses for the CP server
CFG{cps_nic_list}{cpsvip<n>}	List	This variable describes the NICs of the systems for the virtual IP address
CFG{cps_netmasks}	List	This variable describes the netmasks for the virtual IP addresses
CFG{cps_prefix_length}	List	This variable describes the prefix length for the virtual IP addresses
CFG{cps_network_hosts}{cpsnic<n>}	List	This variable describes the network hosts for the NIC resource
CFG{cps_vip2nicres_map}{<vip>}	Scalar	This variable describes the NIC resource to associate with the virtual IP address
CFG{cps_diskgroup}	Scalar	This variable describes the disk group for the CP server database
CFG{cps_volume}	Scalar	This variable describes the volume for the CP server database
CFG{cps_newdg_disks}	List	This variable describes the disks to be used to create a new disk group for the CP server database
CFG{cps_newvol_volsize}	Scalar	This variable describes the volume size to create a new volume for the CP server database
CFG{cps_delete_database}	Scalar	This variable describes if deleting the database of the CP server during the unconfiguration

Table 7-2 describes response file variables to configure CP server (*continued*)

Variable	List or Scalar	Description
CFG{cps_delete_config_log}	Scalar	This variable describes if deleting the config files and log files of the CP server during the unconfiguration

Sample response file for configuring the CP server on single node VCS cluster

Review the response file variables and their definitions.

See [Table 7-2](#) on page 96.

```
#
# Configuration Values:
#
our %CFG;

$CFG{cps_db_dir}="/etc/VRTScps/db";
$CFG{cps_netmasks}=[ qw(255.255.252.0) ];
$CFG{cps_network_hosts}{cpsnic1}=[ qw(10.200.56.22) ];
$CFG{cps_nic_list}{cpsvip1}=[ qw(e1000g0) ];
$CFG{cps_ports}=[ qw(14250) ];
$CFG{cps_security}=0;
$CFG{cps_singlenode_config}=1;
$CFG{cps_vip2nicres_map}{"10.200.58.233"}=1;
$CFG{cps_vips}=[ qw(10.200.58.233) ];
$CFG{cpsname}="cps1";
$CFG{opt}{configcps}=1;
$CFG{opt}{configure}=1;
$CFG{prod}="VCS601";
$CFG{systems}=[ qw(cps1) ];
$CFG{vcs_clusterid}=18523;
$CFG{vcs_clustername}="vcs92216";

1;
```

Sample response file for configuring the CP server on SFHA cluster

Review the response file variables and their definitions.

See [Table 7-2](#) on page 96.

```
#
# Configuration Values:
#
our %CFG;

$CFG{cps_db_dir}="/cpsdb";
$CFG{cps_diskgroup}="mycpsdg";
$CFG{cps_netmasks}=[ qw(255.255.252.0 255.255.252.0) ];
$CFG{cps_network_hosts}{cpsnic1}=[ qw(10.200.56.22) ];
$CFG{cps_network_hosts}{cpsnic2}=[ qw(10.200.56.22) ];
$CFG{cps_nic_list}{cpsvip1}=[ qw( e1000g0 e1000g1) ];
$CFG{cps_nic_list}{cpsvip2}=[ qw( e1000g0 e1000g1) ];
$CFG{cps_ports}=[ qw(65533 14250) ];
$CFG{cps_security}=1;
$CFG{cps_fips_mode}=0;
$CFG{cps_sfha_config}=1;
$CFG{cps_vip2nicres_map}{"10.200.58.231"}=1;
$CFG{cps_vip2nicres_map}{"10.200.58.232"}=2;
$CFG{cps_vips}=[ qw(10.200.58.231 10.200.58.232) ];
$CFG{cps_volume}="mycpsvol";
$CFG{cpsname}="cps1";
$CFG{opt}{configcps}=1;
$CFG{opt}{configure}=1;
$CFG{prod}="SFHA601";
$CFG{systems}=[ qw(cps1 cps2) ];
$CFG{vcs_clusterid}=46707;
$CFG{vcs_clustername}="sfha2233";

1;
```

Verifying the CP server configuration

Perform the following steps to verify the CP server configuration.

To verify the CP server configuration

- 1 Verify that the following configuration files are updated with the information you provided during the CP server configuration process:

- `/etc/vxcps.conf` (CP server configuration file)
 - `/etc/VRTSvcs/conf/config/main.cf` (VCS configuration file)
 - `/etc/VRTSvcs/db` (default location for CP server database)
- 2 Run the `cpsadm` command to check if the `vxcpserver` process is listening on the configured Virtual IP.

```
# cpsadm -s cp_server -a ping_cps
```

where *cp_server* is the virtual IP address or the virtual hostname of the CP server.

Configuring Symantec VirtualStore

This chapter includes the following topics:

- [Overview of tasks to configure Symantec VirtualStore using the script-based installer](#)
- [Configuring SVS using the script-based installer](#)

Overview of tasks to configure Symantec VirtualStore using the script-based installer

[Table 8-1](#) lists the tasks that are involved in configuring Symantec VirtualStore using the script-based installer.

Table 8-1 Tasks to configure Symantec VirtualStore using the script-based installer

Task	Reference
Start the software configuration	See “Starting the software configuration” on page 102.
Specify the systems where you want to configure Symantec VirtualStore	See “Specifying systems for configuration” on page 103.
Configure the basic cluster	See “Configuring private heartbeat links” on page 104.
Configure virtual IP address of the cluster (optional)	See “Configuring the virtual IP of the cluster” on page 108.

Table 8-1 Tasks to configure Symantec VirtualStore using the script-based installer (*continued*)

Task	Reference
Configure the cluster in secure mode (optional)	See “ Configuring Symantec VirtualStore in secure mode ” on page 70.
Add VCS users (required if you did not configure the cluster in secure mode)	See “ Adding VCS users ” on page 114.
Configure SMTP email notification (optional)	See “ Configuring SMTP email notification ” on page 115.
Configure SNMP email notification (optional)	See “ Configuring SNMP trap notification ” on page 116.
Complete the software configuration	See “ Completing the SVS configuration ” on page 119.

Configuring SVS using the script-based installer

Starting the software configuration

You can configure Symantec VirtualStore using the Veritas product installer or the `installsvs` command.

Note: If you want to reconfigure Symantec VirtualStore, before you start the installer you must stop all the resources that are under VCS control using the `hastop` command or the `hagrp -offline` command.

To configure Symantec VirtualStore using the product installer

- 1 Confirm that you are logged in as the superuser and that you have mounted the product disc.
- 2 Start the installer.

```
# ./installer
```

The installer starts the product installation program with a copyright message and specifies the directory where the logs are created.

- 3 From the opening Selection Menu, choose: c for "Configure an Installed Product."
- 4 From the displayed list of products to configure, choose the corresponding number for your product:
Symantec VirtualStore

To configure Symantec VirtualStore using the `installsvs` program

- 1 Confirm that you are logged in as the superuser.
- 2 Start the `installsvs` program.

```
# /opt/VRTS/install/installsvs<version> -configure
```

Where *<version>* is the specific release version.

See ["About the Veritas installer"](#) on page 41.

The installer begins with a copyright message and specifies the directory where the logs are created.

Specifying systems for configuration

The installer prompts for the system names on which you want to configure Symantec VirtualStore. The installer performs an initial check on the systems that you specify.

To specify system names for configuration

- 1 Enter the names of the systems where you want to configure Symantec VirtualStore.

```
Enter the operating_system system names separated  
by spaces: [q,?] (sys1) sys1 sys2
```

- 2 Review the output as the installer verifies the systems you specify.

The installer does the following tasks:

- Checks that the local node running the installer can communicate with remote nodes
If the installer finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases. If ssh binaries cannot communicate with remote nodes, the installer tries remsh binaries. And if both ssh and rsh binaries fail, the installer prompts to help the user to setup ssh or rsh binaries.
- Makes sure that the systems are running with the supported operating system

- Makes sure the installer started from the global zone
 - Checks whether Symantec VirtualStore is installed
 - Exits if 6.0.1 is not installed
- 3 Choose the mode you want to configure Symantec VirtualStore:

- 1) Typical
- 2) Custom

Choose the mode you would like to configure SVS: [1-2,q,?] (1)

- If you choose the **Typical** mode, the configuration automatically generates the cluster ID and automatically configures the network.
 - If you choose the **Custom** mode, then continue to follow the steps.
- 4 Review the installer output about the I/O fencing configuration and confirm whether you want to configure fencing in enabled mode.

Do you want to configure I/O Fencing in enabled mode? [y,n,q,?] (y)

See [“About planning to configure I/O fencing”](#) on page 71.

Configuring the cluster name

Enter the cluster information when the installer prompts you.

To configure the cluster

- 1 Review the configuration instructions that the installer presents.
- 2 Enter the unique cluster name.

Enter the unique cluster name: [q,?] **clus1**

Configuring private heartbeat links

You now configure the private heartbeat links that LLT uses. VCS provides the option to use LLT over Ethernet or over UDP (User Datagram Protocol). Symantec recommends that you configure heartbeat links that use LLT over Ethernet for high performance, unless hardware requirements force you to use LLT over UDP. If you want to configure LLT over UDP, make sure you meet the prerequisites.

See [“Using the UDP layer for LLT”](#) on page 449.

The following procedure helps you configure LLT over Ethernet.

To configure private heartbeat links

- 1 Choose one of the following options at the installer prompt based on whether you want to configure LLT over Ethernet or UDP.
 - Option 1: LLT over Ethernet (answer installer questions)
Enter the heartbeat link details at the installer prompt to configure LLT over Ethernet.
Skip to step 2.
 - Option 2: LLT over UDP (answer installer questions)
Make sure that each NIC you want to use as heartbeat link has an IP address configured. Enter the heartbeat link details at the installer prompt to configure LLT over UDP. If you had not already configured IP addresses to the NICs, the installer provides you an option to detect the IP address for a given NIC.
Skip to step 3.
 - Option 3: Automatically detect configuration for LLT over Ethernet
Allow the installer to automatically detect the heartbeat link details to configure LLT over Ethernet. The installer tries to detect all connected links between all systems.
Skip to step 5.

Note: Option 3 is not available when the configuration is a single node configuration.

- 2 If you chose option 1, enter the network interface card details for the private heartbeat links.

The installer discovers and lists the network interface cards.

Answer the installer prompts. The following example shows different NICs based on architecture:

- For Solaris SPARC:
You must not enter the network interface card that is used for the public network (typically bge0.)

```
Enter the NIC for the first private heartbeat link on sys1:  
[b,q,?] bge0  
Would you like to configure a second private heartbeat link?  
[y,n,q,b,?] (y)  
Enter the NIC for the second private heartbeat link on sys1:  
[b,q,?] bge1
```

Would you like to configure a third private heartbeat link?
[y,n,q,b,?] (n)

Do you want to configure an additional low priority heartbeat link? [y,n,q,b,?] (n)

■ For Solaris x64:

You must not enter the network interface card that is used for the public network (typically e1000g0.)

Enter the NIC for the first private heartbeat link on sys1:
[b,q,?] **e1000g1**

Would you like to configure a second private heartbeat link?
[y,n,q,b,?] (y)

Enter the NIC for the second private heartbeat link on sys1:
[b,q,?] **e1000g2**

Would you like to configure a third private heartbeat link?
[y,n,q,b,?] (n)

- 3** If you chose option 2, enter the NIC details for the private heartbeat links. This step uses examples such as *private_NIC1* or *private_NIC2* to refer to the available names of the NICs.

```

Enter the NIC for the first private heartbeat
link on sys1: [b,q,?] private_NIC1
Do you want to use address 192.168.0.1 for the
first private heartbeat link on sys1: [y,n,q,b,?] (y)
Enter the UDP port for the first private heartbeat
link on sys1: [b,q,?] (50000) ?
Would you like to configure a second private
heartbeat link? [y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat
link on sys1: [b,q,?] private_NIC2
Do you want to use address 192.168.1.1 for the
second private heartbeat link on sys1: [y,n,q,b,?] (y)
Enter the UDP port for the second private heartbeat
link on sys1: [b,q,?] (50001) ?
Do you want to configure an additional low priority
heartbeat link? [y,n,q,b,?] (n) y
Enter the NIC for the low priority heartbeat
link on sys1: [b,q,?] (private_NIC0)
Do you want to use address 192.168.3.1 for
the low priority heartbeat link on sys1: [y,n,q,b,?] (y)
Enter the UDP port for the low priority heartbeat
link on sys1: [b,q,?] (50004)

```

- 4** Choose whether to use the same NIC details to configure private heartbeat links on other systems.

```

Are you using the same NICs for private heartbeat links on all
systems? [y,n,q,b,?] (y)

```

If you want to use the NIC details that you entered for sys1, make sure the same NICs are available on each system. Then, enter **y** at the prompt.

For LLT over UDP, if you want to use the same NICs on other systems, you still must enter unique IP addresses on each NIC for other systems.

If the NIC device names are different on some of the systems, enter **n**. Provide the NIC details for each system as the program prompts.

- 5 If you chose option 3, the installer detects NICs on each system and network links, and sets link priority.

If the installer fails to detect heartbeat links or fails to find any high-priority links, then choose option 1 or option 2 to manually configure the heartbeat links.

See step 2 for option 1, or step 3 for option 2.

- 6 Enter a unique cluster ID:

```
Enter a unique cluster ID number between 0-65535: [b,q,?] (60842)
```

The cluster cannot be configured if the cluster ID 60842 is in use by another cluster. Installer performs a check to determine if the cluster ID is duplicate. The check takes less than a minute to complete.

```
Would you like to check if the cluster ID is in use by another  
cluster? [y,n,q] (y)
```

- 7 Verify and confirm the information that the installer summarizes.

Configuring the virtual IP of the cluster

You can configure the virtual IP of the cluster to use to connect from the Cluster Manager (Java Console), Veritas Operations Manager (VOM), or to specify in the RemoteGroup resource.

See the *Veritas Cluster Server Administrator's Guide* for information on the Cluster Manager.

See the *Veritas Cluster Server Bundled Agents Reference Guide* for information on the RemoteGroup agent.

To configure the virtual IP of the cluster

- 1 Review the required information to configure the virtual IP of the cluster.
- 2 When the system prompts whether you want to configure the virtual IP, enter `y`.
- 3 Confirm whether you want to use the discovered public NIC on the first system.

Do one of the following:

- If the discovered NIC is the one to use, press `Enter`.
- If you want to use a different NIC, type the name of a NIC to use and press `Enter`.

```
Active NIC devices discovered on sys1: bge0
Enter the NIC for Virtual IP of the Cluster to use on sys1:
[b,q,?] (bge0)
```

4 Confirm whether you want to use the same public NIC on all nodes.

Do one of the following:

- If all nodes use the same public NIC, enter *y*.
- If unique NICs are used, enter *n* and enter a NIC for each node.

```
Is bge0 to be the public NIC used by all systems
[y,n,q,b,?] (y)
```

5 Enter the virtual IP address for the cluster.

You can enter either an IPv4 address or an IPv6 address.

For IPv4: ■ Enter the virtual IP address.

```
Enter the Virtual IP address for the Cluster:
[b,q,?] 192.168.1.16
```

- Confirm the default netmask or enter another one:

```
Enter the netmask for IP 192.168.1.16: [b,q,?]
(255.255.240.0)
```

- Verify and confirm the Cluster Virtual IP information.

```
Cluster Virtual IP verification:
```

```
NIC: bge0
IP: 192.168.1.16
Netmask: 255.255.240.0
```

```
Is this information correct? [y,n,q] (y)
```

For IPv6

- Enter the virtual IP address.

```
Enter the Virtual IP address for the Cluster:
[b, q, ?] 2001:454e:205a:110:203:baff:feee:10
```

- Enter the prefix for the virtual IPv6 address you provided. For example:

```
Enter the Prefix for IP
2001:454e:205a:110:203:baff:feee:10: [b, q, ?] 64
```

- Verify and confirm the Cluster Virtual IP information.

```
Cluster Virtual IP verification:
```

```
NIC: bge0
IP: 2001:454e:205a:110:203:baff:feee:10
Prefix: 64
```

```
Is this information correct? [y,n,q] (y)
```

If you want to set up trust relationships for your secure cluster, refer to the following topics:

See [“Configuring a secure cluster node by node”](#) on page 110.

Configuring a secure cluster node by node

For environments that do not support passwordless ssh or passwordless rsh, you cannot use the `-security` option to enable secure mode for your cluster. Instead, you can use the `-securityonnode` option to configure a secure cluster node by node. Moreover, to enable security in fips mode, use the `-fips` option together with `-securityonnode`.

[Table 8-2](#) lists the tasks that you must perform to configure a secure cluster.

Table 8-2 Configuring a secure cluster node by node

Task	Reference
Configure security on one node	See “Configuring the first node” on page 111.
Configure security on the remaining nodes	See “Configuring the remaining nodes” on page 111.
Complete the manual configuration steps	See “Completing the secure cluster configuration” on page 112.

Configuring the first node

Perform the following steps on one node in your cluster.

To configure security on the first node

- 1 Ensure that you are logged in as superuser.
- 2 Enter the following command:

```
# /opt/VRTS/install/installsvs<version> -securityonnode
```

Where *<version>* is the specific release version.

See [“About the Veritas installer”](#) on page 41.

The installer lists information about the cluster, nodes, and service groups. If VCS is not configured or if VCS is not running on all nodes of the cluster, the installer prompts whether you want to continue configuring security. It then prompts you for the node that you want to configure.

```
VCS is not running on all systems in this cluster. All VCS systems  
must be in RUNNING state. Do you want to continue? [y,n,q] (n) y
```

```
1) Perform security configuration on first node and export  
security configuration files.
```

```
2) Perform security configuration on remaining nodes with  
security configuration files.
```

```
Select the option you would like to perform [1-2,q.?] 1
```

Warning: All VCS configurations about cluster users are deleted when you configure the first node. You can use the `/opt/VRTSvcs/bin/hauser` command to create cluster users manually.

- 3 The installer completes the secure configuration on the node. It specifies the location of the security configuration files and prompts you to copy these files to the other nodes in the cluster. The installer also specifies the location of log files, summary file, and response file.
- 4 Copy the security configuration files from the location specified by the installer to temporary directories on the other nodes in the cluster.

Configuring the remaining nodes

On each of the remaining nodes in the cluster, perform the following steps.

To configure security on each remaining node

- 1 Ensure that you are logged in as superuser.
- 2 Enter the following command:

```
# /opt/VRTS/install/installsvs<version> -securityonnode
```

Where *<version>* is the specific release version.

See [“About the Veritas installer”](#) on page 41.

The installer lists information about the cluster, nodes, and service groups. If VCS is not configured or if VCS is not running on all nodes of the cluster, the installer prompts whether you want to continue configuring security. It then prompts you for the node that you want to configure. Enter **2**.

```
VCS is not running on all systems in this cluster. All VCS systems  
must be in RUNNING state. Do you want to continue? [y,n,q] (n) y
```

```
1) Perform security configuration on first node and export  
security configuration files.
```

```
2) Perform security configuration on remaining nodes with  
security configuration files.
```

```
Select the option you would like to perform [1-2,q.?] 2
```

The installer completes the secure configuration on the node. It specifies the location of log files, summary file, and response file.

Completing the secure cluster configuration

Perform the following manual steps to complete the configuration.

To complete the secure cluster configuration

- 1 On the first node, freeze all service groups except the ClusterService service group.

```
# /opt/VRTSvcs/bin/haconf -makerw
# /opt/VRTSvcs/bin/hagrps -list Frozen=0
# /opt/VRTSvcs/bin/hagrps -freeze groupname -persistent
# /opt/VRTSvcs/bin/haconf -dump -makero
```

- 2 On the first node, stop the VCS engine.

```
# /opt/VRTSvcs/bin/hastop -all -force
```

- 3 On all nodes, stop the CmdServer.

```
# /opt/VRTSvcs/bin/CmdServer -stop
```

- 4 On the first node, edit the `/etc/VRTSvcs/conf/config/main.cf` file to resemble the following:

```
cluster clus1 (
SecureClus = 1
)
```

- 5 On all nodes, create the `/etc/VRTSvcs/conf/config/.secure` file.

```
# touch /etc/VRTSvcs/conf/config/.secure
```

- 6 On the first node, start VCS. Then start VCS on the remaining nodes.

```
# /opt/VRTSvcs/bin/hastart
```

- 7 On all nodes, start CmdServer.

```
# /opt/VRTSvcs/bin/CmdServer
```

- 8 On the first node, unfreeze the service groups.

```
# /opt/VRTSvcs/bin/haconf -makerw
```

```
# /opt/VRTSvcs/bin/hagrp -list Frozen=1
```

```
# /opt/VRTSvcs/bin/hagrp -unfreeze groupname -persistent
```

```
# /opt/VRTSvcs/bin/haconf -dump -makero
```

Adding VCS users

If you have enabled a secure VCS cluster, you do not need to add VCS users now. Otherwise, on systems operating under an English locale, you can add VCS users at this time.

To add VCS users

- 1 Review the required information to add VCS users.
- 2 Reset the password for the Admin user, if necessary.

```
Do you wish to accept the default cluster credentials of  
'admin/password'? [y,n,q] (y) n  
Enter the user name: [b,q,?] (admin)  
Enter the password:  
Enter again:
```

- 3 To add a user, enter **y** at the prompt.

```
Do you want to add another user to the cluster? [y,n,q] (y)
```

- 4 Enter the user's name, password, and level of privileges.

```
Enter the user name: [b,q,?] smith  
Enter New Password:*****
```

```
Enter Again:*****
```

```
Enter the privilege for user smith (A=Administrator, O=Operator,  
G=Guest): [b,q,?] a
```

- 5 Enter **n** at the prompt if you have finished adding users.

```
Would you like to add another user? [y,n,q] (n)
```

- 6 Review the summary of the newly added users and confirm the information.

Configuring SMTP email notification

You can choose to configure VCS to send event notifications to SMTP email services. You need to provide the SMTP server name and email addresses of people to be notified. Note that you can also configure the notification after installation.

Refer to the *Veritas Cluster Server Administrator's Guide* for more information.

To configure SMTP email notification

- 1 Review the required information to configure the SMTP email notification.
- 2 Specify whether you want to configure the SMTP notification.

```
Do you want to configure SMTP notification? [y,n,q,?] (n) y
```

If you do not want to configure the SMTP notification, you can skip to the next configuration option.

See [“Configuring SNMP trap notification”](#) on page 116.

- 3 Provide information to configure SMTP notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on sys1: bge0
Enter the NIC for the VCS Notifier to use on sys1:
[b,q,?] (bge0)
Is bge0 to be the public NIC used by all systems?
[y,n,q,b,?] (y)
```

- Enter the SMTP server's host name.

```
Enter the domain-based hostname of the SMTP server
(example: smtp.yourcompany.com): [b,q,?] smtp.example.com
```

- Enter the email address of each recipient.

```
Enter the full email address of the SMTP recipient
(example: user@yourcompany.com): [b,q,?] ozzie@example.com
```

- Enter the minimum security level of messages to be sent to each recipient.

```
Enter the minimum severity of events for which mail should be
sent to ozzie@example.com [I=Information, W=Warning,
E=Error, S=SevereError]: [b,q,?] w
```

4 Add more SMTP recipients, if necessary.

- If you want to add another SMTP recipient, enter `y` and provide the required information at the prompt.

```
Would you like to add another SMTP recipient? [y,n,q,b] (n) y
```

```
Enter the full email address of the SMTP recipient
(example: user@yourcompany.com): [b,q,?] harriet@example.com
```

```
Enter the minimum severity of events for which mail should be
sent to harriet@example.com [I=Information, W=Warning,
E=Error, S=SevereError]: [b,q,?] E
```

- If you do not want to add, answer `n`.

```
Would you like to add another SMTP recipient? [y,n,q,b] (n)
```

5 Verify and confirm the SMTP notification information.

```
NIC: bge0
```

```
SMTP Address: smtp.example.com
```

```
Recipient: ozzie@example.com receives email for Warning or
higher events
```

```
Recipient: harriet@example.com receives email for Error or
higher events
```

```
Is this information correct? [y,n,q] (y)
```

Configuring SNMP trap notification

You can choose to configure VCS to send event notifications to SNMP management consoles. You need to provide the SNMP management console name to be notified and message severity levels.

Note that you can also configure the notification after installation.

Refer to the *Veritas Cluster Server Administrator's Guide* for more information.

To configure the SNMP trap notification

- 1 Review the required information to configure the SNMP notification feature of VCS.

- 2 Specify whether you want to configure the SNMP notification.

```
Do you want to configure SNMP notification? [y,n,q,?] (n) y
```

See [“Configuring global clusters”](#) on page 118.

- 3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on sys1: bge0
Enter the NIC for the VCS Notifier to use on sys1:
[b,q,?] (bge0)
Is bge0 to be the public NIC used by all systems?
[y,n,q,b,?] (y)
```

- Enter the SNMP trap daemon port.

```
Enter the SNMP trap daemon port: [b,q,?] (162)
```

- Enter the SNMP console system name.

```
Enter the SNMP console system name: [b,q,?] sys4
```

- Enter the minimum security level of messages to be sent to each console.

```
Enter the minimum severity of events for which SNMP traps
should be sent to sys4 [I=Information, W=Warning, E=Error,
S=SevereError]: [b,q,?] E
```

- 4 Add more SNMP consoles, if necessary.

- If you want to add another SNMP console, enter `y` and provide the required information at the prompt.

```
Would you like to add another SNMP console? [y,n,q,b] (n) y
Enter the SNMP console system name: [b,q,?] sys4
Enter the minimum severity of events for which SNMP traps
should be sent to sys4 [I=Information, W=Warning,
E=Error, S=SevereError]: [b,q,?] S
```

- If you do not want to add, answer n.

```
Would you like to add another SNMP console? [y,n,q,b] (n)
```

5 Verify and confirm the SNMP notification information.

```
NIC: bge0
```

```
SNMP Port: 162
```

```
Console: sys4 receives SNMP traps for Error or  
higher events
```

```
Console: sys4 receives SNMP traps for SevereError or  
higher events
```

```
Is this information correct? [y,n,q] (y)
```

Configuring global clusters

If you had installed a valid HA/DR license, the installer provides you an option to configure this cluster as global cluster.

You can configure global clusters to link clusters at separate locations and enable wide-area failover and disaster recovery. The installer adds basic global cluster information to the VCS configuration file. You must perform additional configuration tasks to set up a global cluster.

See the *Symantec VirtualStore Installation and Configuration Guide* for instructions to set up Symantec VirtualStore global clusters.

Note: If you installed a HA/DR license to set up replicated data cluster or campus cluster, skip this installer option.

To configure the global cluster option

- 1 Review the required information to configure the global cluster option.
- 2 Specify whether you want to configure the global cluster option.

```
Do you want to configure the Global Cluster Option? [y,n,q] (n) y
```

If you skip this option, the installer proceeds to configure VCS based on the configuration details you provided.

3 Provide information to configure this cluster as global cluster.

The installer prompts you for a NIC, a virtual IP address, and value for the netmask.

If you had entered virtual IP address details, the installer discovers the values you entered. You can use the same virtual IP address for global cluster configuration or enter different values.

You can also enter an IPv6 address as a virtual IP address.

4 Verify and confirm the configuration of the global cluster. For example:

For IPv4: Global Cluster Option configuration verification:

```
NIC: bge0
IP: 10.198.89.22
Netmask: 255.255.240.0
```

Is this information correct? [y,n,q] (y)

On Solaris x64, an example for the NIC's port is bge0.

For IPv6 Global Cluster Option configuration verification:

```
NIC: bge0
IP: 2001:454e:205a:110:203:baff:feee:10
Prefix: 64
```

Is this information correct? [y,n,q] (y)

On Solaris x64, an example for the NIC's port is bge0.

Completing the SVS configuration

After you enter the SVS configuration information, the installer prompts to stop the SVS processes to complete the configuration process. The installer continues to create configuration files and copies them to each system. The installer also configures a cluster UUID value for the cluster at the end of the configuration. After the installer successfully configures SVS, it restarts SVS and its related processes.

To complete the SVS configuration

- 1 If prompted, press Enter at the following prompt.

```
Do you want to stop SVS processes now? [y,n,q,?] (y)
```

- 2 Review the output as the installer stops various processes and performs the configuration. The installer then restarts SVS and its related processes.
- 3 Enter y at the prompt to send the installation information to Symantec.

```
Would you like to send the information about this installation  
to Symantec to help improve installation in the future?  
[y,n,q,?] (y) y
```

- 4 After the installer configures Symantec VirtualStore successfully, note the location of summary, log, and response files that installer creates.

The files provide the useful information that can assist you with the configuration and can also assist future configurations.

summary file	Describes the cluster and its configured resources.
log file	Details the entire configuration.
response file	Contains the configuration information that can be used to perform secure or unattended installations on other systems. See “Configuring SVS using response files” on page 195.

Verifying and updating licenses on the system

After you install Symantec VirtualStore, you can verify the licensing information using the vxlicrep program. You can replace the demo licenses with a permanent license.

See [“Checking licensing information on the system”](#) on page 120.

See [“Updating product licenses”](#) on page 121.

Checking licensing information on the system

You can use the vxlicrep program to display information about the licenses on a system.

To check licensing information

- 1 Navigate to the folder containing the `vxlicrep` program and enter:

```
# vxlicrep
```

- 2 Review the following output to determine the following information:

- The license key
- The type of license
- The product for which it applies
- Its expiration date, if any. Demo keys have expiration dates. Permanent keys and site keys do not have expiration dates.

Updating product licenses

You can use the `./installer -license` command or the `vxlicinst -k` to add the Symantec VirtualStore license key on each node. If you have Symantec VirtualStore already installed and configured and you use a demo license, you can replace the demo license.

See [“Replacing a Symantec VirtualStore demo license with a permanent license”](#) on page 121.

To update product licenses using the installer command

- 1 On each node, enter the license key using the command:

```
# ./installer -license
```

- 2 At the prompt, enter your license number.

To update product licenses using the vxlicinst command

- ◆ On each node, enter the license key using the command:

```
# vxlicinst -k license number
```

Replacing a Symantec VirtualStore demo license with a permanent license

When a Symantec VirtualStore demo key license expires, you can replace it with a permanent license using the `vxlicinst(1)` program.

To replace a demo key

- 1 Make sure you have permissions to log in as root on each of the nodes in the cluster.

- 2 Shut down Symantec VirtualStore on all nodes in the cluster:

```
# hastop -all -force
```

This command does not shut down any running applications.

- 3 Enter the permanent license key using the following command on each node:

```
# vxlicinst -k license key
```

- 4 Make sure demo licenses are replaced on all cluster nodes before starting Symantec VirtualStore.

```
# vxlicrep
```

- 5 Start Symantec VirtualStore on each node:

```
# hastart
```

Configuring SVS for data integrity

This chapter includes the following topics:

- [Setting up disk-based I/O fencing using installsvs](#)
- [Setting up disk-based I/O fencing manually](#)
- [Setting up server-based I/O fencing using installsvs](#)
- [Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsvs](#)
- [Setting up server-based I/O fencing manually](#)
- [Setting up non-SCSI-3 fencing in virtual environments manually](#)
- [Enabling or disabling the preferred fencing policy](#)

Setting up disk-based I/O fencing using installsvs

You can configure I/O fencing using the `-fencing` option of the `installsvs`.

Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

To initialize disks as VxVM disks

- 1 List the new external disks or the LUNs as recognized by the operating system. On each node, enter:

```
# vxdisk list
```

- 2 To initialize the disks as VxVM disks, use one of the following methods:

- Use the interactive `vxdiskadm` utility to initialize the disks as VxVM disks. For more information see the *Veritas Storage Foundation Administrator's Guide*.
- Use the `vxdisksetup` command to initialize a disk as a VxVM disk.

```
# vxdisksetup -i device_name
```

The example specifies the CDS format:

```
# vxdisksetup -i c2t13d0
```

Repeat this command for each disk you intend to use as a coordinator disk.

Configuring disk-based I/O fencing using installsvs

Note: The installer stops and starts Symantec VirtualStore to complete I/O fencing configuration. Make sure to unfreeze any frozen VCS service groups in the cluster for the installer to successfully stop Symantec VirtualStore.

To set up disk-based I/O fencing using the `installsvs`

- 1 Start the `installsvs` with `-fencing` option.

```
# /opt/VRTS/install/installsvs<version> -fencing
```

Where `<version>` is the specific release version.

See “[About the Veritas installer](#)” on page 41.

The `installsvs` starts with a copyright message and verifies the cluster information.

Note the location of log files which you can access in the event of any problem with the configuration process.

- 2 Confirm that you want to proceed with the I/O fencing configuration at the prompt.

The program checks that the local node running the script can communicate with remote nodes and checks whether Symantec VirtualStore 6.0.1 is configured properly.

- 3 Review the I/O fencing configuration options that the program presents. Type **2** to configure disk-based I/O fencing.

```
Select the fencing mechanism to be configured in this  
Application Cluster [1-4,b,q] 2
```

- 4 Review the output as the configuration program checks whether VxVM is already started and is running.

- If the check fails, configure and enable VxVM before you repeat this procedure.
- If the check passes, then the program prompts you for the coordinator disk group information.

- 5 Choose whether to use an existing disk group or create a new disk group to configure as the coordinator disk group.

The program lists the available disk group names and provides an option to create a new disk group. Perform one of the following:

- To use an existing disk group, enter the number corresponding to the disk group at the prompt.
The program verifies whether the disk group you chose has an odd number of disks and that the disk group has a minimum of three disks.
- To create a new disk group, perform the following steps:
 - Enter the number corresponding to the **Create a new disk group** option.

The program lists the available disks that are in the CDS disk format in the cluster and asks you to choose an odd number of disks with at least three disks to be used as coordinator disks.

Symantec recommends that you use three disks as coordination points for disk-based I/O fencing.

If the available VxVM CDS disks are less than the required, installer asks whether you want to initialize more disks as VxVM disks. Choose the disks you want to initialize as VxVM disks and then use them to create new disk group.

- Enter the numbers corresponding to the disks that you want to use as coordinator disks.
 - Enter the disk group name.
- 6 Verify that the coordinator disks you chose meet the I/O fencing requirements. You must verify that the disks are SCSI-3 PR compatible using the `vxfcntlshdw` utility and then return to this configuration program.

See [“Checking shared disks for I/O fencing”](#) on page 127.

- 7 After you confirm the requirements, the program creates the coordinator disk group with the information you provided.
- 8 Enter the I/O fencing disk policy that you chose to use. For example:

```
Enter disk policy for the disk(s) (raw/dmp): [b,q,?] raw
```

The program also does the following:

- Populates the `/etc/vxfendg` file with this disk group information
 - Populates the `/etc/vxfenmode` file on each cluster node with the I/O fencing mode information and with the SCSI-3 disk policy information
- 9 Verify and confirm the I/O fencing configuration information that the installer summarizes.
- 10 Review the output as the configuration program does the following:
- Stops VCS and I/O fencing on each node.
 - Configures disk-based I/O fencing and starts the I/O fencing process.
 - Updates the VCS configuration file `main.cf` if necessary.
 - Copies the `/etc/vxfenmode` file to a date and time suffixed file `/etc/vxfenmode-date-time`. This backup file is useful if any future fencing configuration fails.
 - Updates the I/O fencing configuration file `/etc/vxfenmode`.

- Starts VCS on each node to make sure that the Symantec VirtualStore is cleanly configured to use the I/O fencing feature.
- 11 Review the output as the configuration program displays the location of the log files, the summary files, and the response files.
 - 12 Configure the Coordination Point Agent.

```
Do you want to configure Coordination Point Agent on
the client cluster? [y,n,q] (y)
```

- 13 Enter a name for the service group for the Coordination Point Agent.

```
Enter a non-existing name for the service group for
Coordination Point Agent: [b] (vxfen) vxfen
```

- 14 Set the level two monitor frequency.

```
Do you want to set LevelTwoMonitorFreq? [y,n,q] (y)
```

- 15 Decide the value of the level two monitor frequency.

```
Enter the value of the LevelTwoMonitorFreq attribute: [b,q,?] (5)
```

Installer adds Coordination Point Agent and updates the main configuration file.

See [“Configuring CoordPoint agent to monitor coordination points”](#) on page 157.

Checking shared disks for I/O fencing

Make sure that the shared storage you set up while preparing to configure SVS meets the I/O fencing requirements. You can test the shared disks using the `vxftsthdw` utility. The two nodes must have `ssh` (default) or `rsh` communication. To confirm whether a disk (or LUN) supports SCSI-3 persistent reservations, two nodes must simultaneously have access to the same disks. Because a shared disk is likely to have a different name on each node, check the serial number to verify the identity of the disk. Use the `vxfenadm` command with the `-i` option. This command option verifies that the same serial number for the LUN is returned on all paths to the LUN.

Make sure to test the disks that serve as coordinator disks.

The `vxftsthdw` utility has additional options suitable for testing many disks. Review the options for testing the disk groups (`-g`) and the disks that are listed in a file (`-f`). You can also test disks without destroying data using the `-r` option.

See the *Symantec VirtualStore Administrator's Guide*.

Checking that disks support SCSI-3 involves the following tasks:

- Verifying the Array Support Library (ASL)
See [“Verifying Array Support Library \(ASL\)”](#) on page 128.
- Verifying that nodes have access to the same disk
See [“Verifying that the nodes have access to the same disk”](#) on page 129.
- Testing the shared disks for SCSI-3
See [“Testing the disks using vxfcntl utility”](#) on page 130.

Verifying Array Support Library (ASL)

Make sure that the Array Support Library (ASL) for the array that you add is installed.

To verify Array Support Library (ASL)

- 1 If the Array Support Library (ASL) for the array that you add is not installed, obtain and install it on each node before proceeding.

The ASL for the supported storage device that you add is available from the disk array vendor or Symantec technical support.

- 2 Verify that the ASL for the disk array is installed on each of the nodes. Run the following command on each node and examine the output to verify the installation of ASL.

The following output is a sample:

```
# vxddladm listsupport all
```

LIBNAME	VID	PID
libvx3par.so	3PARdata	VV
libvxCLARiiON.so	DGC	All
libvxFJTSYe6k.so	FUJITSU	E6000
libvxFJTSYe8k.so	FUJITSU	All
libvxap.so	SUN	All
libvxatf.so	VERITAS	ATFNODES
libvxcompellent.so	COMPELNT	Compellent Vol
libvxcopan.so	COPANSYS	8814, 8818

- 3 Scan all disk drives and their attributes, update the VxVM device list, and reconfigure DMP with the new devices. Type:

```
# vxdisk scandisks
```

See the Veritas Volume Manager documentation for details on how to add and configure disks.

Verifying that the nodes have access to the same disk

Before you test the disks that you plan to use as shared data storage or as coordinator disks using the vxfcntl utility, you must verify that the systems see the same disk.

To verify that the nodes have access to the same disk

- 1 Verify the connection of the shared storage for data to two of the nodes on which you installed SVS.
- 2 Ensure that both nodes are connected to the same disk during the testing. Use the vxfenadm command to verify the disk serial number.

```
# vxfenadm -i diskpath
```

Refer to the `vxfenadm` (1M) manual page.

For example, an EMC disk is accessible by the `/dev/rdisk/c1t1d0s2` path on node A and the `/dev/rdisk/c2t1d0s2` path on node B.

From node A, enter:

```
# vxfenadm -i /dev/rdisk/c1t1d0s2
```

```
Vendor id : EMC  
Product id : SYMMETRIX  
Revision : 5567  
Serial Number : 42031000a
```

The same serial number information should appear when you enter the equivalent command on node B using the `/dev/rdisk/c2t1d0s2` path.

On a disk from another manufacturer, Hitachi Data Systems, the output is different and may resemble:

```
# vxfenadm -i /dev/rdisk/c3t1d2s2
```

```
Vendor id      : HITACHI  
Product id     : OPEN-3      -SUN  
Revision       : 0117  
Serial Number  : 0401EB6F0002
```

Testing the disks using vxfcntl utility

This procedure uses the `/dev/rdisk/c1t1d0s2` disk in the steps.

If the utility does not show a message that states a disk is ready, the verification has failed. Failure of verification can be the result of an improperly configured disk array. The failure can also be due to a bad disk.

If the failure is due to a bad disk, remove and replace it. The `vxfcntl` utility indicates a disk can be used for I/O fencing with a message resembling:

```
The disk /dev/rdisk/c1t1d0s2 is ready to be configured for I/O Fencing on  
node sys1
```

For more information on how to replace coordinator disks, refer to the *Symantec VirtualStore Administrator's Guide*.

To test the disks using vxfcntl utility

- 1 Make sure system-to-system communication functions properly.

- 2 From one node, start the utility.

Run the utility with the `-n` option if you use `rsh` for communication.

```
# vxfentsthdw [-n]
```

- 3 The script warns that the tests overwrite data on the disks. After you review the overview and the warning, confirm to continue the process and enter the node names.

Warning: The tests overwrite and destroy data on the disks unless you use the `-r` option.

```
***** WARNING!!!!!!!!!! *****
THIS UTILITY WILL DESTROY THE DATA ON THE DISK!!

Do you still want to continue : [y/n] (default: n) y
Enter the first node of the cluster: sys1
Enter the second node of the cluster: sys2
```

- 4 Enter the names of the disks that you want to check. Each node may know the same disk by a different name:

```
Enter the disk name to be checked for SCSI-3 PGR on node
IP_adrs_of_sys1 in the format:
for dmp: /dev/vx/rdmp/cxtxdxsx
for raw: /dev/rdisk/cxtxdxsx
Make sure it's the same disk as seen by nodes
IP_adrs_ofsys1 and IP_adrs_of_sys2
/dev/rdsk/c2t13d0s2
```

```
Enter the disk name to be checked for SCSI-3 PGR on node
IP_adrs_of_sys2 in the format:
for dmp: /dev/vx/rdmp/cxtxdxsx
for raw: /dev/rdisk/cxtxdxsx
Make sure it's the same disk as seen by nodes
IP_adrs_ofsys1 and IP_adrs_of_sys2
/dev/rdsk/c2t13d0s2
```

If the serial numbers of the disks are not identical, then the test terminates.

- 5 Review the output as the utility performs the checks and reports its activities.

- 6 If a disk is ready for I/O fencing on each node, the utility reports success for each node. For example, the utility displays the following message for the node `sys1`.

```
The disk is now ready to be configured for I/O Fencing on node
sys1
```

```
ALL tests on the disk /dev/rdisk/clt1d0s2 have PASSED
The disk is now ready to be configured for I/O Fencing on node
sys1
```

- 7 Run the `vxmfentsthdw` utility for each disk you intend to verify.

Setting up disk-based I/O fencing manually

[Table 9-1](#) lists the tasks that are involved in setting up I/O fencing.

Table 9-1 Tasks to set up I/O fencing manually

Task	Reference
Initializing disks as VxVM disks	See “Initializing disks as VxVM disks” on page 123.
Identifying disks to use as coordinator disks	See “Identifying disks to use as coordinator disks” on page 133.
Checking shared disks for I/O fencing	See “Checking shared disks for I/O fencing” on page 127.
Setting up coordinator disk groups	See “Setting up coordinator disk groups” on page 133.
Creating I/O fencing configuration files	See “Creating I/O fencing configuration files” on page 134.
Modifying Symantec VirtualStore configuration to use I/O fencing	See “Modifying VCS configuration to use I/O fencing” on page 135.
Configuring CoordPoint agent to monitor coordination points	See “Configuring CoordPoint agent to monitor coordination points” on page 157.
Verifying I/O fencing configuration	See “Verifying I/O fencing configuration” on page 137.

Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See [“Initializing disks as VxVM disks”](#) on page 123.

Review the following procedure to identify disks to use as coordinator disks.

To identify the coordinator disks

- 1 List the disks on each node.

For example, execute the following commands to list the disks:

```
# vxdisk -o alldgs list
```

- 2 Pick three SCSI-3 PR compliant shared disks as coordinator disks.

See [“Checking shared disks for I/O fencing”](#) on page 127.

Setting up coordinator disk groups

From one node, create a disk group named `vxencoorddg`. This group must contain three disks or LUNs. You must also set the coordinator attribute for the coordinator disk group. VxVM uses this attribute to prevent the reassignment of coordinator disks to other disk groups.

Note that if you create a coordinator disk group as a regular disk group, you can turn on the coordinator attribute in Volume Manager.

Refer to the *Veritas Storage Foundation Administrator's Guide* for details on how to create disk groups.

The following example procedure assumes that the disks have the device names `c1t1d0s2`, `c2t1d0s2`, and `c3t1d0s2`.

To create the vxencoorddg disk group

- 1 On any node, create the disk group by specifying the device names:

```
# vxdg init vxencoorddg c1t1d0s2 c2t1d0s2 c3t1d0s2
```

- 2 Set the coordinator attribute value as "on" for the coordinator disk group.

```
# vxdg -g vxencoorddg set coordinator=on
```

- 3 Deport the coordinator disk group:

```
# vxdg deport vxencoorddg
```

- 4 Import the disk group with the `-t` option to avoid automatically importing it when the nodes restart:

```
# vxdg -t import vxfencoorddg
```

- 5 Deport the disk group. Deporting the disk group prevents the coordinator disks from serving other purposes:

```
# vxdg deport vxfencoorddg
```

Creating I/O fencing configuration files

After you set up the coordinator disk group, you must do the following to configure I/O fencing:

- Create the I/O fencing configuration file `/etc/vxfendg`
- Update the I/O fencing configuration file `/etc/vxfenmode`

To update the I/O fencing files and start I/O fencing

- 1 On each nodes, type:

```
# echo "vxfencoorddg" > /etc/vxfendg
```

Do not use spaces between the quotes in the "vxfencoorddg" text.

This command creates the `/etc/vxfendg` file, which includes the name of the coordinator disk group.

- 2 On all cluster nodes depending on the SCSI-3 mechanism, type one of the following selections:

- For DMP configuration:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
```

- For raw device configuration:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_raw /etc/vxfenmode
```

- 3 To check the updated `/etc/vxfenmode` configuration, enter the following command on one of the nodes. For example:

```
# more /etc/vxfenmode
```

- 4 Ensure that you edit the following file on each node in the cluster to change the values of the `VXFEN_START` and the `VXFEN_STOP` environment variables to 1:

```
/etc/default/vxfen
```

Modifying VCS configuration to use I/O fencing

After you add coordination points and configure I/O fencing, add the `UseFence = SCSI3` cluster attribute to the VCS configuration file `/etc/VRTSvcs/conf/config/main.cf`.

If you reset this attribute to `UseFence = None`, VCS does not make use of I/O fencing abilities while failing over service groups. However, I/O fencing needs to be disabled separately.

To modify VCS configuration to enable I/O fencing

- 1 Save the existing configuration:

```
# haconf -dump -makero
```

- 2 Stop VCS on all nodes:

```
# hastop -all
```

- 3 To ensure High Availability has stopped cleanly, run `gabconfig -a`.

In the output of the commands, check that Port `h` is not present.

- 4 If the I/O fencing driver `vxfen` is already running, stop the I/O fencing driver.

```
# svcadm disable -t vxfen
```

- 5 Make a backup copy of the `main.cf` file:

```
# cd /etc/VRTSvcs/conf/config
```

```
# cp main.cf main.orig
```

- 6 On one node, use vi or another text editor to edit the main.cf file. To modify the list of cluster attributes, add the UseFence attribute and assign its value as SCSI3.

```
cluster clus1(  
  UserNames = { admin = "CDRpdxPmHpzS." }  
  Administrators = { admin }  
  HacliUserLevel = COMMANDROOT  
  CounterInterval = 5  
  UseFence = SCSI3  
)
```

Regardless of whether the fencing configuration is disk-based or server-based, the value of the cluster-level attribute UseFence is set to SCSI3.

- 7 Save and close the file.
- 8 Verify the syntax of the file /etc/VRTSvcs/conf/config/main.cf:

```
# hacf -verify /etc/VRTSvcs/conf/config
```

- 9 Using rcp or another utility, copy the VCS configuration file from a node (for example, sys1) to the remaining cluster nodes.

For example, on each remaining node, enter:

```
# rcp sys1:/etc/VRTSvcs/conf/config/main.cf \  
/etc/VRTSvcs/conf/config
```

- 10 Start the I/O fencing driver and VCS. Perform the following steps on each node:

- Start the I/O fencing driver.

The vxfen startup script also invokes the vxfenconfig command, which configures the vxfen driver to start and use the coordination points that are listed in /etc/vxfentab.

```
# svcadm enable vxfen
```

- Start VCS.

```
# /opt/VRTS/bin/hastart
```


Verifying I/O fencing configuration

Verify from the `vxfenadm` output that the SCSI-3 disk policy reflects the configuration in the `/etc/vxfenmode` file.

To verify I/O fencing configuration

- 1 On one of the nodes, type:

```
# vxfenadm -d
```

Output similar to the following appears if the fencing mode is SCSI3 and the SCSI3 disk policy is `dmp`:

```
I/O Fencing Cluster Information:  
=====
```

```
Fencing Protocol Version: 201  
Fencing Mode: SCSI3  
Fencing SCSI3 Disk Policy: dmp  
Cluster Members:
```

```
* 0 (sys1)  
1 (sys2)
```

```
RFSM State Information:  
node 0 in state 8 (running)  
node 1 in state 8 (running)
```

- 2 Verify that the disk-based I/O fencing is using the specified disks.

```
# vxfenconfig -l
```

Setting up server-based I/O fencing using installsvs

You can configure server-based I/O fencing for the Symantec VirtualStore cluster using the `installsvs`.

With server-based fencing, you can have the coordination points in your configuration as follows:

- Combination of CP servers and SCSI-3 compliant coordinator disks
- CP servers only

Symantec also supports server-based fencing with a single highly available CP server that acts as a single coordination point.

See [“About planning to configure I/O fencing”](#) on page 71.

See [“Recommended CP server configurations”](#) on page 76.

This section covers the following example procedures:

Mix of CP servers and coordinator disks See [“To configure server-based fencing for the Symantec VirtualStore cluster \(one CP server and two coordinator disks\)”](#) on page 138.

Single CP server See [“To configure server-based fencing for the Symantec VirtualStore cluster \(single CP server\)”](#) on page 143.

To configure server-based fencing for the Symantec VirtualStore cluster (one CP server and two coordinator disks)

1 Depending on the server-based configuration model in your setup, make sure of the following:

- CP servers are configured and are reachable from the Symantec VirtualStore cluster. The Symantec VirtualStore cluster is also referred to as the application cluster or the client cluster.

See [“Setting up the CP server”](#) on page 79.

- The coordination disks are verified for SCSI3-PR compliance.

See [“Checking shared disks for I/O fencing”](#) on page 127.

2 Start the installsvs with the `-fencing` option.

```
# /opt/VRTS/install/installsvs<version> -fencing
```

Where `<version>` is the specific release version. The `installsvs` starts with a copyright message and verifies the cluster information.

See [“About the Veritas installer”](#) on page 41.

Note the location of log files which you can access in the event of any problem with the configuration process.

3 Confirm that you want to proceed with the I/O fencing configuration at the prompt.

The program checks that the local node running the script can communicate with remote nodes and checks whether Symantec VirtualStore 6.0.1 is configured properly.

4 Review the I/O fencing configuration options that the program presents. Type `1` to configure server-based I/O fencing.

```
Select the fencing mechanism to be configured in this  
Application Cluster [1-4,b,q] 1
```

- 5** Make sure that the storage supports SCSI3-PR, and answer `y` at the following prompt.

```
Does your storage environment support SCSI3 PR? [y,n,q] (y)
```

- 6** Provide the following details about the coordination points at the installer prompt:

- Enter the total number of coordination points including both servers and disks. This number should be at least 3.

```
Enter the total number of co-ordination points including both
Coordination Point servers and disks: [b] (3)
```

- Enter the total number of coordinator disks among the coordination points.

```
Enter the total number of disks among these:
[b] (0) 2
```

- 7** Provide the following CP server details at the installer prompt:

- Enter the total number of virtual IP addresses or the total number of fully qualified host names for each of the CP servers.

```
Enter the total number of Virtual IP addresses or fully
qualified host name for the
Coordination Point Server #1: [b,q,?] (1) 2
```

- Enter the virtual IP addresses or the fully qualified host name for each of the CP servers. The installer assumes these values to be identical as viewed from all the application cluster nodes.

```
Enter the Virtual IP address or fully qualified host name
#1 for the Coordination Point Server #1:
[b] 10.209.80.197
```

The installer prompts for this information for the number of virtual IP addresses you want to configure for each CP server.

- Enter the port that the CP server would be listening on.

```
Enter the port in the range [49152, 65535] which the
Coordination Point Server 10.209.80.197
would be listening on or simply accept the default port suggested:
[b] (14250)
```

8 Provide the following coordinator disks-related details at the installer prompt:

- Enter the I/O fencing disk policy for the coordinator disks.

```
Enter disk policy for the disk(s) (raw/dmp):  
[b,q,?] raw
```

- Choose the coordinator disks from the list of available disks that the installer displays. Ensure that the disk you choose is available from all the Symantec VirtualStore (application cluster) nodes.

The number of times that the installer asks you to choose the disks depends on the information that you provided in step 6. For example, if you had chosen to configure two coordinator disks, the installer asks you to choose the first disk and then the second disk:

```
Select disk number 1 for co-ordination point  
  
1) c1t1d0s2  
2) c2t1d0s2  
3) c3t1d0s2
```

```
Please enter a valid disk which is available from all the  
cluster nodes for co-ordination point [1-3,q] 1
```

- If you have not already checked the disks for SCSI-3 PR compliance in step 1, check the disks now.
The installer displays a message that recommends you to verify the disks in another window and then return to this configuration procedure. Press Enter to continue, and confirm your disk selection at the installer prompt.
- Enter a disk group name for the coordinator disks or accept the default.

```
Enter the disk group name for coordinating disk(s):  
[b] (vxsfencoordg)
```

9 Verify and confirm the coordination points information for the fencing configuration.

For example:

```
Total number of coordination points being used: 3
Coordination Point Server ([VIP or FQHN]:Port):
  1. 10.109.80.197 ([10.109.80.197]:14250)
SCSI-3 disks:
  1. c1t1d0s2
  2. c2t1d0s2
Disk Group name for the disks in customized fencing: vxfencoorddg
Disk policy used for customized fencing: raw
```

The installer initializes the disks and the disk group and departs the disk group on the Symantec VirtualStore (application cluster) node.

10 If the CP server is configured for security, the installer sets up secure communication between the CP server and the Symantec VirtualStore (application cluster).

After the installer establishes trust between the authentication brokers of the CP servers and the application cluster nodes, press Enter to continue.

11 Verify and confirm the I/O fencing configuration information.

```
CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: clus1
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
```

- 12 Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the `/etc/vxfenmode` file with the appropriate details in each of the application cluster nodes.

```
Updating client cluster information on Coordination Point Server 10.210.80.197
Adding the client cluster to the Coordination Point Server 10.210.80.197 ..... Done
Registering client node sys1 with Coordination Point Server 10.210.80.197..... Done
Adding CPClient user for communicating to Coordination Point Server 10.210.80.197 .... Done
Adding cluster clus1 to the CPClient user on Coordination Point Server 10.210.80.197 .. Done
Registering client node sys2 with Coordination Point Server 10.210.80.197 ..... Done
Adding CPClient user for communicating to Coordination Point Server 10.210.80.197 .... Done
Adding cluster clus1 to the CPClient user on Coordination Point Server 10.210.80.197 ..Done
Updating /etc/vxfenmode file on sys1 ..... Done
Updating /etc/vxfenmode file on sys2 ..... Done
```

See [“About I/O fencing configuration files”](#) on page 403.

- 13 Review the output as the installer stops and restarts the VCS and the fencing processes on each application cluster node, and completes the I/O fencing configuration.
- 14 Configure the CP agent on the Symantec VirtualStore (application cluster). The Coordination Point Agent monitors the registrations on the coordination points.

```
Do you want to configure Coordination Point Agent on
the client cluster? [y,n,q] (y)
```

```
Enter a non-existing name for the service group for
Coordination Point Agent: [b] (vxfen)
```

- 15** Additionally the coordination point agent can also monitor changes to the Coordinator Disk Group constitution such as a disk being accidentally deleted from the Coordinator Disk Group. The frequency of this detailed monitoring can be tuned with the LevelTwoMonitorFreq attribute. For example, if you set this attribute to 5, the agent will monitor the Coordinator Disk Group constitution every five monitor cycles.

Note that for the LevelTwoMonitorFreq attribute to be applicable there must be disks as part of the Coordinator Disk Group.

```
Enter the value of the LevelTwoMonitorFreq attribute: (5)
```

```
Adding Coordination Point Agent via sys1 .... Done
```

- 16** Note the location of the configuration log files, summary files, and response files that the installer displays for later use.

To configure server-based fencing for the Symantec VirtualStore cluster (single CP server)

- 1** Make sure that the CP server is configured and is reachable from the Symantec VirtualStore cluster. The Symantec VirtualStore cluster is also referred to as the application cluster or the client cluster.
- 2** See [“Setting up the CP server”](#) on page 79.
- 3** Start the installsvs with `-fencing` option.

```
# /opt/VRTS/install/installsvs<version> -fencing
```

Where <version> is the specific release version. The installsvs starts with a copyright message and verifies the cluster information.

See [“About the Veritas installer”](#) on page 41.

Note the location of log files which you can access in the event of any problem with the configuration process.

- 4** Confirm that you want to proceed with the I/O fencing configuration at the prompt.

The program checks that the local node running the script can communicate with remote nodes and checks whether Symantec VirtualStore 6.0.1 is configured properly.

- 5** Review the I/O fencing configuration options that the program presents. Type **1** to configure server-based I/O fencing.

```
Select the fencing mechanism to be configured in this
Application Cluster [1-4,b,q] 1
```

- 6 Make sure that the storage supports SCSI3-PR, and answer `y` at the following prompt.

```
Does your storage environment support SCSI3 PR? [y,n,q] (y)
```

- 7 Enter the total number of coordination points as `1`.

```
Enter the total number of co-ordination points including both  
Coordination Point servers and disks: [b] (3) 1
```

Read the installer warning carefully before you proceed with the configuration.

- 8 Provide the following CP server details at the installer prompt:
 - Enter the total number of virtual IP addresses or the total number of fully qualified host names for each of the CP servers.

```
Enter the total number of Virtual IP addresses or fully  
qualified host name for the  
Coordination Point Server #1: [b,q,?] (1) 2
```

- Enter the virtual IP address or the fully qualified host name for the CP server. The installer assumes these values to be identical as viewed from all the application cluster nodes.

```
Enter the Virtual IP address or fully qualified host name  
#1 for the Coordination Point Server #1:  
[b] 10.209.80.197
```

The installer prompts for this information for the number of virtual IP addresses you want to configure for each CP server.

- Enter the port that the CP server would be listening on.

```
Enter the port in the range [49152, 65535] which the  
Coordination Point Server 10.209.80.197  
would be listening on or simply accept the default  
port suggested: [b] (14250)
```

- 9 Verify and confirm the coordination points information for the fencing configuration.

For example:

```
Total number of coordination points being used: 1  
Coordination Point Server ([VIP or FQHN]:Port):  
1. 10.109.80.197 ([10.109.80.197]:14250)
```


- 10** If the CP server is configured for security, the installer sets up secure communication between the CP server and the Symantec VirtualStore (application cluster).

After the installer establishes trust between the authentication brokers of the CP servers and the application cluster nodes, press Enter to continue.

- 11** Verify and confirm the I/O fencing configuration information.

```
CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: clus1
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
```

- 12** Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the `/etc/vxfenmode` file with the appropriate details in each of the application cluster nodes.

The installer also populates the `/etc/vxfenmode` file with the entry `single_cp=1` for such single CP server fencing configuration.

```
Updating client cluster information on Coordination Point Server 10.210.80.197

Adding the client cluster to the Coordination Point Server 10.210.80.197 ..... Done

Registering client node sys1 with Coordination Point Server 10.210.80.197..... Done
Adding CPClient user for communicating to Coordination Point Server 10.210.80.197 .... Done
Adding cluster clus1 to the CPClient user on Coordination Point Server 10.210.80.197 .. Done

Registering client node sys2 with Coordination Point Server 10.210.80.197 ..... Done
Adding CPClient user for communicating to Coordination Point Server 10.210.80.197 .... Done
Adding cluster clus1 to the CPClient user on Coordination Point Server 10.210.80.197 .. Done

Updating /etc/vxfenmode file on sys1 ..... Done
Updating /etc/vxfenmode file on sys2 ..... Done
```

See [“About I/O fencing configuration files”](#) on page 403.

- 13** Review the output as the installer stops and restarts the VCS and the fencing processes on each application cluster node, and completes the I/O fencing configuration.

14 Configure the CP agent on the Symantec VirtualStore (application cluster).

```
Do you want to configure Coordination Point Agent on the
client cluster? [y,n,q] (y)
```

```
Enter a non-existing name for the service group for
Coordination Point Agent: [b] (vxfen)
```

```
Adding Coordination Point Agent via sys1 ... Done
```

15 Note the location of the configuration log files, summary files, and response files that the installer displays for later use.

Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsvs

If you have installed VCS in virtual environments that do not support SCSI-3 PR-compliant storage, you can configure non-SCSI-3 fencing.

To configure I/O fencing using the installsvs in a non-SCSI-3 PR-compliant setup

- 1 Start the installsvs with `-fencing` option.

```
# /opt/VRTS/install/installsvs<version> -fencing
```

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

The installsvs starts with a copyright message and verifies the cluster information.

- 2 Confirm that you want to proceed with the I/O fencing configuration at the prompt.

The program checks that the local node running the script can communicate with remote nodes and checks whether Symantec VirtualStore 6.0.1 is configured properly.

- 3 Review the I/O fencing configuration options that the program presents. Type **1** to configure server-based I/O fencing.

```
Select the fencing mechanism to be configured in this
Application Cluster
[1-4,b,q] 1
```

Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsvs

- 4** Enter **n** to confirm that your storage environment does not support SCSI-3 PR.

```
Does your storage environment support SCSI3 PR?
[y,n,q] (y) n
```

- 5** Confirm that you want to proceed with the non-SCSI-3 I/O fencing configuration at the prompt.
- 6** Enter the number of CP server coordination points you want to use in your setup.
- 7** Enter the following details for each CP server:
- Enter the virtual IP address or the fully qualified host name.
 - Enter the port address on which the CP server listens for connections. The default value is 14250. You can enter a different port address. Valid values are between 49152 and 65535.

The installer assumes that these values are identical from the view of the SVS cluster nodes that host the applications for high availability.

- 8** Verify and confirm the CP server information that you provided.
- 9** Verify and confirm the SVS cluster configuration information.

Review the output as the installer performs the following tasks:

- Updates the CP server configuration files on each CP server with the following details:
 - Registers each node of the SVS cluster with the CP server.
 - Adds CP server user to the CP server.
 - Adds SVS cluster to the CP server user.
- Updates the following configuration files on each node of the SVS cluster
 - `/etc/vxfenmode` file
 - `/etc/default/vxfen` file
 - `/etc/vxenviron` file
 - `/etc/llttab` file
 - `/etc/vxfentab`

10 Review the output as the installer stops Symantec VirtualStore on each node, starts I/O fencing on each node, updates the VCS configuration file `main.cf`, and restarts Symantec VirtualStore with non-SCSI-3 server-based fencing.

Confirm to configure the CP agent on the SVS cluster.

11 Confirm whether you want to send the installation information to Symantec.

12 After the installer configures I/O fencing successfully, note the location of summary, log, and response files that installer creates.

The files provide useful information which can assist you with the configuration, and can also assist future configurations.

Setting up server-based I/O fencing manually

Tasks that are involved in setting up server-based I/O fencing manually include:

Table 9-2 Tasks to set up server-based I/O fencing manually

Task	Reference
Preparing the CP servers for use by the Symantec VirtualStore cluster	See “Preparing the CP servers manually for use by the SVS cluster” on page 148.
Modifying I/O fencing configuration files to configure server-based I/O fencing	See “Configuring server-based fencing on the SVS cluster manually” on page 151.
Modifying Symantec VirtualStore configuration to use I/O fencing	See “Modifying VCS configuration to use I/O fencing” on page 135.
Configuring Coordination Point agent to monitor coordination points	See “Configuring CoordPoint agent to monitor coordination points” on page 157.
Verifying the server-based I/O fencing configuration	See “Verifying server-based I/O fencing configuration” on page 159.

Preparing the CP servers manually for use by the SVS cluster

Use this procedure to manually prepare the CP server for use by the SVS cluster or clusters.

[Table 9-3](#) displays the sample values used in this procedure.

Table 9-3 Sample values in procedure

CP server configuration component	Sample name
CP server	cps1
Node #1 - SVS cluster	sys1
Node #2 - SVS cluster	sys2
Cluster name	clus1
Cluster UUID	{f0735332-1dd1-11b2}

To manually configure CP servers for use by the SVS cluster

- 1** Determine the cluster name and uuid on the SVS cluster.

For example, issue the following commands on one of the SVS cluster nodes (sys1):

```
# grep cluster /etc/VRTSvcs/conf/config/main.cf

cluster clus1

# cat /etc/vx/.uuids/clusuuid

{f0735332-1dd1-11b2-bb31-00306eea460a}
```

- 2** Use the `cpsadm` command to check whether the SVS cluster and nodes are present in the CP server.

For example:

```
# cpsadm -s cps1.symantecexample.com -a list_nodes

ClusName  UUID                               Hostname(Node ID) Registered
clus1     {f0735332-1dd1-11b2-bb31-00306eea460a} sys1(0)           0
clus1     {f0735332-1dd1-11b2-bb31-00306eea460a} sys2(1)           0
```

If the output does not show the cluster and nodes, then add them as described in the next step.

For detailed information about the `cpsadm` command, see the *Symantec VirtualStore Administrator's Guide*.

3 Add the SVS cluster and nodes to each CP server.

For example, issue the following command on the CP server (cps1.symantecexample.com) to add the cluster:

```
# cpsadm -s cps1.symantecexample.com -a add_clus\  
-c clus1 -u {f0735332-1dd1-11b2}
```

```
Cluster clus1 added successfully
```

Issue the following command on the CP server (cps1.symantecexample.com) to add the first node:

```
# cpsadm -s cps1.symantecexample.com -a add_node\  
-c clus1 -u {f0735332-1dd1-11b2} -h sys1 -n0
```

```
Node 0 (sys1) successfully added
```

Issue the following command on the CP server (cps1.symantecexample.com) to add the second node:

```
# cpsadm -s cps1.symantecexample.com -a add_node\  
-c clus1 -u {f0735332-1dd1-11b2} -h sys2 -n1
```

```
Node 1 (sys2) successfully added
```

4 If security is to be enabled, check whether the CPSADM@VCS_SERVICES@*cluster_uid* users are created in the CP server.

If the output below does not show the users, then add them as described in the next step.

```
# cpsadm -s cps1.symantecexample.com -a list_users
```

```
Username/Domain Type Cluster Name / UUID Role  
  
CPSADM@VCS_SERVICES@f0735332-1dd1-11b2/vx  
clus1/{f0735332-1dd1-11b2} Operator
```

If security is to be disabled, then add the user name "cpsclient@hostname" to the server instead of the CPSADM@VCS_SERVICES@*cluster_uid* (for example, cpsclient@sys1).

The CP server can only run in either secure mode or non-secure mode, both connections are not accepted at the same time.

5 Add the users to the CP server.

Issue the following commands on the CP server (cps1.symantecexample.com):

```
# cpsadm -s cps1.symantecexample.com -a add_user -e\  
CPSADM@VCS_SERVICES@cluster_uuid\  
-f cps_operator -g vx
```

```
User CPSADM@VCS_SERVICES@cluster_uuid  
successfully added
```

6 Authorize the CP server user to administer the SVS cluster. You must perform this task for the CP server users corresponding to each node in the SVS cluster.

For example, issue the following command on the CP server (cps1.symantecexample.com) for SVS cluster clus1 with two nodes sys1 and sys2:

```
# cpsadm -s cps1.symantecexample.com -a\  
add_clus_to_user -c clus1\  
-u {f0735332-1dd1-11b2}\  
-e CPSADM@VCS_SERVICES@cluster_uuid\  
-f cps_operator -g vx
```

```
Cluster successfully added to user  
CPSADM@VCS_SERVICES@cluster_uuid privileges.
```

Configuring server-based fencing on the SVS cluster manually

The configuration process for the client or SVS cluster to use CP server as a coordination point requires editing the `/etc/vxfenmode` file.

You need to edit this file to specify the following information for your configuration:

- Fencing mode
- Fencing mechanism
- Fencing disk policy (if applicable to your I/O fencing configuration)
- Appropriate value for the security configuration
- CP server or CP servers
- Coordinator disk group (if applicable to your I/O fencing configuration)

Note: Whenever coordinator disks are used as coordination points in your I/O fencing configuration, you must create a disk group (vxfencoordg). You must specify this disk group in the `/etc/vxfenmode` file.

See [“Setting up coordinator disk groups”](#) on page 133.

The customized fencing framework also generates the `/etc/vxfentab` file which has security setting and the coordination points (all the CP servers and disks from disk group specified in `/etc/vxfenmode` file).

To configure server-based fencing on the SVS cluster manually

- 1 Use a text editor to edit the following file on each node in the cluster:

```
/etc/default/vxfen
```

You must change the values of the `VXFEN_START` and the `VXFEN_STOP` environment variables to 1.

- 2 Use a text editor to edit the `/etc/vxfenmode` file values to meet your configuration specifications.

If your server-based fencing configuration uses a single highly available CP server as its only coordination point, make sure to add the `single_cp=1` entry in the `/etc/vxfenmode` file.

The following sample file output displays what the `/etc/vxfenmode` file contains:

See [“Sample vxfenmode file output for server-based fencing”](#) on page 152.

- 3 After editing the `/etc/vxfenmode` file, run the `vxfen` init script to start fencing.

For example:

```
# svcadm enable vxfen
```

- 4 Make sure that `/etc/vxfenmode` file contains the value of security is set to 1.

Make sure that following command displays the certificate being used by `cpsadm` client,

```
EAT_DATA_DIR=/vat/VRTSvcs/vcsauth/data/CPSADM cpsat showcred
```

Sample vxfenmode file output for server-based fencing

The following is a sample `vxfenmode` file for server-based fencing:


```
#
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=customized

# vxfen_mechanism determines the mechanism for customized I/O
# fencing that should be used.
#
# available options:
# cps        - use a coordination point server with optional script
#              controlled scsi3 disks
# security - 1
# security - 0

vxfen_mechanism=cps

#
# scsi3_disk_policy determines the way in which I/O Fencing
# communicates with the coordination disks. This field is
# required only if customized coordinator disks are being used.
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
scsi3_disk_policy=dmp

# security when enabled uses secure communication to the cp server
# using VxAT (Veritas Authentication Service)
# available options:
# 0 - don't use Veritas Authentication Service for cp server
#    communication
# 1 - use Veritas Authentication Service for cp server
#    communication
security=1

#
# Specify 3 or more odd number of coordination points in this file,
```

```
# one in its own line. They can be all-CP servers, all-SCSI-3
# compliant coordinator disks, or a combination of CP servers and
# SCSI-3 compliant coordinator disks. Please ensure that the CP
# server coordination points are numbered sequentially and in the
# same order on all the cluster nodes.
#
# Coordination Point Server(CPS) is specified as:
#
# cps<number>=[<vip/vhn>]:<port>
#
# If a CPS supports multiple virtual IPs or virtual hostnames over
# different subnets, all of the IPs/names can be specified in a
# comma separated list as follows:
#
# cps<number>=[<vip_1/vhn_1>]:<port_1>,[<vip_2/vhn_2>]:<port_2>,...,
# [<vip_n/vhn_n>]:<port_n>
#
# Where,
# <number>
# is the serial number of the CPS as a coordination point; must
# start with 1.
# <vip>
# is the virtual IP address of the CPS, must be specified in
# square brackets ("[]").
# <vhn>
# is the virtual hostname of the CPS, must be specified in square
# brackets ("[]").
# <port>
# is the port number bound to a particular <vip/vhn> of the CPS.
# It is optional to specify a <port>. However, if specified, it
# must follow a colon (":") after <vip/vhn>. If not specified, the
# colon (":") must not exist after <vip/vhn>.
#
# For all the <vip/vhn>s which do not have a specified <port>, a
# default port can be specified as follows:
#
# port=<default_port>
#
# Where <default_port> is applicable to all the <vip/vhn>s for
# which a <port> is not specified. In other words, specifying <port>
# with a <vip/vhn> overrides the <default_port> for that <vip/vhn>.
# If the <default_port> is not specified, and there are <vip/vhn>s for
# which <port> is not specified, then port number 14250 will be used
```

```
# for such <vip/vhn>s.
#
# Example of specifying CP Servers to be used as coordination points:
# port=57777
# cps1=[192.168.0.23],[192.168.0.24]:58888,[cps1.company.com]
# cps2=[192.168.0.25]
# cps3=[cps2.company.com]:59999
#
# In the above example,
# - port 58888 will be used for vip [192.168.0.24]
# - port 59999 will be used for vhn [cps2.company.com], and
# - default port 57777 will be used for all remaining <vip/vhn>s:
#   [192.168.0.23]
#   [cps1.company.com]
#   [192.168.0.25]
# - if default port 57777 were not specified, port 14250 would be used
#   for all remaining <vip/vhn>s:
#   [192.168.0.23]
#   [cps1.company.com]
#   [192.168.0.25]
#
# SCSI-3 compliant coordinator disks are specified as:
#
# vxfendg=<coordinator disk group name>
# Example:
# vxfendg=vxfencoordg
#
# Examples of different configurations:
# 1. All CP server coordination points
# cps1=
# cps2=
# cps3=
#
# 2. A combination of CP server and a disk group having two SCSI-3
# coordinator disks
# cps1=
# vxfendg=
# Note: The disk group specified in this case should have two disks
#
# 3. All SCSI-3 coordinator disks
# vxfendg=
# Note: The disk group specified in case should have three disks
#
```

Table 9-4 defines the vxfenmode parameters that must be edited.

Table 9-4 vxfenmode file parameters

vxfenmode File Parameter	Description
vxfen_mode	Fencing mode of operation. This parameter must be set to “customized”.
vxfen_mechanism	Fencing mechanism. This parameter defines the mechanism that is used for fencing. If one of the three coordination points is a CP server, then this parameter must be set to “cps”.
scsi3_disk_policy	Configure the vxfen module to use either DMP devices, "dmp" or the underlying raw character devices, "raw". Note: The configured disk policy is applied on all the nodes.
security	Security parameter 1 indicates that secure mode is used for CP server communications. Security parameter 0 indicates that communication with the CP server is made in non-secure mode. The default security value is 1.
fips_mode	[For future use] Set the value to 0.
cps1, cps2, or vxfendg	Coordination point parameters. Enter either the virtual IP address or the FQHN (whichever is accessible) of the CP server. <i>cps<number>=[virtual_ip_address/virtual_host_name]:port</i> Where <i>port</i> is optional. The default port value is 14250. If you have configured multiple virtual IP addresses or host names over different subnets, you can specify these as comma-separated values. For example: <i>cps1=[192.168.0.23], [192.168.0.24]:58888, [cps1.company.com]</i> Note: Whenever coordinator disks are used in an I/O fencing configuration, a disk group has to be created (vxfencoordg) and specified in the /etc/vxfenmode file. Additionally, the customized fencing framework also generates the /etc/vxfentab file which specifies the security setting and the coordination points (all the CP servers and the disks from disk group specified in /etc/vxfenmode file).

Table 9-4 vxfenmode file parameters (*continued*)

vxfenmode File Parameter	Description
port	<p>Default port for the CP server to listen on.</p> <p>If you have not specified port numbers for individual virtual IP addresses or host names, the default port number value that the CP server uses for those individual virtual IP addresses or host names is 14250. You can change this default port value using the port parameter.</p>
single_cp	<p>Value 1 for single_cp parameter indicates that the server-based fencing uses a single highly available CP server as its only coordination point.</p> <p>Value 0 for single_cp parameter indicates that the server-based fencing uses at least three coordination points.</p>

Configuring CoordPoint agent to monitor coordination points

The following procedure describes how to manually configure the CoordPoint agent to monitor coordination points.

The CoordPoint agent can monitor CP servers and SCSI-3 disks.

See the *Veritas Cluster Server Bundled Agents Reference Guide* for more information on the agent.

To configure CoordPoint agent to monitor coordination points

- 1 Ensure that your SVS cluster has been properly installed and configured with fencing enabled.
- 2 Create a parallel service group vxfen and add a coordpoint resource to the vxfen service group using the following commands:

```
# haconf -makerw
# hagrps -add vxfen
# hagrps -modify vxfen SystemList sys1 0 sys2 1
# hagrps -modify vxfen AutoFailOver 0
# hagrps -modify vxfen Parallel 1
# hagrps -modify vxfen SourceFile "./main.cf"
# hares -add coordpoint CoordPoint vxfen
# hares -modify coordpoint FaultTolerance 0
# hares -override coordpoint LevelTwoMonitorFreq
# hares -modify coordpoint LevelTwoMonitorFreq 5
# hares -modify coordpoint Enabled 1
# haconf -dump -makero
```

- 3 Verify the status of the agent on the SVS cluster using the `hares` commands. For example:

```
# hares -state coordpoint
```

The following is an example of the command and output::

```
# hares -state coordpoint

# Resource      Attribute  System  Value
coordpoint     State     sys1    ONLINE
coordpoint     State     sys2    ONLINE
```

- 4 Access the engine log to view the agent log. The agent log is written to the engine log.

The agent log contains detailed CoordPoint agent monitoring information; including information about whether the CoordPoint agent is able to access all the coordination points, information to check on which coordination points the CoordPoint agent is reporting missing keys, etc.

To view the debug logs in the engine log, change the `dbg` level for that node using the following commands:

```
# haconf -makerw

# hatype -modify Coordpoint LogDbg 10

# haconf -dump -makero
```

The agent log can now be viewed at the following location:

```
/var/VRTSvcs/log/engine_A.log
```

Verifying server-based I/O fencing configuration

Follow the procedure described below to verify your server-based I/O fencing configuration.

To verify the server-based I/O fencing configuration

- 1 Verify that the I/O fencing configuration was successful by running the `vxfenadm` command. For example, run the following command:

```
# vxfenadm -d
```

Note: For troubleshooting any server-based I/O fencing configuration issues, refer to the *Symantec VirtualStore Administrator's Guide*.

- 2 Verify that I/O fencing is using the specified coordination points by running the `vxfenconfig` command. For example, run the following command:

```
# vxfenconfig -l
```

If the output displays `single_cp=1`, it indicates that the application cluster uses a CP server as the single coordination point for server-based fencing.

Setting up non-SCSI-3 fencing in virtual environments manually

To manually set up I/O fencing in a non-SCSI-3 PR compliant setup

- 1 Configure I/O fencing in customized mode with only CP servers as coordination points.

See [“Setting up server-based I/O fencing manually”](#) on page 148.

- 2 Make sure that the Symantec VirtualStore cluster is online and check that the fencing mode is customized.

```
# vxfenadm -d
```

- 3 Make sure that the cluster attribute `UseFence` is set to `SCSI3`.

```
# haclus -value UseFence
```

- 4 On each node, edit the `/etc/vxenvron` file as follows:

```
data_disk_fencing=off
```

- 5 On each node, edit the `/kernel/drv/vxfen.conf` file as follows:

```
vxfen_vxfnd_tmt=25
```


- 6** On each node, edit the `/etc/vxfenmode` file as follows:

```
loser_exit_delay=55
vxfen_script_timeout=25
```

Refer to the sample `/etc/vxfenmode` file.

- 7** On each node, set the value of the LLT `sendhbcap` timer parameter value as follows:

- Run the following command:

```
lltconfig -T sendhbcap:3000
```

- Add the following line to the `/etc/llttab` file so that the changes remain persistent after any reboot:

```
set-timer senhbcap:3000
```

- 8** On any one node, edit the VCS configuration file as follows:

- Make the VCS configuration file writable:

```
# haconf -makerw
```

- For each resource of the type `DiskGroup`, set the value of the `MonitorReservation` attribute to 0 and the value of the `Reservation` attribute to `NONE`.

```
# hares -modify <dg_resource> MonitorReservation 0
```

```
# hares -modify <dg_resource> Reservation "NONE"
```

- Run the following command to verify the value:

```
# hares -list Type=DiskGroup MonitorReservation!=0
```

```
# hares -list Type=DiskGroup Reservation!="NONE"
```

The command should not list any resources.

- Modify the default value of the `Reservation` attribute at type-level.

```
# haattr -default DiskGroup Reservation "NONE"
```

- Make the VCS configuration file read-only

```
# haconf -dump -makero
```

- 9 Make sure that the UseFence attribute in the VCS configuration file main.cf is set to SCSI3.
- 10 To make these VxFEN changes take effect, stop and restart VxFEN and the dependent modules
 - On each node, run the following command to stop VCS:

```
# svcadm disable -t vcs
```
 - After VCS takes all services offline, run the following command to stop VxFEN:

```
# svcadm disable -t vxfen
```
 - On each node, run the following commands to restart VxFEN and VCS:

```
# svcadm enable vxfen
```

Sample /etc/vxfenmode file for non-SCSI-3 fencing

```
=====
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=customized

# vxfen_mechanism determines the mechanism for customized I/O
# fencing that should be used.
#
# available options:
# cps        - use a coordination point server with optional script
#              controlled scsi3 disks
#
vxfen_mechanism=cps

#
# scsi3_disk_policy determines the way in which I/O Fencing
# communicates with the coordination disks. This field is required
# only if customized coordinator disks are being used.
```

```

#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
# scsi3_disk_policy=dmp

#
# Seconds for which the winning sub cluster waits to allow for the
# losing subcluster to panic & drain I/Os. Useful in the absence of
# SCSI3 based data disk fencing
loser_exit_delay=55

#
# Seconds for which vxfsend process wait for a customized fencing
# script to complete. Only used with vxfsend_mode=customized
vxfsend_script_timeout=25

#
# security when enabled uses secure communication to the cp server
# using VxAT (Veritas Authentication Service)
# available options:
# 0 - don't use Veritas Authentication Service for cp server
#   communication
# 1 - use Veritas Authentication Service for cp server
#   communication
security=1

#
# Specify 3 or more odd number of coordination points in this file,
# one in its own line. They can be all-CP servers, all-SCSI-3
# compliant coordinator disks, or a combination of CP servers and
# SCSI-3 compliant coordinator disks. Please ensure that the CP
# server coordination points are numbered sequentially and in the
# same order on all the cluster nodes.
#
# Coordination Point Server(CPS) is specified as:
#
# cps<number>=[<vip/vhn>]:<port>
#
# If a CPS supports multiple virtual IPs or virtual hostnames over
# different subnets, all of the IPs/names can be specified in a
# comma separated list as follows:

```

```
#  
# cps<number>=[<vip_1/vhn_1>]:<port_1>,[<vip_2/vhn_2>]:<port_2>,...,  
#  [<vip_n/vhn_n>]:<port_n>  
#  
# Where,  
# <number>  
# is the serial number of the CPS as a coordination point; must  
# start with 1.  
# <vip>  
# is the virtual IP address of the CPS, must be specified in  
# square brackets ("[]").  
# <vhn>  
# is the virtual hostname of the CPS, must be specified in square  
# brackets ("[]").  
# <port>  
# is the port number bound to a particular <vip/vhn> of the CPS.  
# It is optional to specify a <port>. However, if specified, it  
# must follow a colon (":") after <vip/vhn>. If not specified, the  
# colon (":") must not exist after <vip/vhn>.  
#  
# For all the <vip/vhn>s which do not have a specified <port>, a  
# default port can be specified as follows:  
#  
# port=<default_port>  
#  
# Where <default_port> is applicable to all the <vip/vhn>s for  
# which a <port> is not specified. In other words, specifying <port>  
# with a <vip/vhn> overrides the <default_port> for that <vip/vhn>.  
# If the <default_port> is not specified, and there are <vip/vhn>s for  
# which <port> is not specified, then port number 14250 will be used  
# for such <vip/vhn>s.  
#  
# Example of specifying CP Servers to be used as coordination points:  
# port=57777  
# cps1=[192.168.0.23],[192.168.0.24]:58888,[cps1.company.com]  
# cps2=[192.168.0.25]  
# cps3=[cps2.company.com]:59999  
#  
# In the above example,  
# - port 58888 will be used for vip [192.168.0.24]  
# - port 59999 will be used for vhn [cps2.company.com], and  
# - default port 57777 will be used for all remaining <vip/vhn>s:  
#   [192.168.0.23]
```

```

# [cps1.company.com]
# [192.168.0.25]
# - if default port 57777 were not specified, port 14250 would be used
# for all remaining <vip/vhn>s:
# [192.168.0.23]
# [cps1.company.com]
# [192.168.0.25]
#
# SCSI-3 compliant coordinator disks are specified as:
#
# vxfendg=<coordinator disk group name>
# Example:
# vxfendg=vxfencoorddg
#
# Examples of different configurations:
# 1. All CP server coordination points
# cps1=
# cps2=
# cps3=
#
# 2. A combination of CP server and a disk group having two SCSI-3
# coordinator disks
# cps1=
# vxfendg=
# Note: The disk group specified in this case should have two disks
#
# 3. All SCSI-3 coordinator disks
# vxfendg=
# Note: The disk group specified in case should have three disks
#
cps1=[cps1.company.com]
cps2=[cps2.company.com]
cps3=[cps3.company.com]
port=14250
=====

```

Enabling or disabling the preferred fencing policy

You can enable or disable the preferred fencing feature for your I/O fencing configuration.

You can enable preferred fencing to use system-based race policy or group-based race policy. If you disable preferred fencing, the I/O fencing configuration uses the default count-based race policy.

See [“About preferred fencing”](#) on page 26.

To enable preferred fencing for the I/O fencing configuration

- 1 Make sure that the cluster is running with I/O fencing set up.

```
# vxfenadm -d
```

- 2 Make sure that the cluster-level attribute UseFence has the value set to SCSI3.

```
# haclus -value UseFence
```

- 3 To enable system-based race policy, perform the following steps:

- Make the VCS configuration writable.

```
# haconf -makerw
```

- Set the value of the cluster-level attribute PreferredFencingPolicy as System.

```
# haclus -modify PreferredFencingPolicy System
```

- Set the value of the system-level attribute FencingWeight for each node in the cluster.

For example, in a two-node cluster, where you want to assign sys1 five times more weight compared to sys2, run the following commands:

```
# hasys -modify sys1 FencingWeight 50
```

```
# hasys -modify sys2 FencingWeight 10
```

- Save the VCS configuration.

```
# haconf -dump -makero
```

- 4 To enable group-based race policy, perform the following steps:

- Make the VCS configuration writable.

```
# haconf -makerw
```

- Set the value of the cluster-level attribute PreferredFencingPolicy as Group.

```
# haclus -modify PreferredFencingPolicy Group
```

- Set the value of the group-level attribute Priority for each service group. For example, run the following command:

```
# hagrps -modify service_group Priority 1
```

Make sure that you assign a parent service group an equal or lower priority than its child service group. In case the parent and the child service groups are hosted in different subclusters, then the subcluster that hosts the child service group gets higher preference.

- Save the VCS configuration.

```
# haconf -dump -makero
```

- 5 To view the fencing node weights that are currently set in the fencing driver, run the following command:

```
# vxfenconfig -a
```

To disable preferred fencing for the I/O fencing configuration

- 1 Make sure that the cluster is running with I/O fencing set up.

```
# vxfenadm -d
```

- 2 Make sure that the cluster-level attribute UseFence has the value set to SCSI3.

```
# haclus -value UseFence
```

- 3 To disable preferred fencing and use the default race policy, set the value of the cluster-level attribute PreferredFencingPolicy as Disabled.

```
# haconf -makerw
```

```
# haclus -modify PreferredFencingPolicy Disabled
```

```
# haconf -dump -makero
```


Installation using the Web-based installer

- [Chapter 10. Installing Symantec VirtualStore using the Web-based installer](#)
- [Chapter 11. Configuring Symantec VirtualStore](#)

Installing Symantec VirtualStore using the Web-based installer

This chapter includes the following topics:

- [About the Web-based installer](#)
- [Before using the Veritas Web-based installer](#)
- [Starting the Veritas Web-based installer](#)
- [Obtaining a security exception on Mozilla Firefox](#)
- [Performing a pre-installation check with the Veritas Web-based installer](#)
- [Setting installer options with the Web-based installer](#)
- [Installing SVS with the Web-based installer](#)

About the Web-based installer

Use the Web-based installer interface to install Veritas products. The Web-based installer can perform most of the tasks that the script-based installer performs.

You use the `webinstaller` script to start and stop the Veritas XPortal Server `xprtlwid` process. The `webinstaller` script can also be used to check the status of the XPortal Server.

When the `webinstaller` script starts the `xprtlwid` process, the script displays a URL. Use this URL to access the Web-based installer from a Web browser such as Internet Explorer or FireFox.

The Web installer creates log files whenever the Web installer is operating. While the installation processes are operating, the log files are located in a session-based directory under the `/var/tmp` directory. After the install process completes, the log files are located in the `/opt/VRTS/install/logs` directory. It is recommended that you keep these files for auditing, debugging, and future use.

The location of the Veritas XPortal Server configuration file is `/var/opt/webinstaller/xprtlwid.conf`.

See [“Before using the Veritas Web-based installer”](#) on page 172.

See [“Starting the Veritas Web-based installer”](#) on page 172.

Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

Table 10-1 Web-based installer requirements

System	Function	Requirements
Target system	The systems where you plan to install the Veritas products.	Must be a supported platform for 6.0.1.
Installation server	The server where you start the installation. The installation media is accessible from the installation server.	Must use the same operating system as the target systems and must be at one of the supported operating system update levels.
Administrative system	The system where you run the Web browser to perform the installation.	Must have a Web browser. Supported browsers: <ul style="list-style-type: none">■ Internet Explorer 6, 7, and 8■ Firefox 3.x and later

Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

To start the Web-based installer

- 1 Start the Veritas XPortal Server process `xprt1wid`, on the installation server:

```
# ./webinstaller start
```

The webinstaller script displays a URL. Note this URL.

Note: If you do not see the URL, run the command again.

The default listening port is 14172. If you have a firewall that blocks port 14172, use the `-port` option to use a free port instead.

- 2 On the administrative server, start the Web browser.
- 3 Navigate to the URL that the script displayed.
- 4 Certain browsers may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

When prompted, enter `root` and root's password of the installation server.

- 5 Log in as superuser.

Obtaining a security exception on Mozilla Firefox

You may need to get a security exception on Mozilla Firefox.

The following instructions are general. They may change because of the rapid release cycle of Mozilla browsers.

To obtain a security exception

- 1 Click **Or you can add an exception** link.
- 2 Click **I Understand the Risks**, or **You can add an exception**.
- 3 Click **Get Certificate** button.
- 4 Uncheck **Permanently Store this exception checkbox (recommended)**.
- 5 Click **Confirm Security Exception** button.
- 6 Enter `root` in User Name field and root password of the web server in the Password field.

Performing a pre-installation check with the Veritas Web-based installer

This section describes performing a pre-installation check with the Veritas Web-based installer.

To perform a pre-installation check

- 1 Start the Web-based installer.
See [“Starting the Veritas Web-based installer”](#) on page 172.
- 2 On the Select a task and a product page, select **Perform a Pre-installation Check** from the **Task** drop-down list. Select **Veritas Storage Foundation and High Availability** from the **Product** drop-down list and click **Next**.
- 3 Select the Symantec VirtualStore from the **Product** drop-down list, and click **Next**.
- 4 Indicate the systems on which to perform the precheck. Enter one or more system names, separated by spaces. Click **Next**.
- 5 The installer performs the precheck and displays the results.
- 6 If the validation completes successfully, click **Next**. The installer prompts you to begin the installation. Click **Yes** to install on the selected system. Click **No** to install later.
- 7 Click **Finish**. The installer prompts you for another task.

Setting installer options with the Web-based installer

You can use the Web-based installer for certain command-line installer options.

The supported options follow:

- `-serial`
- `-require path_to_hotfix_file`
- `-mediapath directory_path_to_install_media`
- `-logpath directory_path_to_save_logs`
- `-tmppath directory_path_to_save_temp_files`

See [“Installation script options”](#) on page 395.

To use installer options

- 1 On the Web-installer's entry page, click the **Advanced Options** link.
- 2 In the Command line options field, enter the option that you want to use.
For example, if you want to use the serial option and the logpath option, enter:

```
-serial -logpath /opt/VRTS/install/advlogs
```

Where */opt/VRTS/install/advlogs* is the path that you want to use. Separate the command with a space.

- 3 Click the **OK** button and proceed.

Installing SVS with the Web-based installer

This section describes installing SVS with the Veritas Web-based installer.

To install SVS using the Web-based installer

- 1 Perform preliminary steps.
See [“Performing a pre-installation check with the Veritas Web-based installer”](#) on page 174.
- 2 Start the Web-based installer.

Note: The installer displays a warning and asks to install VMware vSphere Perl SDK on all nodes before proceeding to install. You can ignore the warning message and proceed with this step.

See [“Starting the Veritas Web-based installer”](#) on page 172.

- 3 Select **Install a Product** from the **Task** drop-down list.
- 4 Select **Symantec VirtualStore** from the Product drop-down list, and click **Next**.
- 5 On the License agreement page, read the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.
- 6 Select the installation mode: **Typical** or **Custom**.
Typical: automatically configures your SVS after installation with typical settings.
Custom: shows GUI for user inputs for each configuration steps.
- 7 Indicate the systems where you want to install. Separate multiple system names with spaces. Click **Next**.

- 8** If you have not yet configured a communication mode among systems, you have the option to let the installer configure ssh or rsh. If you choose to allow this configuration, select the communication mode and provide the superuser passwords for the systems.
- 9** After the validation completes successfully, click **Next** to install SVS on the selected system.
- 10** The installer prompts you to configure the cluster. Select **Yes** to continue with configuring the product.

If you select **No**, you can exit the installer. You must configure the product before you can use SVS.

After the installation completes, the installer displays the location of the log and summary files. If required, view the files to confirm the installation status.

- 11** If prompted, select the checkbox to specify whether you want to send your installation information to Symantec.

Would you like to send the information about this installation to Symantec to help improve installation in the future?

Click **Finish**. The installer asks if you would like to read the summary file. Select **Yes** to read the summary file. If you select **No**, the installer prompts you for another task.

Configuring Symantec VirtualStore

This chapter includes the following topics:

- [Configuring Symantec VirtualStore using the Web-based installer](#)

Configuring Symantec VirtualStore using the Web-based installer

Before you begin to configure Symantec VirtualStore using the Web-based installer, review the configuration requirements.

By default, the communication between the systems is selected as SSH. If SSH is used for communication between systems, the SSH commands execute without prompting for passwords or confirmations.

You can click **Quit** to quit the Web-installer at any time during the configuration process.

To configure Symantec VirtualStore on a cluster

- 1 Start the Web-based installer.
See [“Starting the Veritas Web-based installer”](#) on page 172.
- 2 On the Select a task and a product page, select the task and the product as follows:

Task	Configure a Product
Product	Symantec VirtualStore

Click **Next**.

- 3 On the Select Systems page, enter the system names where you want to configure Symantec VirtualStore, and click **Next**.

Example: **sys1 sys2**

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

Click **Next** after the installer completes the system verification successfully.

- 4 Choose the mode you would like to configure your product.

If you choose the **Typical** mode, the configuration prompts you only one question about the cluster ID and automatically configuring networks. The cluster ID is the unique cluster ID that you entered during installation.

If you choose the **Custom** mode, then follow the steps below.

- 5 In the Confirmation dialog box that appears, choose whether or not to configure I/O fencing.

To configure I/O fencing, click **Yes**.

To configure I/O fencing later, click **No**. You can configure I/O fencing later using the Web-based installer.

See [“Configuring Symantec VirtualStore for data integrity using the Web-based installer”](#) on page 182.

You can also configure I/O fencing later using the `installsvs<version>-fencing` command, the response files, or manually configure.

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

6 On the Set Cluster Name/ID page, specify the following information for the cluster.

- | | |
|--|---|
| Cluster Name | Enter a unique cluster name. |
| Cluster ID | Enter a unique cluster ID.

Note that you can have the installer check to see if the cluster ID is unique. Symantec recommends that you use the installer to check for duplicate cluster IDs in multi-cluster environments. |
| Check duplicate cluster ID | Select the check box if you want the installer to verify if the given cluster ID is unique in your private network. The verification is performed after you specify the heartbeat details in the following pages. The verification takes some time to complete. |
| LLT Type | Select an LLT type from the list. You can choose to configure LLT over UDP or over Ethernet. |
| Number of Heartbeats | Choose the number of heartbeat links you want to configure. |
| Additional Low Priority Heartbeat NIC | Select the check box if you want to configure a low priority link. The installer configures one heartbeat link as low priority link. |
| Unique Heartbeat NICs per system | For LLT over Ethernet, select the check box if you do not want to use the same NIC details to configure private heartbeat links on other systems.

For LLT over UDP, this check box is selected by default. |

Click **Next**.

7 On the Set Cluster Heartbeat page, select the heartbeat link details for the LLT type you chose on the Set Cluster Name/ID page.

For **LLT over Ethernet**: Do the following:

- If you are using the same NICs on all the systems, select the NIC for each private heartbeat link.
- If you had selected **Unique Heartbeat NICs per system** on the Set Cluster Name/ID page, provide the NIC details for each system.

For **LLT over UDP**: Select the NIC, Port, and IP address for each private heartbeat link. You must provide these details for each system.

Click **Next**.

- 8** On the Optional Configuration page, decide the optional VCS features that you want to configure. Click the corresponding tab to specify the details for each option:

Security

To configure a secure SVS cluster, select the **Configure secure cluster** check box.

If you want to perform this task later, do not select the **Configure secure cluster** check box. You can use the `-security` option of the `installsvs`.

Virtual IP

- Select the **Configure Virtual IP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- Select the interface on which you want to configure the virtual IP.
- Enter a virtual IP address and value for the netmask. You can use an IPv4 or an IPv6 address.

VCS Users

- Reset the password for the Admin user, if necessary.
- Select the **Configure VCS users** option.
- Click **Add** to add a new user.
Specify the user name, password, and user privileges for this user.

SMTP

- Select the **Configure SMTP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- If all the systems use the same NIC, select the NIC for the VCS Notifier to be used on all systems. If not, select the NIC to be used by each system.
- In the **SMTP Server** box, enter the domain-based hostname of the SMTP server. Example: `smtp.yourcompany.com`
- In the **Recipient** box, enter the full email address of the SMTP recipient. Example: `user@yourcompany.com`.
- In the **Event** list box, select the minimum security level of messages to be sent to each recipient.
- Click **Add** to add more SMTP recipients, if necessary.

SNMP

- Select the **Configure SNMP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- If all the systems use the same NIC, select the NIC for the VCS Notifier to be used on all systems. If not, select the NIC to be used by each system.
- In the **SNMP Port** box, enter the SNMP trap daemon port: (162).
- In the **Console System Name** box, enter the SNMP console system name.
- In the **Event** list box, select the minimum security level of messages to be sent to each console.
- Click **Add** to add more SNMP consoles, if necessary.

GCO

If you installed a valid HA/DR license, you can now enter the wide-area heartbeat link details for the global cluster that you would set up later.

- Select the **Configure GCO** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- Select a NIC.
- Enter a virtual IP address and value for the netmask. You can use an IPv4 or an IPv6 address.

Click **Next**.

- 9 On the Stop Processes page, click **Next** after the installer stops all the processes successfully.
- 10 On the Start Processes page, click **Next** after the installer performs the configuration based on the details you provided and starts all the processes successfully.

If you did not choose to configure I/O fencing in step 5, then skip to step 12. Go to step 11 to configure fencing.

11 On the Select Fencing Type page, choose the type of fencing configuration:

- | | |
|--|---|
| Configure Coordination Point client based fencing | Choose this option to configure server-based I/O fencing. |
| Configure disk based fencing | Choose this option to configure disk-based I/O fencing. |

Based on the fencing type you choose to configure, follow the installer prompts.

See [“Configuring Symantec VirtualStore for data integrity using the Web-based installer”](#) on page 182.

12 Click **Next** to complete the process of configuring Symantec VirtualStore. On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

13 Select the checkbox to specify whether you want to send your installation information to Symantec.

Click **Finish**. The installer prompts you for another task.

Configuring Symantec VirtualStore for data integrity using the Web-based installer

After you configure Symantec VirtualStore, you must configure the cluster for data integrity. Review the configuration requirements.

See [“Configuring Symantec VirtualStore using the Web-based installer”](#) on page 177.

See [“About planning to configure I/O fencing”](#) on page 71.

Ways to configure I/O fencing using the Web-based installer:

- See [“Configuring disk-based fencing for data integrity using the Web-based installer”](#) on page 183.
- See [“Configuring server-based fencing for data integrity using the Web-based installer”](#) on page 185.
- See [“Configuring fencing in disabled mode using the Web-based installer”](#) on page 187.
- See [“Online fencing migration mode using the Web-based installer”](#) on page 188.

Configuring disk-based fencing for data integrity using the Web-based installer

After you configure Symantec VirtualStore, you must configure the cluster for data integrity. Review the configuration requirements.

See [“Configuring Symantec VirtualStore using the Web-based installer”](#) on page 177.

See [“About planning to configure I/O fencing”](#) on page 71.

To configure Symantec VirtualStore for data integrity

- 1 Start the Web-based installer.

See [“Starting the Veritas Web-based installer”](#) on page 172.

- 2 On the Select a task and a product page, select the task and the product as follows:

Task	I/O fencing configuration
Product	Symantec VirtualStore

Click **Next**.

- 3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.

- 4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

- 5 On the Select Fencing Type page, select the `Configure disk-based fencing` option.

- 6 In the Confirmation dialog box that appears, confirm whether your storage environment supports SCSI-3 PR.

You can configure non-SCSI-3 server-based fencing in a virtual environment that is not SCSI-3 PR compliant.

- 7 On the Configure Fencing page, the installer prompts for details based on the fencing type you chose to configure. Specify the coordination points details.

Click **Next**.

- 8 On the Configure Fencing page, specify the following information:

- Select a Disk Group** Select the **Create a new disk group** option or select one of the disk groups from the list.
- If you selected one of the disk groups that is listed, choose the fencing disk policy for the disk group.
 - If you selected the **Create a new disk group** option, make sure you have SCSI-3 PR enabled disks, and click **Yes** in the confirmation dialog box. Click **Next**.

9 On the Create New DG page, specify the following information:

New Disk Group Name Enter a name for the new coordinator disk group you want to create.

Select Disks Select at least three disks to create the coordinator disk group.

If you want to select more than three disks, make sure to select an odd number of disks.

Fencing Disk Policy Choose the fencing disk policy for the disk group.

10 If you want to configure the Coordination Point agent on the client cluster, do the following:

- At the prompt for configuring the Coordination Point agent on the client cluster, click **Yes** and enter the Coordination Point agent service group name.
- If you want to set the LevelTwoMonitorFreq attribute, click **Yes** at the prompt and enter a value (0 to 65535).
- Follow the rest of the prompts to complete the Coordination Point agent configuration.

11 Click **Next** to complete the process of configuring I/O fencing.

On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

12 Select the checkbox to specify whether you want to send your installation information to Symantec.

Click **Finish**. The installer prompts you for another task.

Configuring server-based fencing for data integrity using the Web-based installer

After you configure Symantec VirtualStore, you must configure the cluster for data integrity. Review the configuration requirements.

See [“Configuring Symantec VirtualStore using the Web-based installer”](#) on page 177.

See [“About planning to configure I/O fencing”](#) on page 71.

To configure Symantec VirtualStore for data integrity

- 1 Start the Web-based installer.

See [“Starting the Veritas Web-based installer”](#) on page 172.

- 2 On the Select a task and a product page, select the task and the product as follows:

Task	I/O fencing configuration
Product	Symantec VirtualStore

Click **Next**.

- 3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.

- 4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

- 5 On the Select Fencing Type page, select the `Configure server-based fencing` option.

- 6 In the Confirmation dialog box that appears, confirm whether your storage environment supports SCSI-3 PR.

You can configure non-SCSI-3 server-based fencing in a virtual environment that is not SCSI-3 PR compliant.

- 7 On the Configure Fencing page, the installer prompts for details based on the fencing type you chose to configure. Specify the coordination points details.

Click **Next**.

- 8 Provide the following details for each of the CP servers:

- Enter the virtual IP addresses or host names of the virtual IP address. The installer assumes these values to be identical as viewed from all the application cluster nodes.
 - Enter the port that the CP server must listen on.
 - Click **Next**.
- 9 If your server-based fencing configuration also uses disks as coordination points, perform the following steps:
- If you have not already checked the disks for SCSI-3 PR compliance, check the disks now, and click OK in the dialog box.
 - If you do not want to use the default coordinator disk group name, enter a name for the new coordinator disk group you want to create.
 - Select the disks to create the coordinator disk group.
 - Choose the fencing disk policy for the disk group.
The default fencing disk policy for the disk group is dmp.
- 10 In the Confirmation dialog box that appears, confirm whether the coordination points information you provided is correct, and click **Yes**.
- 11 Verify and confirm the I/O fencing configuration information.
The installer stops and restarts the VCS and the fencing processes on each application cluster node, and completes the I/O fencing configuration.
- 12 If you want to configure the Coordination Point agent on the client cluster, do the following:
- At the prompt for configuring the Coordination Point agent on the client cluster, click **Yes** and enter the Coordination Point agent service group name.
 - Follow the rest of the prompts to complete the Coordination Point agent configuration.
- 13 Click **Next** to complete the process of configuring I/O fencing.
On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.
- 14 Select the checkbox to specify whether you want to send your installation information to Symantec.
Click **Finish**. The installer prompts you for another task.

Configuring fencing in disabled mode using the Web-based installer

After you configure Symantec VirtualStore, you must configure the cluster for data integrity. Review the configuration requirements.

See [“Configuring Symantec VirtualStore using the Web-based installer”](#) on page 177.

See [“About planning to configure I/O fencing”](#) on page 71.

To configure Symantec VirtualStore for data integrity

- 1 Start the Web-based installer.

See [“Starting the Veritas Web-based installer”](#) on page 172.

- 2 On the Select a task and a product page, select the task and the product as follows:

Task	I/O fencing configuration
Product	Symantec VirtualStore

Click **Next**.

- 3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.
- 4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

- 5 Fencing may be enabled, installer may prompt whether you want to reconfigure it.

Click **Yes**.

- 6 On the Select Fencing Type page, select the `Configure fencing in disabled mode` option.

- 7 Installer stops VCS before applying the selected fencing mode to the cluster.

Note: Unfreeze any frozen service group and unmount any file system that is mounted in the cluster.

Click **Yes**.

- 8 Installer restarts VCS on all systems of the cluster. I/O fencing is disabled.

- 9 Verify and confirm the I/O fencing configuration information.
On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.
- 10 Select the checkbox to specify whether you want to send your installation information to Symantec.
Click **Finish**. The installer prompts you for another task.

Online fencing migration mode using the Web-based installer

After you configure Symantec VirtualStore, you must configure the cluster for data integrity. Review the configuration requirements.

See [“Configuring Symantec VirtualStore using the Web-based installer”](#) on page 177.

See [“About planning to configure I/O fencing”](#) on page 71.

To configure Symantec VirtualStore for data integrity

- 1 Start the Web-based installer.
See [“Starting the Veritas Web-based installer”](#) on page 172.
- 2 On the Select a task and a product page, select the task and the product as follows:

Task	I/O fencing configuration
Product	Symantec VirtualStore

Click **Next**.

- 3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.
- 4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.
- 5 Fencing may be enabled, installer may prompt whether you want to reconfigure it.
Click **Yes**.
- 6 On the Select Fencing Type page, select the `Online fencing migration` option.

- 7 The installer prompts to select the coordination points you want to remove from the currently configured coordination points.
Click **Next**.
- 8 Provide the number of Coordination point server and disk coordination points to be added to the configuration.
Click **Next**.
- 9 Provide the number of virtual IP addresses or Fully Qualified Host Name (FQHN) used for each coordination point server.
Click **Next**.
- 10 Provide the IP or FQHN and port number for each coordination point server.
Click **Next**.
- 11 Installer prompts to confirm the online migration coordination point servers.
Click **Yes**.

Note: If the coordination point servers are configured in secure mode, then the communication between coordination point servers and client servers happen in secure mode.

- 12 Installer proceeds with migration of the new coordination point servers. VCS is restarted during configuration.
Click **Next**.
- 13 You can add a Coordination Point agent to the client cluster and also provide name to the agent.
- 14 Click **Next**.
- 15 On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.
- 16 Select the checkbox to specify whether you want to send your installation information to Symantec.
Click **Finish**. The installer prompts you for another task.

Automated installation using response files

- [Chapter 12. Performing an automated Symantec VirtualStore installation](#)
- [Chapter 13. Performing an automated Symantec VirtualStore configuration](#)
- [Chapter 14. Performing an automated I/O fencing configuration using response files](#)

Performing an automated Symantec VirtualStore installation

This chapter includes the following topics:

- [Installing SVS using response files](#)

Installing SVS using response files

Typically, you can use the response file that the installer generates after you perform SVS installation on one cluster to install SVS on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To install SVS using response files

- 1 Make sure the systems where you want to install SVS meet the installation requirements.
- 2 Make sure the preinstallation tasks are completed.
- 3 Copy the response file to one of the cluster systems where you want to install SVS.
- 4 Edit the values of the response file variables as necessary.

- 5 Mount the product disc and navigate to the directory that contains the installation program.
- 6 Start the installation from the system to which you copied the response file. For example:

```
# ./installer -responsefile /tmp/response_file  
  
# ./installsvs<version> -responsefile /tmp/response_file
```

Where <version> is the specific release version and */tmp/response_file* is the response file's full path name.

See [“About the Veritas installer”](#) on page 41.

Performing an automated Symantec VirtualStore configuration

This chapter includes the following topics:

- [Configuring SVS using response files](#)
- [Response file variables to configure Symantec VirtualStore](#)

Configuring SVS using response files

Typically, you can use the response file that the installer generates after you perform SVS configuration on one cluster to configure SVS on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To configure SVS using response files

- 1 Make sure the SVS packages are installed on the systems where you want to configure SVS.
- 2 Copy the response file to one of the cluster systems where you want to configure SVS.

- 3 Edit the values of the response file variables as necessary.

To configure optional features, you must define appropriate values for all the response file variables that are related to the optional feature.

See “[Response file variables to configure Symantec VirtualStore](#)” on page 196.

- 4 Start the configuration from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/installsvs<version>
-responsefile /tmp/response_file
```

Where *<version>* is the specific release version, and */tmp/response_file* is the response file’s full path name.

See “[About the Veritas installer](#)” on page 41.

Response file variables to configure Symantec VirtualStore

[Table 13-1](#) lists the response file variables that you can define to configure SVS.

Table 13-1 Response file variables specific to configuring Symantec VirtualStore

Variable	List or Scalar	Description
\$CFG{config_cfs}	Scalar	Performs the Cluster File System configuration for SF Sybase CE (Required) Set the value to 1 to configure Cluster File System for SF Sybase CE
CFG{opt}{configure}	Scalar	Performs the configuration if the packages are already installed. (Required) Set the value to 1 to configure SVS.
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)
CFG{systems}	List	List of systems on which the product is to be configured. (Required)

Table 13-1 Response file variables specific to configuring Symantec VirtualStore
(continued)

Variable	List or Scalar	Description
CFG{prod}	Scalar	Defines the product to be configured. The value is VCS60 for VCS. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{rsh}	Scalar	Defines that <i>rsh</i> must be used instead of <i>ssh</i> as the communication method between systems. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is <i>/opt/VRTS/install/logs</i> . Note: The installer copies the response files and summary files also to the specified <i>logpath</i> location. (Optional)
CFG{uploadlogs}	Scalar	Defines a Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site. (Optional)

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (*csgnic*, *csgvip*, and *csgnetmask*) must be defined if any are defined. The same is true for the SMTP notification (*smtpserver*, *smtprecp*, and *smtpsev*), the

SNMP trap notification (snmpport, snmpcons, and snmpcsev), and the Global Cluster Option (gconic, gcovip, and gconetmask).

Table 13-2 lists the response file variables that specify the required information to configure a basic Symantec VirtualStore cluster.

Table 13-2 Response file variables specific to configuring a basic Symantec VirtualStore cluster

Variable	List or Scalar	Description
CFG{vcs_clusterid}	Scalar	An integer between 0 and 65535 that uniquely identifies the cluster. (Required)
CFG{vcs_clustername}	Scalar	Defines the name of the cluster. (Required)
CFG{vcs_allowcomms}	Scalar	Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)
CFG{fencingenabled}	Scalar	In a Symantec VirtualStore configuration, defines if fencing is enabled. Valid values are 0 or 1. (Required)

Table 13-3 lists the response file variables that specify the required information to configure LLT over Ethernet.

Table 13-3 Response file variables specific to configuring private LLT over Ethernet

Variable	List or Scalar	Description
CFG{vcs_lltlink#} {"system"}	Scalar	<p>Defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (lltlink1 and lltlink2). You can configure up to four LLT links.</p> <p>You must enclose the system name within double quotes.</p> <p>(Required)</p>
CFG{vcs_lltlinklowpri#} {"system"}	Scalar	<p>Defines a low priority heartbeat link. Typically, lltlinklowpri is used on a public network link to provide an additional layer of communication.</p> <p>If you use different media speed for the private NICs, you can configure the NICs with lesser speed as low-priority links to enhance LLT performance. For example, lltlinklowpri1, lltlinklowpri2, and so on.</p> <p>You must enclose the system name within double quotes.</p> <p>(Optional)</p>

[Table 13-4](#) lists the response file variables that specify the required information to configure LLT over UDP.

Table 13-4 Response file variables specific to configuring LLT over UDP

Variable	List or Scalar	Description
CFG{lltoverudp}=1	Scalar	<p>Indicates whether to configure heartbeat link using LLT over UDP.</p> <p>(Required)</p>

Table 13-4 Response file variables specific to configuring LLT over UDP
(continued)

Variable	List or Scalar	Description
CFG{vcs_udplink<n>_address} {<system1>}	Scalar	Stores the IP address (IPv4 or IPv6) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required)
CFG {vcs_udplinklowpri<n>_address} {<system1>}	Scalar	Stores the IP address (IPv4 or IPv6) that the low priority heartbeat link uses on node1. You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required)
CFG{vcs_udplink<n>_port} {<system1>}	Scalar	Stores the UDP port (16-bit integer value) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required)
CFG{vcs_udplinklowpri<n>_port} {<system1>}	Scalar	Stores the UDP port (16-bit integer value) that the low priority heartbeat link uses on node1. You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required)

Table 13-4 Response file variables specific to configuring LLT over UDP
(continued)

Variable	List or Scalar	Description
CFG{vcs_udplink<n>_netmask} {<system1>}	Scalar	Stores the netmask (prefix for IPv6) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required)
CFG{vcs_udplinklowpri<n>_netmask} {<system1>}	Scalar	Stores the netmask (prefix for IPv6) that the low priority heartbeat link uses on node1. You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required)

Table 13-5 lists the response file variables that specify the required information to configure virtual IP for Symantec VirtualStore cluster.

Table 13-5 Response file variables specific to configuring virtual IP for Symantec VirtualStore cluster

Variable	List or Scalar	Description
CFG{vcs_csgnic} {system}	Scalar	Defines the NIC device to use on a system. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional)
CFG{vcs_csgvip}	Scalar	Defines the virtual IP address for the cluster. (Optional)
CFG{vcs_csgnetmask}	Scalar	Defines the Netmask of the virtual IP address for the cluster. (Optional)

Table 13-6 lists the response file variables that specify the required information to configure the Symantec VirtualStore cluster in secure mode.

Table 13-6 Response file variables specific to configuring Symantec VirtualStore cluster in secure mode

Variable	List or Scalar	Description
CFG{vcs_eat_security}	Scalar	Specifies if the cluster is in secure enabled mode or not.
CFG{opt}{securityonnode}	Scalar	Specifies that the securityonnode option is being used.
CFG{securityonnode_menu}	Scalar	Specifies the menu option to choose to configure the secure cluster one at a time. <ul style="list-style-type: none"> ■ 1—Configure the first node ■ 2—Configure the other node
CFG{security_conf_dir}	Scalar	Specifies the directory where the configuration files are placed.
CFG{opt}{security}	Scalar	Specifies that the security option is being used.
CFG{opt}{fips}	Scalar	Specifies that the FIPS option is being used.
CFG{vcs_eat_security_fips}	Scalar	Specifies that the enabled security is FIPS compliant.

Table 13-7 lists the response file variables that specify the required information to configure VCS users.

Table 13-7 Response file variables specific to configuring VCS users

Variable	List or Scalar	Description
CFG{vcs_userenpw}	List	List of encoded passwords for VCS users The value in the list can be "Administrators Operators Guests" Note: The order of the values for the vcs_userenpw list must match the order of the values in the vcs_username list. (Optional)
CFG{vcs_username}	List	List of names of VCS users (Optional)
CFG{vcs_userpriv}	List	List of privileges for VCS users Note: The order of the values for the vcs_userpriv list must match the order of the values in the vcs_username list. (Optional)

[Table 13-8](#) lists the response file variables that specify the required information to configure VCS notifications using SMTP.

Table 13-8 Response file variables specific to configuring VCS notifications using SMTP

Variable	List or Scalar	Description
CFG{vcs_smtpserver}	Scalar	Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for Web notification. (Optional)
CFG{vcs_smtprecpl}	List	List of full email addresses (example: user@symantecexample.com) of SMTP recipients. (Optional)

Table 13-8 Response file variables specific to configuring VCS notifications using SMTP (*continued*)

Variable	List or Scalar	Description
CFG{vcs_smtprsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SMTP recipients are to receive. Note that the ordering of severity levels must match that of the addresses of SMTP recipients. (Optional)

[Table 13-9](#) lists the response file variables that specify the required information to configure VCS notifications using SNMP.

Table 13-9 Response file variables specific to configuring VCS notifications using SNMP

Variable	List or Scalar	Description
CFG{vcs_snmpport}	Scalar	Defines the SNMP trap daemon port (default=162). (Optional)
CFG{vcs_snmpcons}	List	List of SNMP console system names (Optional)
CFG{vcs_snmpcsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names. (Optional)

[Table 13-10](#) lists the response file variables that specify the required information to configure Symantec VirtualStore global clusters.

Table 13-10 Response file variables specific to configuring Symantec VirtualStore global clusters

Variable	List or Scalar	Description
CFG{vcs_gconic} {system}	Scalar	Defines the NIC for the Virtual IP that the Global Cluster Option uses. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional)
CFG{vcs_gcovip}	Scalar	Defines the virtual IP address to that the Global Cluster Option uses. (Optional)
CFG{vcs_gconetmask}	Scalar	Defines the Netmask of the virtual IP address that the Global Cluster Option uses. (Optional)

Performing an automated I/O fencing configuration using response files

This chapter includes the following topics:

- [Configuring I/O fencing using response files](#)
- [Response file variables to configure disk-based I/O fencing](#)
- [Sample response file for configuring disk-based I/O fencing](#)
- [Response file variables to configure server-based I/O fencing](#)
- [Sample response file for configuring server-based I/O fencing](#)
- [Response file variables to configure non-SCSI-3 server-based I/O fencing](#)
- [Sample response file for configuring non-SCSI-3 server-based I/O fencing](#)

Configuring I/O fencing using response files

Typically, you can use the response file that the installer generates after you perform I/O fencing configuration to configure I/O fencing for Symantec VirtualStore.

To configure I/O fencing using response files

- 1 Make sure that Symantec VirtualStore is configured.
- 2 Based on whether you want to configure disk-based or server-based I/O fencing, make sure you have completed the preparatory tasks.

See [“About planning to configure I/O fencing”](#) on page 71.

- 3 Copy the response file to one of the cluster systems where you want to configure I/O fencing.

See “[Sample response file for configuring disk-based I/O fencing](#)” on page 211.

See “[Sample response file for configuring server-based I/O fencing](#)” on page 213.

- 4 Edit the values of the response file variables as necessary.

See “[Response file variables to configure disk-based I/O fencing](#)” on page 208.

See “[Response file variables to configure server-based I/O fencing](#)” on page 211.

- 5 Start the configuration from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/installsvs<version>  
-responsefile /tmp/response_file
```

Where *<version>* is the specific release version, and */tmp/response_file* is the response file’s full path name.

See “[About the Veritas installer](#)” on page 41.

Response file variables to configure disk-based I/O fencing

[Table 14-1](#) lists the response file variables that specify the required information to configure disk-based I/O fencing for SVS.

Table 14-1 Response file variables specific to configuring disk-based I/O fencing

Variable	List or Scalar	Description
CFG{opt}{fencing}	Scalar	Performs the I/O fencing configuration. (Required)

Table 14-1 Response file variables specific to configuring disk-based I/O fencing
(continued)

Variable	List or Scalar	Description
CFG{fencing_option}	Scalar	<p>Specifies the I/O fencing configuration mode.</p> <ul style="list-style-type: none"> ■ 1—Coordination Point Server-based I/O fencing ■ 2—Coordinator disk-based I/O fencing ■ 3—Disabled mode ■ 4—Fencing migration when the cluster is online <p>(Required)</p>
CFG {fencing_scsi3_disk_policy}	Scalar	<p>Specifies the I/O fencing mechanism.</p> <p>This variable is not required if you had configured fencing in disabled mode. For disk-based fencing, you must configure the <code>fencing_scsi3_disk_policy</code> variable and either the <code>fencing_dgname</code> variable or the <code>fencing_newdg_disks</code> variable.</p> <p>(Optional)</p>
CFG{fencing_dgname}	Scalar	<p>Specifies the disk group for I/O fencing.</p> <p>(Optional)</p> <p>Note: You must define the <code>fencing_dgname</code> variable to use an existing disk group. If you want to create a new disk group, you must use both the <code>fencing_dgname</code> variable and the <code>fencing_newdg_disks</code> variable.</p>

Table 14-1 Response file variables specific to configuring disk-based I/O fencing
(continued)

Variable	List or Scalar	Description
CFG{fencing_newdg_disks}	List	<p>Specifies the disks to use to create a new disk group for I/O fencing.</p> <p>(Optional)</p> <p>Note: You must define the <code>fencing_dgname</code> variable to use an existing disk group. If you want to create a new disk group, you must use both the <code>fencing_dgname</code> variable and the <code>fencing_newdg_disks</code> variable.</p>
CFG{fencing_cpagent_monitor_freq}	Scalar	<p>Specifies the frequency at which the Coordination Point Agent monitors for any changes to the Coordinator Disk Group constitution.</p> <p>Note: Coordination Point Agent can also monitor changes to the Coordinator Disk Group constitution such as a disk being accidentally deleted from the Coordinator Disk Group. The frequency of this detailed monitoring can be tuned with the <code>LevelTwoMonitorFreq</code> attribute. For example, if you set this attribute to 5, the agent will monitor the Coordinator Disk Group constitution every five monitor cycles. If <code>LevelTwoMonitorFreq</code> attribute is not set, the agent will not monitor any changes to the Coordinator Disk Group. 0 means not to monitor the Coordinator Disk Group constitution.</p>

Table 14-1 Response file variables specific to configuring disk-based I/O fencing (continued)

Variable	List or Scalar	Description
CFG {fencing_config_cpagent}	Scalar	Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter "0" if you do not want to configure the Coordination Point agent using the installer. Enter "1" if you want to use the installer to configure the Coordination Point agent.
CFG {fencing_cpagentgrp}	Scalar	Name of the service group which will have the Coordination Point agent resource as part of it. Note: This field is obsolete if the fencing_config_cpagent field is given a value of '0'.

Sample response file for configuring disk-based I/O fencing

Review the disk-based I/O fencing response file variables and their definitions.

See [“Response file variables to configure disk-based I/O fencing”](#) on page 208.

Response file variables to configure server-based I/O fencing

You can use a coordination point server-based fencing response file to configure server-based customized I/O fencing.

[Table 14-2](#) lists the fields in the response file that are relevant for server-based customized I/O fencing.

Table 14-2 Coordination point server (CP server) based fencing response file definitions

Response file field	Definition
CFG {fencing_config_cpagent}	<p>Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not.</p> <p>Enter "0" if you do not want to configure the Coordination Point agent using the installer.</p> <p>Enter "1" if you want to use the installer to configure the Coordination Point agent.</p>
CFG {fencing_cpagentgrp}	<p>Name of the service group which will have the Coordination Point agent resource as part of it.</p> <p>Note: This field is obsolete if the <code>fencing_config_cpagent</code> field is given a value of '0'.</p>
CFG {fencing_cps}	<p>Virtual IP address or Virtual hostname of the CP servers.</p>
CFG {fencing_reusedg}	<p>This response file field indicates whether to reuse an existing DG name for the fencing configuration in customized fencing (CP server and coordinator disks).</p> <p>Enter either a "1" or "0".</p> <p>Entering a "1" indicates reuse, and entering a "0" indicates do not reuse.</p> <p>When reusing an existing DG name for the mixed mode fencing configuration, you need to manually add a line of text, such as "<code>CFG{fencing_reusedg}=0</code>" or "<code>CFG{fencing_reusedg}=1</code>" before proceeding with a silent installation.</p>
CFG {fencing_dgname}	<p>The name of the disk group to be used in the customized fencing, where at least one disk is being used.</p>
CFG {fencing_disks}	<p>The disks being used as coordination points if any.</p>
CFG {fencing_ncp}	<p>Total number of coordination points being used, including both CP servers and disks.</p>
CFG {fencing_ndisks}	<p>The number of disks being used.</p>

Table 14-2 Coordination point server (CP server) based fencing response file definitions (*continued*)

Response file field	Definition
CFG {fencing_cps_vips}	The virtual IP addresses or the fully qualified host names of the CP server.
CFG {fencing_ports}	The port that the virtual IP address or the fully qualified host name of the CP server listens on.
CFG {fencing_scsi3_disk_policy}	The disk policy that the customized fencing uses. The value for this field is either "raw" or "dmp"

Sample response file for configuring server-based I/O fencing

The following is a sample response file used for server-based I/O fencing:

```

$CFG{fencing_config_cpagent}=0;
$CFG{fencing_cps}=[ qw(10.200.117.145) ];
$CFG{fencing_cps_vips}{"10.200.117.145"}=[ qw(10.200.117.145) ];
$CFG{fencing_dgname}="vxfencoorddg";
$CFG{fencing_disks}=[ qw(emc_clariion0_37 emc_clariion0_13) ];
$CFG{fencing_scsi3_disk_policy}="raw";
$CFG{fencing_ncp}=3;
$CFG{fencing_ndisks}=2;
$CFG{fencing_ports}{"10.200.117.145"}=14250;
$CFG{fencing_reusedg}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="SFCFSHA601";
$CFG{systems}=[ qw(sys1 sys2) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{fencing_option}=1;

```

Response file variables to configure non-SCSI-3 server-based I/O fencing

[Table 14-3](#) lists the fields in the response file that are relevant for non-SCSI-3 server-based customized I/O fencing.

See “[About I/O fencing for Symantec VirtualStore in virtual machines that do not support SCSI-3 PR](#)” on page 24.

Table 14-3 Non-SCSI-3 server-based I/O fencing response file definitions

Response file field	Definition
CFG{non_scsi3_fencing}	Defines whether to configure non-SCSI-3 server-based I/O fencing. Valid values are 1 or 0. Enter 1 to configure non-SCSI-3 server-based I/O fencing.
CFG {fencing_config_cpagent}	Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter "0" if you do not want to configure the Coordination Point agent using the installer. Enter "1" if you want to use the installer to configure the Coordination Point agent.
CFG {fencing_cpagentgrp}	Name of the service group which will have the Coordination Point agent resource as part of it. Note: This field is obsolete if the <code>fencing_config_cpagent</code> field is given a value of '0'.
CFG {fencing_cps}	Virtual IP address or Virtual hostname of the CP servers.
CFG {fencing_cps_vips}	The virtual IP addresses or the fully qualified host names of the CP server.
CFG {fencing_ncp}	Total number of coordination points (CP servers only) being used.
CFG {fencing_ports}	The port of the CP server that is denoted by <i>cps</i> .

Sample response file for configuring non-SCSI-3 server-based I/O fencing

The following is a sample response file used for non-SCSI-3 server-based I/O fencing :

```
$CFG{fencing_config_cpagent}=0;
$CFG{fencing_cps}=[ qw(10.198.89.251 10.198.89.252 10.198.89.253) ];
```

```
$CFG{fencing_cps_vips}{"10.198.89.251"}=[ qw(10.198.89.251) ];  
$CFG{fencing_cps_vips}{"10.198.89.252"}=[ qw(10.198.89.252) ];  
$CFG{fencing_cps_vips}{"10.198.89.253"}=[ qw(10.198.89.253) ];  
$CFG{fencing_ncp}=3;  
$CFG{fencing_ndisks}=0;  
$CFG{fencing_ports}{"10.198.89.251"}=14250;  
$CFG{fencing_ports}{"10.198.89.252"}=14250;  
$CFG{fencing_ports}{"10.198.89.253"}=14250;  
$CFG{non_scsi3_fencing}=1;  
$CFG{opt}{configure}=1;  
$CFG{opt}{fencing}=1;  
$CFG{prod}="SVS60";  
$CFG{systems}=[ qw(sys1 sys2) ];  
$CFG{vcs_clusterid}=1256;  
$CFG{vcs_clustername}="clus1";  
$CFG{fencing_option}=1;
```

216 | Performing an automated I/O fencing configuration using response files
Sample response file for configuring non-SCSI-3 server-based I/O fencing

Installation using operating system-specific methods

- [Chapter 15. Installing Symantec VirtualStore using operating system-specific methods](#)

Installing Symantec VirtualStore using operating system-specific methods

This chapter includes the following topics:

- [Installing SVS on Solaris 10 using JumpStart](#)
- [Installing SVS on Solaris 11 using Automated Installer](#)
- [Manually installing packages on Oracle Solaris 11 systems](#)
- [Manually installing packages on Solaris brand non-global zones](#)
- [Installing SVS using the system command](#)

Installing SVS on Solaris 10 using JumpStart

This installation method applies only to Solaris 10. These JumpStart instructions assume a working knowledge of JumpStart. See the JumpStart documentation that came with your operating system for details on using JumpStart.

Upgrading is not supported. The following procedure assumes a stand-alone configuration.

For the language pack, you can use JumpStart to install packages. You add the language packages in the script, and put those files in the JumpStart server directory.

You can use a Flash archive to install SVS and the operating system in conjunction with JumpStart.

See [“Using a Flash archive to install SVS and the operating system”](#) on page 223.

Overview of JumpStart installation tasks

Review the summary of tasks before you perform the JumpStart installation.

Summary of tasks

- 1 Add a client (register to the JumpStart server). See the JumpStart documentation that came with your operating system for details.
- 2 Read the JumpStart installation instructions.
- 3 Generate the finish scripts.
See [“Generating the finish scripts”](#) on page 220.
- 4 Prepare shared storage installation resources.
See [“Preparing installation resources”](#) on page 222.
- 5 Modify the rules file for JumpStart.
See the JumpStart documentation that came with your operating system for details.
- 6 Install the operating system using the JumpStart server.
- 7 When the system is up and running, run the installer command from the installation media to configure the Veritas software.

```
# /opt/VRTS/install/installer -configure
```

See [“About the Veritas installer”](#) on page 41.

Generating the finish scripts

Perform these steps to generate the finish scripts to install SVS.

To generate the script

- 1 Run the product installer program to generate the scripts for all products.

```
./installer -jumpstart directory_to_generate_scripts
```

Or

```
./install<productname> -jumpstart directory_to_generate_script
```

where *<productname>* is the product's installation command, and *directory_to_generate_scripts* is where you want to put the product's script.

For example:

```
# ./installsvs -jumpstart /js_scripts
```

- 2 When you are prompted to encapsulate the root disk automatically, choose **yes** to do so. If you do not want to encapsulate it automatically, choose **no** and go to step 6.

- 3 Specify a disk group name for the root disk.

Specify the disk group name of the root disk to be encapsulated:
rootdg

- 4 Specify private region length.

Specify the private region length of the root disk to be encapsulated: **(65536)**

- 5 Specify the disk's media name of the root disk to encapsulate.

Specify the disk media name of the root disk to be encapsulated:
(rootdg_01)

- 6 JumpStart finish scripts and encapsulation scripts are generated in the directory you specified in step 1.

List the *js_scripts* directory.

```
# ls /js_scripts
```

Output resembles:

```
encap_bootdisk_vm.fin jumpstart_svs.fin
```

Preparing installation resources

Prepare resources for the JumpStart installation.

To prepare the resources

- 1 Copy the pkgs directory of the installation media to the shared storage.

```
# cd /path_to_installation_media
# cp -r pkgs BUILDSRC
```

- 2 Generate the response file with the list of packages.

```
# cd BUILDSRC/pkgs/
# pkgask -r package_name.response -d /
BUILDSRC/pkgs/packages_name.pkg
```

- 3 Create the adminfile file under *BUILDSRC/pkgs/* directory.

```
mail=
instance=overwrite
partial=nocheck
runlevel=quit
idepend=quit
rdepend=nocheck
space=quit
setuid=nocheck
conflict=nocheck
action=nocheck
basedir=default
```

- 4 If you want to encapsulate the root disk automatically when you perform the JumpStart installation, copy the scripts *encap_bootdisk_vm.fin* generated previously to *ENCAPSRC*.

See [“Generating the finish scripts”](#) on page 220.

Adding language pack information to the finish file

To add the language pack information to the finish file, perform the following procedure.

To add the language pack information to the finish file

- 1 For the language pack, copy the language packages from the language pack installation disc to the shared storage.

```
# cd /cdrom/cdrom0/pkg  
# cp -r * BUILDSRC/pkg
```

If you downloaded the language pack:

```
# cd /path_to_language_pack_installation_media/pkg  
# cp -r * BUILDSRC/pkg
```

- 2 In the finish script, copy the product package information and replace the product packages with language packages.
- 3 The finish script resembles:

```
. . .  
for PKG in product_packages  
do  
...  
done. . .  
for PKG in language_packages  
do  
...  
done. . .
```

Using a Flash archive to install SVS and the operating system

You can only use Flash archive on the Solaris 10 operating system. In the following outline, refer to Solaris documentation for Solaris-specific tasks.

Note: Symantec does not support Flash Archive installation if the root disk of the master system is encapsulated.

The following is an overview of the creation and installation of a Flash archive with Veritas software.

- If you plan to start flar (flash archive) creation from bare metal, perform step 1 through step 10.
- If you plan to start flar creation from a system where you have installed, but not configured the product, perform step 1 through step 4. Skip step 5 and finish step 6 through step 10.

- If you plan to start flar creation from a system where you have installed and configured the product, perform step 5 through step 10.

Flash archive creation overview

- 1 Ensure that you have installed Solaris 10 on the master system.
- 2 Use JumpStart to create a clone of a system.
- 3 Reboot the cloned system.
- 4 Install the Veritas products on the master system.
Perform one of the installation procedures from this guide.
- 5 If you have configured the product on the master system, create the `vrts_deployment.sh` file and the `vrts_deployment.cf` file and copy them to the master system.
See [“Creating the Veritas post-deployment scripts”](#) on page 224.
- 6 Use the `flarcreate` command to create the Flash archive on the master system.
- 7 Copy the archive back to the JumpStart server.
- 8 Use JumpStart to install the Flash archive to the selected systems.
- 9 Configure the Veritas product on all nodes in the cluster. Start configuration with the following command:

```
# /opt/VRTS/install/installsvs -configure
```

See [“About the Veritas installer”](#) on page 41.
- 10 Perform post-installation and configuration tasks.
See the product installation guide for the post-installation and configuration tasks.

Creating the Veritas post-deployment scripts

The generated files `vrts_deployment.sh` and `vrts_post-deployment.cf` are customized Flash archive post-deployment scripts. These files clean up Veritas product settings on a cloned system before you reboot it for the first time. Include these files in your Flash archives.

To create the post-deployment scripts

- 1 Mount the product disc.
- 2 From the prompt, run the `-flash_archive` option for the installer. Specify a directory where you want to create the files.

```
# ./installer -flash_archive /tmp
```

- 3 Copy the `vrts_postdeployment.sh` file and the `vrts_postdeployment.cf` file to the golden system.
- 4 On the golden system perform the following:
 - Put the `vrts_postdeployment.sh` file in the `/etc/flash/postdeployment` directory.
 - Put the `vrts_postdeployment.cf` file in the `/etc/vx` directory.
- 5 Make sure that the two files have the following ownership and permissions:

```
# chown root:root /etc/flash/postdeployment/vrts_postdeployment.sh
# chmod 755 /etc/flash/postdeployment/vrts_postdeployment.sh
# chown root:root /etc/vx/vrts_postdeployment.cf
# chmod 644 /etc/vx/vrts_postdeployment.cf
```

Note that you only need these files in a Flash archive where you have installed Veritas products.

Installing SVS on Solaris 11 using Automated Installer

You can use the Oracle Solaris Automated Installer (AI) to install the Solaris 11 operating system on multiple client systems in a network. AI performs a hands-free installation (automated installation without manual interactions) of both x86 and SPARC systems. You can also use AI media (AI bootable image, provided by Oracle, which can be downloaded from the Oracle Web site) to install the Oracle Solaris OS on a single SPARC or x86 platform. All cases require access to a package repository on the network to complete the installation.

About Automated Installation

AI automates the installation of the Oracle Solaris 11 OS on one or more SPARC or x86 clients in a network. Automated Installation applies to Solaris 11 only. You can install the Oracle Solaris OS on many different types of clients. The clients can differ in:

- architecture

- memory characteristics
- MAC address
- IP address
- CPU

The installations can differ depending on specifications including network configuration and packages installed.

An automated installation of a client in a local network consists of the following high-level steps:

- 1 A client system boots and gets IP information from the DHCP server
- 2 Characteristics of the client determine which AI service and which installation instructions are used to install the client.
- 3 The installer uses the AI service instructions to pull the correct packages from the package repositories and install the Oracle Solaris OS on the client.

Using Automated Installer

To use Automated Installer to install systems over the network, set up DHCP and set up an AI service on an AI server. The DHCP server and AI server can be the same system or two different systems.

Make sure that the systems can access an Oracle Solaris Image Packaging System (IPS) package repository. The IPS package repository can reside on the AI server, on another server on the local network, or on the Internet.

An AI service is associated with a SPARC or x86 AI install image and one or more sets of installation instructions. The installation instructions specify one or more IPS package repositories from where the system retrieves the packages needed to complete the installation. The installation instructions also include the names of additional packages to install and information such as target device and partition information. You can also specify instructions for post-installation configuration of the system.

Consider the operating systems and packages you are installing on the systems. Depending on your configuration and needs, you may want to do one of the following:

- If two systems have different architectures or need to be installed with different versions of the Oracle Solaris OS, create two AI services, and associate each AI service with a different AI image.
- If two systems need to be installed with the same version of the Oracle Solaris OS but need to be installed differently in other ways, create two sets of installation instructions for the AI service. The different installation

instructions can specify different packages to install or a different slice as the install target.

The installation begins when you boot the system. DHCP directs the system to the AI install server, and the system accesses the install service and the installation instructions within that service.

For more information, see the *Oracle® Solaris 11 Express Automated Installer Guide*.

Using AI to install the Solaris 11 operating system and SFHA products

Use the following procedure to install the Solaris 11 operating system and SFHA products using AI.

To use AI to install the Solaris 11 operating system and SFHA products

- 1 Follow the Oracle documentation to setup a Solaris AI server and DHCP server. You can find the documentation at <http://docs.oracle.com>.
- 2 Set up the Symantec package repository.

Run the following commands to start up necessary SMF services and create directories:

```
# svcadm enable svc:/network/dns/multicast:default
# mkdir /ai
# zfs create -o compression=on -o mountpoint=/ai rpool/ai
```

- 3 Run the following commands to set up the IPS repository for Symantec Opteron packages:

```
# mkdir -p /ai/repo_symc_x64
# pkgrepo create /ai/repo_symc_x64
# pkgrepo add-publisher -s /ai/repo_symc_x64 Symantec
# pkgrecv -s <media_x64>/pkgs/VRTSpkgs.p5p -d /ai/repo_symc_x64 '*'
# svccfg -s pkg/server add symcx64
# svccfg -s pkg/server list
# svccfg -s pkg/server:symcx64 addpg pkg application
# svccfg -s pkg/server:symcx64 setprop pkg/port=10002
# svccfg -s pkg/server:symcx64 setprop pkg/inst_root=/ai/repo_symc_x64
# svccfg -s pkg/server:symcx64 addpg general framework
# svccfg -s pkg/server:symcx64 addpropvalue
general/complete astring: symcx64
# svccfg -s pkg/server:symcx64 addpropvalue general/enable
boolean: true
# svcs -a | grep pkg/server
# svcadm refresh application/pkg/server:symcx64
# svcadm enable application/pkg/server:symcx64
```

Or run the following commands to set up the private depot server for testing purposes:

```
# /usr/lib/pkg.depotd -d /ai/repo_symc_x64 -p 10002 > /dev/null &
```

Check the following URL on IE or Firefox browser:

<http://<host>:10002>

- 4 Run the following commands to setup IPS repository for Symantec Sparc packages:

```
# mkdir -p /ai/repo_symc_sparc
# pkgrepo create /ai/repo_symc_sparc
# pkgrepo add-publisher -s /ai/repo_symc_sparc Symantec
# pkgrecv -s <media_sparc>/pkgs/VRTSpkgs.p5p -d
/ai/repo_symc_sparc '*'
# svccfg -s pkg/server list
# svcs -a | grep pkg/server
# svccfg -s pkg/server add symcsparc
# svccfg -s pkg/server:symcsparc addpg pkg application
# svccfg -s pkg/server:symcsparc setprop pkg/port=10003
# svccfg -s pkg/server:symcsparc setprop pkg/inst_root=
/ai/repo_symc_sparc
# svccfg -s pkg/server:symcsparc addpg general framework
# svccfg -s pkg/server:symcsparc addpropvalue general/complete
astring: symcsparc
# svccfg -s pkg/server:symcsparc addpropvalue general/enable
boolean: true
# svcs -a | grep pkg/server
# svcadm refresh application/pkg/server:symcsparc
# svcadm enable application/pkg/server:symcsparc
```

Or run the following commands to set up the private depot server for testing purposes:

```
# /usr/lib/pkg.depotd -d /ai/repo_symc_sparc -p 10003 > /dev/null &
```

Check the following URL on IE or Firefox browser:

<http://<host>:10003>

- 5 Run the following commands to setup IPS repository to merge Symantec Sparc and x64 packages:

```
# mkdir /ai/repo_symc
# pkgrepo create /ai/repo_symc
# pkgrepo add-publisher -s /ai/repo_symc Symantec
# pkgmerge -s arch=sparc,/ai/repo_symc_sparc -s arch=i386,
/ai/repo_symc_x64 -d /ai/repo_symc
# svcs -a | grep pkg/server
# svccfg -s pkg/server list
# svccfg -s pkg/server add symcmmerged
# svccfg -s pkg/server:symcmmerged addpg pkg application
# svccfg -s pkg/server:symcmmerged setprop pkg/port=10004
# svccfg -s pkg/server:symcmmerged setprop pkg/inst_root=/ai/repo_symc
# svccfg -s pkg/server:symcmmerged addpg general framework
# svccfg -s pkg/server:symcmmerged addpropvalue general/complete
astring: symcmmerged
# svccfg -s pkg/server:symcmmerged addpropvalue general/enable
boolean: true
# svcadm refresh application/pkg/server:symcmmerged
# svcadm enable application/pkg/server:symcmmerged
# svcs -a | grep pkg/server
```

Or run the following commands to set up the private depot server for testing purposes:

```
# # /usr/lib/pkg.depotd -d /ai/repo_symc -p 10004 > /dev/null &
```

Check the following URL on IE or Firefox browser:

<http://<host>:10004>

6 Set up the install service on the AI server.

Run the following command:

```
# mkdir /ai/iso
```

Download the AI image from the Oracle Web site and place the `iso` in the `/ai/iso` directory.

Create an install service.

For example:

To set up the AI install server for Opteron platform::

```
# installadm create-service -n sol11x86 -s  
/ai/iso/sol-11-1111-ai-x86.iso -d /ai/aiboot/
```

To set up the AI install server for SPARC platform::

```
# # installadm create-service -n sol11sparc -s\  
/ai/iso/sol-11-1111-ai-sparc.iso -d /ai/aiboot/
```

7 Run the installer to generate manifest XML files for all the SFHA products that you plan to install.

```
# mkdir /ai/manifests  
# <media>/installer -ai /ai/manifests
```

8 For each system, generate the system configuration and include the hostname, user accounts, and IP addresses. For example, enter one of the following:

```
# mkdir /ai/profiles  
# sysconfig create-profile -o /ai/profiles/profile_client.xml
```

or

```
# cp /ai/aiboot/auto-install/sc_profiles/sc_sample.xml  
/ai/profiles/profile_client.xml
```

- 9 Add a system and match it to the specified product manifest and system configuration.

Run the following command to add an Opteron system, for example:

```
# installadm create-client -e "<client_MAC>" -n soll1x86
# installadm add-manifest -n soll1x86 -f \
/ai/manifests/vrts_manifest_sfha.xml
# installadm create-profile -n soll1x86 -f \
/ai/profiles/profile_client.xml -p profile_sc
# installadm set-criteria -n soll1x86 -m vrts_sfha
-p profile_sc -c mac="<client_MAC>"
# installadm list -m -c -p -n soll1x86
```

Run the following command to add a SPARC system, for example:

```
# installadm create-client -e "<client_MAC>" -n soll1sparc
# installadm add-manifest -n soll1sparc -f \
/ai/manifests/vrts_manifest_sfha.xml
# installadm create-profile -n soll1sparc -f \
/ai/profiles/profile_client.xml -p profile_sc
# installadm set-criteria -n soll1sparc -m \
vrts_sfha -p profile_sc -c mac="<client_MAC>"
# installadm list -m -c -p -n soll1sparc
```

- 10 For Opteron system, use Preboot Execution Environment(PXE) to reboot the system and install the operating system and Storage Foundation products.

For Sparc system, run the following command to reboot the system and install the operating system and Storage Foundation products:

```
# boot net:dhcp - install
```


Manually installing packages on Oracle Solaris 11 systems

To install packages on Solaris 11 system

1 Copy the VRTSpkgs.p5p package from the pkgs directory from the installation media to the system at `/tmp/install` directory.

2 Disable the publishers that are not reachable as package install may fail if any of the already added repositories are unreachable.

```
# pkg set-publisher --disable <publisher name>
```

3 Add a file-based repository in the system.

```
# pkg set-publisher -p /tmp/install/VRTSpkgs.p5p Symantec
```

4 Install the required packages.

5 Remove the publisher from the system.

```
# pkg unset-publisher Symantec
```

6 Clear the state of the SMF service if non-global zones are present in the system. In presence of non-global zones, setting the file-based repository causes SMF service `svc:/application/pkg/system-repository:default` to go into maintenance state.

```
# svcadm clear svc:/application/pkg/system-repository:default
```

7 Enable the publishers that were disabled earlier.

```
# pkg set-publisher --enable <publisher name>
```

Manually installing packages on Solaris brand non-global zones

With Oracle Solaris 11, you must manually install SVS packages inside non-global zones. The native non-global zones are called Solaris brand zones.

To install packages manually on Solaris brand non-global zones:

- 1 Ensure that the SMF service `svc:/application/pkg/system-repository:default` is online on the global zone.

```
# svcsvcs svc:/application/pkg/system-repository
```

- 2 Log on to the non-global zone as a superuser.
- 3 Copy the `VRTSpkgs.p5p` package from the `pkgs` directory from the installation media to the non-global zone (for example at `/tmp/install` directory).
- 4 Disable the publishers that are not reachable, as package install may fail if any of the already added repositories are unreachable.

```
#pkg set-publisher --disable <publisher name>
```

- 5 Add a file-based repository in the non-global zone.

```
# pkg set-publisher -p/tmp/install/VRTSpkgs.p5p Symantec
```

- 6 Install the required packages.

- 7 Remove the publisher on the non-global zone.

```
#pkg unset-publisher Symantec
```

- 8 Clear the state of the SMF service, as setting the file-based repository causes SMF service `svc:/application/pkg/system-repository:default` to go into maintenance state.

```
# svcadm clear svc:/application/pkg/system-repository:default
```

- 9 Enable the publishers that were disabled earlier.

```
# pkg set-publisher --enable <publisher>
```

Note: Perform steps 2 through 9 on each non-global zone.

Installing SVS using the system command

Installing SVS on Solaris 10 using the `pkgadd` command

On Solaris 10, the packages must be installed while in the global zone.

To install SVS on Solaris 10 using the pkgadd command

- 1 Mount the software disc.
- 2 Copy the supplied VRTS* files from the installation media to a temporary location. Modify them if needed.

```
# cp /cdrom/cdrom0/pkgsvs/VRTS* \  
    /tmp/pkgsvs
```

- 3 Create the admin file in the current directory. Specify the `-a adminfile` option when you use the `pkgadd` command:

```
mail=  
instance=overwrite  
partial=nocheck  
runlevel=quit  
idepend=quit  
rdepend=nocheck  
space=quit  
setuid=nocheck  
conflict=nocheck  
action=nocheck  
basedir=default
```

- 4 Use the product-specific install command with one of the following options to get a list of packages in the order to be installed:
 - `minpkgs`
 - `recpkgs`
 - `allpkgs`

See [“About the Veritas installer”](#) on page 41.

See [“Installation script options”](#) on page 395.

- 5 Install the packages listed in step 4.

```
# pkgadd -a adminfile -d /tmp/pkgsvs pkgname.pkg
```

On Solaris 10, these packages must be installed while in the global zone. If a package's `pkginfo` file contains the variable `SUNW_PKG_ALLZONES` set not equal to true, the `-G` option should additionally be specified to the `pkgadd` command.

- 6 Verify that the packages are installed:

```
# pkginfo -l  
    packagename
```

- 7 Start the processes.

Installing SVS on Solaris 11 using the pkg install command

To install SVS on Solaris 11 using the pkg install command

- 1 Mount the software disc.
- 2 Copy the supplied VRTS* files from the installation media to a temporary location. Modify them if needed.

```
# cp /cdrom/cdrom0/pkgsvs/VRTS* \  
    /tmp/pkgsvs
```

- 3 Use the product-specific install command with one of the following options to get a list of packages in the order to be installed:

- minpkgs
- recpkgs
- allpkgs

See [“About the Veritas installer”](#) on page 41.

See [“Installation script options”](#) on page 395.

- 4 Install the packages listed in step 3.

```
# /usr/bin/pkg set-publisher -p /tmp/pkgsvs/VRTSpkgs.p5p Symantec  
  
# /usr/bin/pkg install -accept pkgname  
  
# /usr/bin/pkg unset-publisher Symantec
```

- 5 Verify that the packages are installed:

```
# pkg info packagename
```

- 6 Start the processes.

Upgrading Symantec VirtualStore

- [Chapter 16. Preparing to upgrade](#)
- [Chapter 17. Performing a full upgrade using the installer](#)
- [Chapter 18. Performing a phased upgrade](#)
- [Chapter 19. Performing a rolling upgrade](#)
- [Chapter 20. Upgrading the operating system](#)

Preparing to upgrade

This chapter includes the following topics:

- [Upgrade methods for SVS](#)
- [Supported upgrade paths](#)
- [About using the installer to upgrade when the root disk is encapsulated](#)
- [Preparing to upgrade SVS](#)

Upgrade methods for SVS

Symantec offers you several different ways to upgrade. You need to decide which upgrade method best suits your environment, your expertise, and the downtime required.

Table 16-1 Review this table to determine how you want to perform the upgrade

Upgrade types and considerations	Methods available for upgrade
Typical upgrades—use a Veritas provided tool or you can perform the upgrade manually. Requires some server downtime.	<p>Script-based—you can use this to upgrade for the supported upgrade paths</p> <p>Web-based—you can use this to upgrade for the supported upgrade paths</p> <p>Manual—you can use this to upgrade from the previous release</p> <p>Response file—you can use this to upgrade from the supported upgrade paths</p>

Table 16-1 Review this table to determine how you want to perform the upgrade
(continued)

Upgrade types and considerations	Methods available for upgrade
Rolling upgrade—use a Veritas provided tool or you can perform the upgrade manually. Requires least amount of server downtime.	Script-based—you can use this to upgrade from the previous release Web-based—you can use this to upgrade from the previous release
Phased upgrades—use a Veritas provided tool and some manual steps. Requires less server downtime than a regular upgrade.	Script-based with some manual steps—you can use this to upgrade from the previous release
Native operating system upgrade—use the upgrade software that comes with the operating system. Note that not all operating systems support native upgrades.	Operating system specific methods Operating system upgrades

Supported upgrade paths

The following tables describe upgrading to 6.0.1

Table 16-2 Solaris SPARC upgrades using the script- or Web-based installer

Veritas software versions	Solaris 8 or older	Solaris 9	Solaris 10	Solaris 11
5.1 SP1 5.1 SP1 RPx 5.1 SP1 PR3	N/A	Upgrade to Solaris 10. Use the installer to upgrade to 6.0.1.	Use the installer to upgrade to 6.0.1.	N/A
6.0	N/A	N/A	Use the installer to upgrade to 6.0.1.	N/A
6.0 RP1	N/A	N/A	Use the installer to upgrade to 6.0.1.	N/A
6.0 PR1	N/A	N/A	N/A	Use the installer to upgrade to 6.0.1.

Table 16-2 Solaris SPARC upgrades using the script- or Web-based installer (continued)

Veritas software versions	Solaris 8 or older	Solaris 9	Solaris 10	Solaris 11
New installation	N/A	N/A	Use the installer to install 6.0.1.	Use the installer to install 6.0.1.

Table 16-3 Solaris x64 upgrades using the script- or Web-based installer

Veritas software versions	Solaris 10	Solaris 11
5.1 SP1* 5.1 SP1 RPx 5.1 SP1 PR3	Use the installer to upgrade to 6.0.1.	N/A
6.0	Use the installer to upgrade to 6.0.1.	N/A
6.0 RP1	Use the installer to upgrade to 6.0.1.	N/A
6.0 PR1	Use the installer to upgrade to 6.0.1.	N/A
New installation	Use the installer to upgrade to 6.0.1.	Use the installer to install 6.0.1.

*When you upgrade to 6.0 from 5.1 SP1 using the Web-based installer, you must first upgrade to 5.1 SP1 RP1 if you want the installer to create a backup of the boot disk. You can upgrade directly to 6.0 from 5.1 SP1 if you do not want the installer to create a backup of the boot disk.

About using the installer to upgrade when the root disk is encapsulated

In prior versions of SVS, when upgrading a system with an encapsulated root disk, you first had to unencapsulate. When upgrading to SVS 6.0.1, that is no longer necessary, as shown in the table below.

Table 16-4 Upgrading using installer when the root disk is encapsulated

Starting version	Ending version	Action required
5.0 MP3 RPx	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
5.1 or 5.1 RPx	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
5.1 SP1 or 5.1 SP1 RPx	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.

Preparing to upgrade SVS

Before you upgrade, you need to prepare the systems and storage. Review the following procedures and perform the appropriate tasks.

Getting ready for the upgrade

Complete the following tasks before you perform the upgrade:

- Review the Symantec Technical Support website for additional information: <http://www.symantec.com/techsupp/>
- If you are upgrading from 5.1SP1, you need to unregister the plugin before you upgrade and after the upgrade, you need to register the new plugin. See “[Register the new plugin](#)” on page 289.
- For Solaris 10, make sure that all non-global zones are booted and in the running state before you use the Veritas product installer to upgrade the Storage Foundation products in the global zone. If the non-global zones are not mounted and running at the time of the upgrade, you must upgrade each package in each non-global zone manually.
For Live Upgrade, if the alternative root environment also has a zone, you cannot install `VRTSodm`. You must remove the `VRTSodm` package first then install the Storage Foundation product. After you reboot the alternative root, you can install `VRTSodm`.
- Make sure that the administrator who performs the upgrade has root access and a good knowledge of the operating system's administration.
- Make sure that all users are logged off and that all major user applications are properly shut down.

- Make sure that you have created a valid backup. See [“Creating backups”](#) on page 243.
- Ensure that you have enough file system space to upgrade. Identify where you want to copy the packages, for example `/packages/Veritas` when the root file system has enough space or `/var/tmp/packages` if the `/var` file system has enough space.
Do not put the files under `/tmp`, which is erased during a system reboot. Do not put the files on a file system that is inaccessible prior to running the upgrade script.
You can use a Veritas-supplied disc for the upgrade as long as modifications to the upgrade script are not required. If `/usr/local` was originally created as a slice, modifications are required.
- For any startup scripts in `/sbin/rcS.d`, comment out any application commands or processes that are known to hang if their file systems are not present.
- Make sure that the current operating system supports version 6.0.1 of the product. If the operating system does not support it, plan for a staged upgrade.
- Schedule sufficient outage time and downtime for the upgrade and any applications that use the Veritas products. Depending on the configuration, the outage can take several hours.
- Any swap partitions not in `rootdg` must be commented out of `/etc/vfstab`. If possible, swap partitions other than those on the root disk should be commented out of `/etc/vfstab` and not mounted during the upgrade. Active swap partitions that are not in `rootdg` cause `upgrade_start` to fail.
- Make sure the file systems are clean before upgrading. See [“Verifying that the file systems are clean”](#) on page 251.
- Upgrade arrays (if required). See [“Upgrading the array support”](#) on page 252.
- To reliably save information on a mirrored disk, shut down the system and physically remove the mirrored disk. Removing the disk in this manner offers a fallback point.

Creating backups

Save relevant system information before the upgrade.

Note: Unconfigure any FLR jobs for any file systems before unmounting specific file systems.

To create backups

- 1 Log in as superuser.
- 2 Before the upgrade, ensure that you have made backups of all data that you want to preserve.

Back up the `/etc/system` file.

- 3 Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.

If not, a warning message is displayed.

Warning: Backup `/etc/vx/cbr/bk` directory.

- 4 Run the `vxlicrep`, `vxdisk list`, and `vxprint -ht` commands and record the output. Use this information to reconfigure your system after the upgrade.
- 5 If you are installing the high availability version of the Veritas Storage Foundation 6.0.1 software, follow the guidelines given in the *Veritas Cluster Server Installation Guide* and *Veritas Cluster Server Release Notes* for information on preserving your VCS configuration across the installation procedure.

Determining if the root disk is encapsulated

Before you upgrade, you need to determine if the root disk is encapsulated by running the following command:

```
# mount | grep "/" on"
```

If the output from this command includes a path name that contains `vx` and `rootvol` as in `/dev/vx/dsk/bootdg/rootvol`, then the root disk is encapsulated.

If the root disk is encapsulated, follow the appropriate upgrade procedures.

See [“About using the installer to upgrade when the root disk is encapsulated”](#) on page 241.

Pre-upgrade planning for Veritas Volume Replicator

Before installing or upgrading Veritas Volume Replicator (VVR):

- Confirm that your system has enough free disk space to install VVR.
- Make sure you have root permissions. You must have root permissions to perform the install and upgrade procedures.

- If replication using VVR is configured, Symantec recommends that the disk group version is at least 110 prior to upgrading.

You can check the Disk Group version using the following command:

```
# vxdg list diskgroup
```

- If replication using VVR is configured, make sure the size of the SRL volume is greater than 110 MB.

Refer to the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide*.

- If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date on all the hosts.

```
# /usr/sbin/vxrlink -g diskgroup status rlink_name
```

Note: Do not continue until the primary RLINKs are up-to-date.

- If VCS is used to manage VVR replication, follow the preparation steps to upgrade VVR and VCS agents.
- Make sure that you have worked out all terminal emulation issues. Make sure that the terminal you use is fully functional for OpenBoot prompts and single-user and multi-user run levels.

See the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide* for more information.

See the *Getting Started Guide* for more information on the documentation.

Planning an upgrade from the previous VVR version

If you plan to upgrade VVR from the previous VVR version, you can upgrade VVR with reduced application downtime by upgrading the hosts at separate times. While the Primary is being upgraded, the application can be migrated to the Secondary, thus reducing downtime. The replication between the (upgraded) Primary and the Secondary, which have different versions of VVR, will still continue. This feature facilitates high availability even when the VVR upgrade is not complete on both the sites. Symantec recommends that the Secondary hosts be upgraded before the Primary host in the Replicated Data Set (RDS).

See the *Symantec VirtualStore Release Notes* for information regarding VVR support for replicating across Storage Foundation versions

Replicating between versions is intended to remove the restriction of upgrading the Primary and Secondary at the same time. VVR can continue to replicate an

existing RDS with Replicated Volume Groups (RVGs) on the systems that you want to upgrade. When the Primary and Secondary are at different versions, VVR does not support changing the configuration with the `vradmin` command or creating a new RDS.

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in [Table 16-5](#), if either the Primary or Secondary are running a version of VVR prior to 6.0.1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 6.0.1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

Table 16-5 VVR versions and checksum calculations

VVR prior to 6.0.1 (DG version <= 140)	VVR 6.0.1 (DG version >= 150)	VVR calculates checksum TCP connections?
Primary	Secondary	Yes
Secondary	Primary	Yes
Primary and Secondary		Yes
	Primary and Secondary	No

Note: When replicating between versions of VVR, avoid using commands associated with new features. The earlier version may not support new features and problems could occur.

If you do not need to upgrade all the hosts in the RDS simultaneously, you can use replication between versions after you upgrade one host. You can then upgrade the other hosts in the RDS later at your convenience.

Note: If you have a cluster setup, you must upgrade all the nodes in the cluster at the same time.

Planning and upgrading VVR to use IPv6 as connection protocol

Symantec VirtualStore supports using IPv6 as the connection protocol.

This release supports the following configurations for VVR:

- VVR continues to support replication between IPv4-only nodes with IPv4 as the internet protocol

- VVR supports replication between IPv4-only nodes and IPv4/IPv6 dual-stack nodes with IPv4 as the internet protocol
- VVR supports replication between IPv6-only nodes and IPv4/IPv6 dual-stack nodes with IPv6 as the internet protocol
- VVR supports replication between IPv6 only nodes
- VVR supports replication to one or more IPv6 only nodes and one or more IPv4 only nodes from a IPv4/IPv6 dual-stack node
- VVR supports replication of a shared disk group only when all the nodes in the cluster that share the disk group are at IPv4 or IPv6

Additional settings for using VVR in a localized environment

If the language packages for VVR are installed, VVR displays localized messages, if the client locale is a supported non-English locale. The client locale is the locale from which you are accessing the VVR command line or GUI. For example, if the Japanese version of VVR is installed, then the messages are displayed in the Japanese locale, if the client locale is Japanese.

Make sure that the appropriate locale has been installed on all the hosts that are intended to be a part of the VVR RDS setup. Otherwise, some VVR error messages will be displayed in English, because it is the default locale. Make sure the following settings are done on all hosts that are intended to be part of the RDS:

- Install the required client locale from the Operating System disc.
- Install the required Volume Manager and VVR localized packages.
- Set the client locale, before using any of the VVR interfaces:
 - For the VVR command line, set the locale using the appropriate method for your operating system.
 - For VRW, select the locale from the VRW login page.

Preparing to upgrade VVR when VCS agents are configured

To prepare to upgrade VVR when VCS agents for VVR are configured, perform the following tasks in the order presented:

- [Freezing the service groups and stopping all the applications](#)
- [Preparing for the upgrade when VCS agents are configured](#)

Freezing the service groups and stopping all the applications

This section describes how to freeze the service groups and stop all applications.

To freeze the service groups and stop applications

Perform the following steps for the Primary and Secondary clusters:

- 1 Log in as the superuser.
- 2 Make sure that `/opt/VRTS/bin` is in your PATH so that you can execute all the product commands.
- 3 Before the upgrade, cleanly shut down all applications.
 - OFFLINE all application service groups that do not contain RVG resources. Do not OFFLINE the service groups containing RVG resources.
 - If the application resources are part of the same service group as an RVG resource, then OFFLINE only the application resources. In other words, ensure that the RVG resource remains ONLINE so that the private disk groups containing these RVG objects do not get deported.

Note: You must also stop any remaining applications not managed by VCS.

- 4 On any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

- 5 On any node in the cluster, list the groups in your configuration:

```
# hagrps -list
```

- 6 On any node in the cluster, freeze all service groups except the ClusterService group by typing the following command for each group name displayed in the output from step 5.

```
# hagrps -freeze group_name -persistent<sys_name>
```

Note: Make a note of the list of frozen service groups for future use.

- 7 On any node in the cluster, save the configuration file (`main.cf`) with the groups frozen:

```
# haconf -dump -makero
```

Note: Continue only after you have performed steps 3 to step 7 for each node of the cluster.

- 8 Display the list of service groups that have RVG resources and the nodes on which each service group is online by typing the following command on any node in the cluster:

```
# hares -display -type RVG -attribute State
Resource      Attribute      System      Value
VVRGrp        State          system02    ONLINE
ORAGrp        State          system02    ONLINE
```

Note: For the resources that are ONLINE, write down the nodes displayed in the System column of the output.

- 9 Repeat step 8 for each node of the cluster.
- 10 For private disk groups, determine and note down the hosts on which the disk groups are imported.
 See [“Determining the nodes on which disk groups are online”](#) on page 249.
- 11 For shared disk groups, run the following command on any node in the CVM cluster:

```
# vxdctl -c mode
```

Note the master and record it for future use.

Determining the nodes on which disk groups are online

For private disk groups, determine and note down the hosts on which the disk groups containing RVG resources are imported. This information is required for restoring the configuration after the upgrade.

To determine the online disk groups

- 1 On any node in the cluster, list the disk groups in your configuration, and note down the disk group names listed in the output for future use:

```
# hares -display -type RVG -attribute DiskGroup
```

Note: Write down the list of the disk groups that are under VCS control.

- 2 For each disk group listed in the output in step 1, list its corresponding disk group resource name:

```
# hares -list DiskGroup=diskgroup Type=DiskGroup
```

- 3 For each disk group resource name listed in the output in step 2, get and note down the node on which the disk group is imported by typing the following command:

```
# hares -display dg_resname -attribute State
```

The output displays the disk groups that are under VCS control and nodes on which the disk groups are imported.

Preparing for the upgrade when VCS agents are configured

If you have configured the VCS agents, it is recommended that you take backups of the configuration files, such as `main.cf` and `types.cf`, which are present in the `/etc/VRTSvcs/conf/config` directory.

To prepare a configuration with VCS agents for an upgrade

- 1 List the disk groups on each of the nodes by typing the following command on each node:

```
# vxdisk -o alldgs list
```

The output displays a list of the disk groups that are under VCS control and the disk groups that are not under VCS control.

Note: The disk groups that are not locally imported are displayed in parentheses.

- 2 If any of the disk groups have not been imported on any node, import them. For disk groups in your VCS configuration, you can import them on any node. For disk groups that are not under VCS control, choose an appropriate node on which to import the disk group. Enter the following command on the appropriate node:

```
# vxdg -t import diskgroup
```

- 3 If a disk group is already imported, then recover the disk group by typing the following command on the node on which it is imported:

```
# vxrecover -bs
```

- 4 Verify that all the Primary RLINKs are up to date.

```
# vxrlink -g diskgroup status rlink_name
```

Note: Do not continue until the Primary RLINKs are up-to-date.

Verifying that the file systems are clean

Verify that all file systems have been cleanly unmounted.

To make sure the file systems are clean

- 1 Verify that all file systems have been cleanly unmounted:

```
# echo "8192B.p S" | /opt/VRTSvxfs/sbin/fsdb filesystem | \  
    grep clean  
    flags 0 mod 0 clean clean_value
```

A *clean_value* value of 0x5a indicates the file system is clean. A value of 0x3c indicates the file system is dirty. A value of 0x69 indicates the file system is dusty. A dusty file system has pending extended operations.

- 2 If a file system is not clean, enter the following commands for that file system:

```
# opt/VRTS/bin/fsck -F vxfs filesystem  
# opt/VRTS/bin/mount -F vxfs Block_Device  
    mountpoint  
# opt/VRTS/bin/umount mountpoint
```

These commands should complete any extended operations on the file system and unmount the file system cleanly.

A pending large package clone removal extended operation might be in progress if the `umount` command fails with the following error:

```
file system device busy
```

An extended operation is in progress if the following message is generated on the console:

```
Storage Checkpoint asynchronous operation on file_system  
file system still in progress.
```

- 3 If an extended operation is in progress, you must leave the file system mounted for a longer time to allow the operation to complete. Removing a very large package clone can take several hours.
- 4 Repeat step 1 to verify that the unclean file system is now clean.

Upgrading the array support

The Storage Foundation 6.0.1 release includes all array support in a single package, VRTSaslapm. The array support package includes the array support previously included in the VRTSvxvm package. The array support package also includes support previously packaged as external array support libraries (ASLs) and array policy modules (APMs).

See the 6.0.1 Hardware Compatibility List for information about supported arrays.

See [“Hardware compatibility list \(HCL\)”](#) on page 29.

When you upgrade Storage Foundation products with the product installer, the installer automatically upgrades the array support. If you upgrade Storage Foundation products with manual steps, you should remove any external ASLs or APMs that were installed previously on your system. Installing the VRTSvxvm package exits with an error if external ASLs or APMs are detected.

After you have installed Storage Foundation 6.0.1, Symantec provides support for new disk arrays through updates to the `VRTSaslapm` package.

For more information about array support, see the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide*.

Performing a full upgrade using the installer

This chapter includes the following topics:

- [Performing a full upgrade](#)

Performing a full upgrade

Performing a full upgrade involves the following tasks:

- Ensuring that the file systems are clean
- Updating the main.cf file
- Performing the upgrade
- Updating the configuration and confirming startup

Ensuring the file systems are clean

Before upgrading to SVS 6.0.1, ensure that the file systems are clean. To ensure that the logs have been replayed and the file systems are marked clean:

To ensure the file systems are clean

- 1 Log in as superuser onto any node in the cluster.
- 2 Take the service group offline on each node of the cluster, which contains VxFS and CFS resources:

```
# hagrps -offline group -sys system01
# hagrps -offline group -sys system02
# hagrps -offline group -sys system03
# hagrps -offline group -sys system04
```

where *group* is the VCS service group that has the CVMVolDg and CFMount resource.

Repeat this step for each SVS service group.

Note: This unmounts the CFS file systems.

- 3 Unmount all VxFS file systems not under VCS control:

```
# umount mount_point
```

- 4 Check and repair each VxFS file system:

```
# fsck -F vxfs /dev/vx/rdisk/diskgroup/volume
```

The `fsck` command in `/opt/VRTS/bin` accepts either the block or character device (`/dev/vx/dsk/dg/vol`) or (`/dev/vx/rdisk/dg/vol`). The operating system version of `fsck` may limit the device types it accepts.

For more information, see the `fsck` and `fsck_vxfs` man pages.

Repeat this step for each file system.

Modifying the main.cf file

Save a copy of the `main.cf` file and modify the configuration information in the `main.cf` file.

To modify the main.cf file

- 1 On any node, make a copy of the current `main.cf` file. For example:

```
# cp /etc/VRTSvcs/conf/config/main.cf \  
    /etc/VRTSvcs/conf/main.save
```

- 2 Choose one node from the cluster to execute step 3 through step 9.
- 3 On the node you selected in step 2, enter:

```
# haconf -makerw  
# hares -unlink vxfsckd qlogckd  
# hares -unlink qlogckd cvm_clus  
# hares -link vxfsckd cvm_clus  
# hares -delete qlogckd  
# haconf -dump -makero
```

- 4 On all the nodes in the cluster, enter:

```
# ps -ef | grep qlogckd  
# kill -9 pid_of_qlogckd  
# modinfo | grep -i qlog  
# modunload -i module_id_of_qlog
```

- 5 On the node you selected in step 2, stop VCS on all nodes:

```
# /opt/VRTS/bin/hastop -all -force
```

- 6 On the node you selected in step 2 and if you have configured the VCS Cluster Manager (Web Console), complete the following to modify the `/etc/VRTSvcs/conf/config/main.cf` file.

- Remove VRTSweb:

```
Process VRTSweb (  
    PathName = "/opt/VRTSvcs/bin/haweb"  
    Arguments = "10.129.96.64 8181"  
)
```

- Replace it with:

```
VRTSWebApp VCSweb (  
    Critical =0  
    AppName = vcs  
    InstallDir = "/opt/VRTSweb/VERITAS"
```

```
TimeForOnline = 5  
)
```

- Add the NIC resource in the ClusterService group. For example, where the name of the NIC resource is named `csgnic` and the public NIC device is `hme0`, add:

```
NIC csgnic (  
    Device = hme0
```

- Add new dependencies for the new resources in the ClusterService group. For example, using the names of the VRTSWebApp, NotifierMgr, IP, and NIC resources, enter lines that resemble:

```
VCSweb requires webip  
ntfr requires csgnic  
webip requires csgnic
```

- 7 On the node you selected in step 2, remove `qlogckd` from the `/etc/VRTSvcs/conf/config/main.cf` file. For example:

```
CFSQlogckd qlogckd (  
    Critical = 0  
)
```

Make sure you remove all dependencies on `qlogckd` from the `main.cf` file.

- 8 On the node you selected in step 2, verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file:

```
# cd /etc/VRTSvcs/conf/config  
# /opt/VRTS/bin/hacf -verify .
```

- 9 On the node you selected in step 2, start VCS:

```
# /opt/VRTS/bin/hastart
```

- 10 On the remaining nodes in the cluster, start VCS:

```
# /opt/VRTS/bin/hastart
```

- 11 If VVR is configured, freeze the service groups and stop the applications.

See [“Freezing the service groups and stopping all the applications”](#) on page 247.

Performing the upgrade

To perform the upgrade

- 1 Log in as superuser.
- 2 Insert the appropriate media disc into your system's DVD-ROM drive.
- 3 If volume management software is running on your system, the software disc automatically mounts as `/cdrom`.

If volume management software is not available to mount the disc, you must mount it manually, enter:

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

where `c#t#d#` is the location of the CD drive.

- 4 Change to the top-level directory on the disc:

```
# cd /cdrom
```

- 5 Verify there are no VxFS file systems mounted on the nodes being upgraded:

```
# mount -p | grep vxfs
```

If any VxFS file systems are mounted, offline the group on each node of the cluster:

```
# hagr -offline group -sys system01
# hagr -offline group -sys system02
# hagr -offline group -sys system03
# hagr -offline group -sys system04
```

where `group` is the VCS service group that has the CVMVolDg and CFSSMount resource.

If VxFS are not managed by VCS then unmount them manually:

```
# umount mount_point
```

Repeat this step for each SVS service group.

- 6 Start the upgrade from any node in the cluster. Enter the following command, and then press `y` to upgrade the cluster configuration.

```
# ./installsvs -upgrade
```

- 7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA).

```
Do you agree with the terms of the End User License Agreement
as specified in the storage_foundation_cluster_file_system_ha/EULA/
en/EULA_productname_Ux_version.pdf file present on media? [y,n,q,?] y
```

- 8 The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the system's boot disk group before the upgrade proceeds. If you want to split the boot disk group to create a backup, answer **y**.
- 9 The installer then prompts you to name the backup boot disk group. Enter the name for it or press **Enter** to accept the default.
- 10 If you are prompted to start the split operation. Press **y** to continue.

Note: The split operation can take some time to complete.

- 11 You are prompted to enter the system names (in the following example, "sys1" and "sys2") on which the software is to be upgraded. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces: sys1 sys2
```

- 12 During the initial system check, the installer verifies that communication between systems has been set up.

If the installer hangs or asks for a login password, stop the installer and set up ssh or rsh. Then run the installer again.

See [“About configuring secure shell or remote shell communication modes before installing products”](#) on page 415.

- 13 After you accept EULA and the system checks complete, the installer displays a list of the packages that will be upgraded. Press Enter to continue with the upgrade.
- 14 Output shows information that SVS must be stopped on a running system. Enter **y** to continue.
- 15 Press **Return** to begin removing the previous packages and installing the new.

- 16 Press **Return** again for summary information about logs and reboots.
Do not remove the log files until the Veritas products are working properly on your system. Technical Support will need these log files for debugging purposes.
- 17 Update the configuration.
- 18 Only perform this step if you have split the mirrored root disk to back it up. After a successful reboot, verify the upgrade and re-join the backup disk group. If the upgrade fails, revert to the backup disk group.
See [“Re-joining the backup boot disk group into the current disk group”](#) on page 288.
See [“Reverting to the backup boot disk group after an unsuccessful upgrade”](#) on page 288.

Updating the configuration and confirming startup

Perform the following steps on each upgraded node.

To update the configuration and confirm startup

- 1 Remove the `/etc/VRTSvcs/conf/config/.stale` file, if it exists.

```
# rm -f /etc/VRTSvcs/conf/config/.stale
```
- 2 Reboot the upgraded nodes, if installer prompts you for the reboot.

```
# /usr/sbin/shutdown -i6 -g0 -y
```
- 3 After the nodes reboot, verify that LLT is running:

```
# lltconfig
LLT is running
```
- 4 Verify GAB is configured:

```
# gabconfig -l | grep 'Driver.state' | \
grep Configured
Driver state : Configured
```
- 5 Verify VxVM daemon is started and enabled:

```
# /opt/VRTS/bin/vxdctl mode
mode: enabled
```

- 6 Confirm all upgraded nodes are in a running state.

```
# gabconfig -a
```

- 7 If VVR is configured, and the CVM and SVS groups are offline, bring the groups online in the following order:

Bring online the CVM groups on all systems.

```
# /opt/VRTS/bin/hagrp -online group_name -sys sys1
# /opt/VRTS/bin/hagrp -online group_name -sys sys2
```

where *group_name* is the VCS service group that has the CVMVolDg resource.

Bring online the RVGShared groups and the virtual IP on the master node using the following commands:

```
# hagrp -online RVGShared -sys masterhost
# hares -online ip_name -sys masterhost
```

Bring online the SVS groups on all systems.

```
# /opt/VRTS/bin/hagrp -online group_name -sys sys1
# /opt/VRTS/bin/hagrp -online group_name -sys sys2
```

where *group_name* is the VCS service group that has the CFSSMount resource.

If the SVS service groups do not come online then your file system could be dirty.

Note: If you upgrade to SVS 6.0.1 and the file systems are dirty, you have to deport the shared disk group and import it as non-shared. After the import, run `fsck`. `fsck` should succeed. Then deport the disk group and import it back as shared.

- 8 Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

- 9 On the CVM master node, upgrade the CVM protocol. Enter the following:

```
# vxdctl upgrade
```

Performing a phased upgrade

This chapter includes the following topics:

- [Performing a phased upgrade of SVS stack from version 5.1 SP1](#)

Performing a phased upgrade of SVS stack from version 5.1 SP1

Performing a phased upgrade involves the following tasks:

- Moving the service groups to the second subcluster
- Upgrading the SVS stack on the first subcluster
- Preparing the second subcluster
- Activating the first subcluster
- Upgrading the operating system on the second subcluster
- Upgrading the second subcluster
- Finishing the phased upgrade

Before you start the upgrade on the first half of the cluster, back up the VCS configuration files `main.cf` and `types.cf` which are in the directory `/etc/VRTSvcs/conf/config/`.

Prerequisites for a phased upgrade

Before you start the upgrade, confirm that you have licenses for all the nodes that you plan to upgrade. Note that your applications have downtime during this procedure.

Planning for a phased upgrade

Plan out the movement of the service groups from node-to-node to minimize the downtime for any particular service group. Some basic guidelines follow:

- Split the cluster in half. If the cluster has an odd number of nodes, calculate $(n+1)/2$, and start the upgrade with the even number of nodes.
- Split the cluster so that your high priority service groups remain online during the upgrade of the first subcluster.

Phased upgrade limitations

The following limitations primarily describe not to tamper with configurations or service groups during the phased upgrade:

- While you perform the upgrades, do not start any modules. Also, do not add or remove service groups to any of the nodes.
- Depending on your configuration, you may find that you cannot upgrade multiple nodes at the same time. You may only be able to upgrade one node at a time.
- For very large clusters, you might have to repeat these steps multiple times to upgrade your cluster.
- You can perform a phased upgrade when the root disk is encapsulated.

Moving the service groups to the second subcluster

To move the service groups to the second subcluster

- 1 Switch failover groups from the first half of the cluster to one of the nodes in the second half of the cluster. In this procedure, `sys1` is a node in the first half of the cluster and `sys4` is a node in the second half of the cluster. Enter the following:

```
# hagrps -switch failover_group -to sys4
```

- 2 On the first half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the applications.

- 3 On the first half of the cluster, unmount the VxFS or CFS file systems that are not managed by VCS.

```
# mount -p | grep vxfs
```

Verify that no processes use the VxFS or CFS mount point. Enter the following:

```
# fuser -c mount_point
```

Stop any processes using a VxFS or CFS mount point with the mechanism provided by the application.

Unmount the VxFS or CFS file system. Enter the following:

```
# umount /mount_point
```

- 4 On the first half of the cluster, bring all the VCS service groups offline including CVM group. Enter the following:

```
# hagr -offline group_name -sys sys1
```

When the CVM group becomes OFFLINE, all the parallel service groups such as the CFS file system will also become OFFLINE on the first half of the cluster nodes.

- 5 Verify that the VCS service groups are offline on all the nodes in first half of the cluster. Enter the following:

```
# hagr -state group_name
```

- 6 Freeze the nodes in the first half of the cluster. Enter the following:

```
# haconf -makerw
# hasys -freeze -persistent sys1
# haconf -dump -makero
```

- 7 If the cluster-wide attribute UseFence is set to SCSI3, then reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file, in first half of the cluster.

- 8 Verify that only GAB ports a, b, d and h are open. Enter the following:

```
# gabconfig -a
GAB Port Memberships
=====
Port a gen 6b5901 membership 01
Port b gen 6b5904 membership 01
Port d gen 6b5907 membership 01
Port h gen ada40f membership 01
```

Do not stop VCS. Port h should be up and running.

- 9 In the first half of the cluster, stop all VxVM and CVM volumes. Enter the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open. Enter the following:

```
# vxprint -Aht -e v_open
```

- 10 On first half of the cluster, upgrade the operating system on all the nodes, if applicable. For instructions, see the upgrade paths for the operating system.

Upgrading the SVS stack on the first subcluster

To upgrade the SVS stack on the first subcluster

- ◆ **Note:** This procedure is based on an "in-place" upgrade path; that is, if the operating system is upgraded, the release will be the same, but only the path level will change. If you are moving from major operating system release to another, you must uninstall the SVS stack before you upgrade the operating system. After the operating system is upgraded, you must reinstall SVS.
-

On the first half of the cluster, upgrade SVS by using the `installsvs` script. For example use the `installsvs` script as shown below:

```
# ./installsvs sys1
```

where `<sys1>` is the node on the first subcluster.

After the upgrade for first half of the cluster is complete, no GAB ports will be shown in `gabconfig -a` output.

To upgrade your operating system, follow the normal procedures for your platform.

Note: After the installation completes, you can safely ignore any instructions that the installer displays.

Preparing the second subcluster

To prepare the second subcluster

- 1 On the second half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the application.
[Downtime starts now.]

- 2 On the second half of the cluster, unmount the VxFS and CFS file systems that are not managed by VCS. Enter the following:

```
# mount -p | grep vxfs
```

Verify that no processes use the VxFS and CFS mount point. Enter the following:

```
# fuser -c mount_point
```

Stop any processes using a VxFS and CFS mount point with the mechanism provided by the application.

Unmount the VxFS and CFS file system. Enter the following:

```
# umount /mount_point
```

- 3 On the second half of the cluster, unfreeze all the VCS service groups on all the nodes using the following commands:

```
# haconf -makerw
# hagr -unfreeze group_name -persistent
# haconf -dump -makero
```

- 4 On the second half of the cluster, bring all the VCS service groups offline, including CVM group. Enter the following:

```
# hagr -offline group_name -sys sys4
```

- 5 On the second half of the cluster, verify that the VCS service groups are offline. Enter the following:

```
# hagr -state group_name
```

- 6 Stop VCS on the second half of the cluster. Enter the following:

```
# hastop -local
```

- 7 If the cluster-wide attribute UseFence is set to SCSI3, reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file, in second half of the cluster.
- 8 On the second half on cluster, stop the following SVS modules: VCS, VxFEN, ODM, GAB, and LLT. Enter the following:

For Solaris 9:

```
# modunload -i [modid of vxglm]
# modunload -i [modid of vxgms]
# /etc/init.d/vxodm stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

For Solaris 10 and 11:

```
# modunload -i [modid of vxglm]
# /usr/sbin/svccadm -st disable vxodm
# modunload -i [modid of vxgms]
# /usr/sbin/svccadm -st disable vxfen
# /usr/sbin/svccadm -st disable gab
# /usr/sbin/svccadm -st disable llt
```

Or

You can enter the following to stop all these processes:

```
# ./installer/installsfcfs/installsfcfsha - stop
```

Note: You can use this command to stop the processes only if you have upgraded to product version 5.1 or later. You should use the manual steps if you have upgraded from 5.0 MP3.

- 9 If the cluster-wide attribute UseFence is set to NONE, reset the value to SCSI3 in the `/etc/VRTSvcs/conf/config/main.cf` file, in first half of the cluster.

Activating the first subcluster

To activate the first subcluster

- 1 Restart the upgraded nodes in the first half of the cluster:

```
# /usr/sbin/shutdown -i6 -g0 -y
```

When the first half of the cluster nodes come up, no GAB ports are OPEN. The following command does not show any GAB ports:

```
# /sbin/gabconfig -a  
GAB Port Memberships
```

```
=====
```

- 2 If required, force gab to form a cluster after the upgraded nodes are rebooted in first half of the cluster.

```
# /sbin/gabconfig -x
```

GAB ports a, b, d and h appear in `gabconfig -a` command output.

Note: If port b and h are not up, you need to bring fencing and VCS manually online.

- 3 On the first half of the cluster, bring the VCS service groups online. Enter the following:

```
# hagrps -online group_name -sys node_name
```

After you bring the CVM service group ONLINE, all the GAB ports u, v, w and f come ONLINE and all the CFS mounts service groups also come ONLINE automatically. Only failover service groups need to be brought ONLINE manually.

- 4 Manually mount the VxFS and CFS file systems that are not managed by VCS. [Downtime ends now.]

Upgrading the operating system on the second subcluster

To upgrade the operating system on the second subcluster

- ◆ Enter the following.

For Solaris 9:

```
# modunload -i [modid of vxglm]
# modunload -i [modid of vxgms]
# /etc/init.d/vxodm stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

For Solaris 10 and 11:

```
# modunload -i [modid of vxglm]
# /usr/sbin/svccadm -st disable vxodm
# modunload -i [modid of vxgms]
# /usr/sbin/svccadm -st disable vxfen
# /usr/sbin/svccadm -st disable gab
# /usr/sbin/svccadm -st disable llt
```

Or

You can enter the following to stop all these processes:

```
# ./installer/installsfcfs/installsfcfsha - stop
```

Note: You can use this command to stop the processes only if you have upgraded to product version 5.1 or later. You should use the manual steps if you have upgraded from 5.0 MP3.

On the second half of the cluster, upgrade the operating system, if applicable. For instructions, see the upgrade paths for the operating system.

Upgrading the second subcluster

To upgrade the second subcluster

- ◆ Enter the following:

```
# ./installsvs node_name
```

Completing the phased upgrade

To complete the phased upgrade

- 1 Verify that the cluster UUID on the nodes in the second subcluster is the same as the cluster UUID on the nodes in the first subcluster. Run the following command to display the cluster UUID:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -display nodename
```

If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -copy -from_sys \  
node01 -to_sys node03 node04
```

- 2 Restart the upgraded nodes in the second half of the cluster:

```
# /usr/sbin/shutdown -i6 -g0 -y
```

When second half of the nodes come up, all the GAB ports a, b, d, h, u, v, w and f are ONLINE. Also all the CFS mounts service groups come online automatically.

- 3 Manually mount the VxFS and CFS file systems that are not managed by VCS in the second half of the cluster.
- 4 Find out which node is the CVM master. Enter the following:

```
# vxctl -c node
```

- 5 On the CVM master node, upgrade the CVM protocol. Enter the following:

```
# vxctl upgrade
```


Performing a rolling upgrade

This chapter includes the following topics:

- [Performing a rolling upgrade using the installer](#)
- [Performing a rolling upgrade of SVS using the Web-based installer](#)

Performing a rolling upgrade using the installer

Use a rolling upgrade to upgrade Symantec VirtualStore to the latest release with minimal application downtime.

About rolling upgrades

The rolling upgrade minimizes downtime for highly available clusters to the amount of time that it takes to perform a service group failover. The rolling upgrade has two main phases where the installer upgrades kernel packages in phase 1 and VCS agent packages in phase 2.

Note: You need to perform a rolling upgrade on a completely configured cluster.

The following is an overview of the flow for a rolling upgrade:

1. The installer performs prechecks on the cluster.

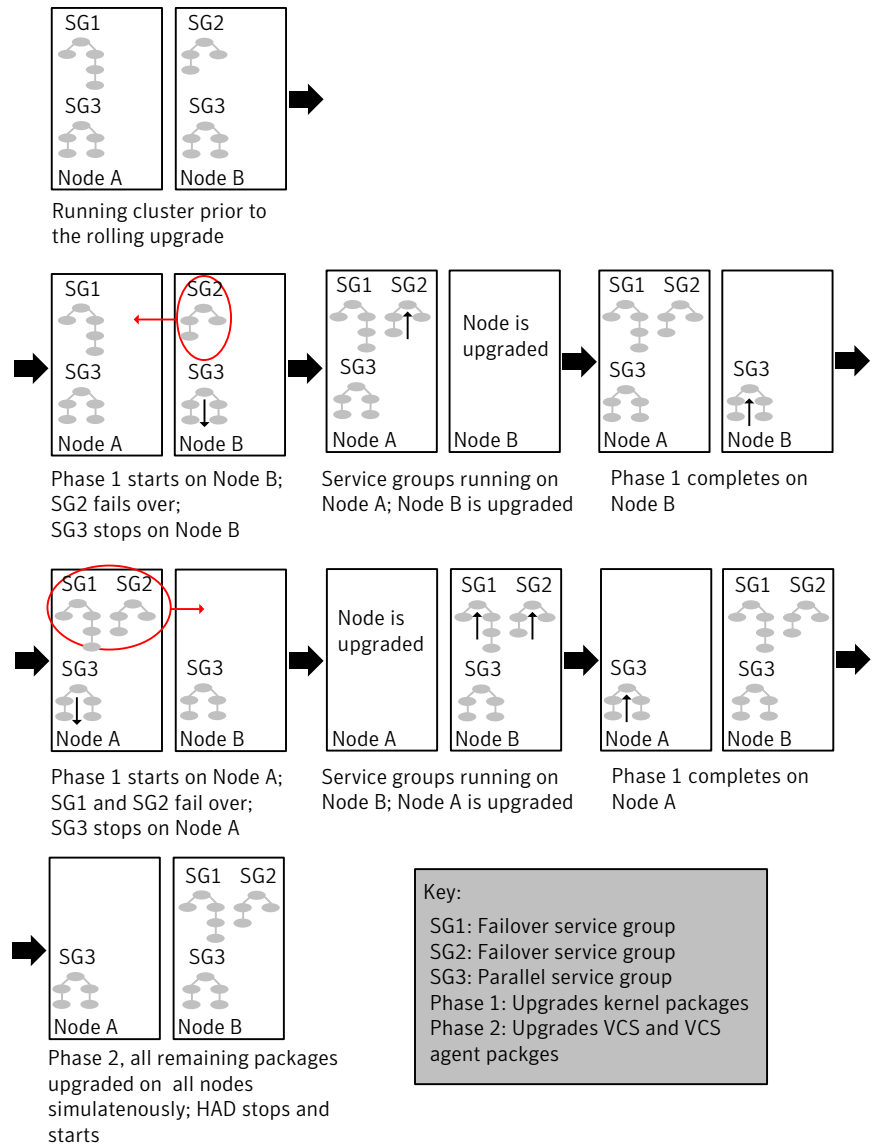
2. The installer moves service groups to free nodes for the first phase of the upgrade as is needed.

Application downtime occurs during the first phase as the installer moves service groups to free nodes for the upgrade. The only downtime that is incurred is the normal time required for the service group to fail over. The downtime is limited to the applications that are failed over and not the entire cluster.

3. The installer performs the second phase of the upgrade on all of the nodes in the cluster. The second phase of the upgrade includes downtime of the Veritas Cluster Server (VCS) engine HAD, but does not include application downtime.

[Figure 19-1](#) illustrates an example of the installer performing a rolling upgrade for three service groups on a two node cluster.

Figure 19-1 Example of the installer performing a rolling upgrade



The following limitations apply to rolling upgrades:

- Rolling upgrades are not compatible with phased upgrades. Do not mix rolling upgrades and phased upgrades.
- You can perform a rolling upgrade from 5.1 and later versions.

Supported rolling upgrade paths

You can perform a rolling upgrade of SVS with the script-based installer, the Web-based installer, or manually.

The rolling upgrade procedures support both major and minor operating system upgrades.

Table 19-1 shows the versions of SVS for which you can perform a rolling upgrade to 6.0.1.

Table 19-1 Supported rolling upgrade paths

Platform	SVS version
Solaris 10 SPARC	5.1SP1, 5.1SP1RPs, 5.1SP1PR3 6.0, 6.0RP1
Solaris 11 SPARC	6.0PR1
Solaris 10 x64	5.1SP1, 5.1SP1RPs, 5.1SP1PR3 6.0, 6.0RP1

Performing a rolling upgrade using the script-based installer

Before you start the rolling upgrade, make sure that Veritas Cluster Server (VCS) is running.

To perform a rolling upgrade

- 1 Complete the preparatory steps on the first sub-cluster.
- 2 Log in as superuser and mount the SVS 6.0.1 installation media.
- 3 From root, start the installer.

```
# ./installer
```
- 4 From the menu, select `Upgrade` and from the sub menu, select `Rolling Upgrade`.
- 5 The installer suggests system names for the upgrade. Enter `Yes` to upgrade the suggested systems, or enter `No`, and then enter the name of any one system in the cluster on which you want to perform a rolling upgrade.
- 6 The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type `y` to continue.

- 7 The installer inventories the running service groups and determines the node or nodes to upgrade in phase 1 of the rolling upgrade. Type **y** to continue. If you choose to specify the nodes, type **n** and enter the names of the nodes.
- 8 The installer performs further prechecks on the nodes in the cluster and may present warnings. You can type **y** to continue or quit the installer and address the precheck's warnings.
- 9 Review the end-user license agreement, and type **y** if you agree to its terms.
- 10 After the installer shows the package list, it detects if there are online failover service groups on the nodes to be upgraded. If there are online failover service groups, the installer prompts you to do one of the following:
 - Manually switch service groups
 - Use the CPI to automatically switch service groups

The downtime is the time that it normally takes for the service group's failover.
- 11 The installer prompts you to stop the applicable processes. Type **y** to continue.

The installer evacuates all service groups to the node or nodes that are not upgraded at this time. The installer stops parallel service groups on the nodes that are to be upgraded.
- 12 The installer stops relevant processes, uninstalls old kernel packages, and installs the new packages. When prompted, enable replication or global cluster capabilities, if required, and register the software.

The installer performs the upgrade configuration and re-starts processes.

If some processes fail to start, you may need to reboot the nodes and manually check the cluster's status.
- 13 Complete the preparatory steps on the nodes that you have not yet upgraded.
- 14 The installer begins phase 1 of the upgrade on the remaining node or nodes. Type **y** to continue the rolling upgrade.

If the installer prompts to reboot nodes, reboot the nodes.

Restart the installer.

The installer repeats step 7 through step 12.

For clusters with larger number of nodes, this process may repeat several times. Service groups come down and are brought up to accommodate the upgrade.

- 15 When phase 1 of the rolling upgrade completes, begin phase 2 of the upgrade. Phase 2 of the upgrade includes downtime for the VCS engine (HAD), which does not include application downtime. Type **y** to continue.

Reboot the nodes if the installer requires.

- 16 The installer determines the remaining packages to upgrade. Press **Enter** to continue.
- 17 The installer stops Veritas Cluster Server (VCS) processes but the applications continue to run. Type **y** to continue.

The installer performs prechecks, uninstalls old packages, and installs the new packages. It performs post-installation tasks, and the configuration for the upgrade.

- 18 Type **y** or **n** to help Symantec improve the automated installation.

- 19 If you have network connection to the Internet, the installer checks for updates.

If updates are discovered, you can apply them now.

- 20 A prompt message appears to ask if the user would like to read the summary file. You can choose **y** if you want to read the install summary file.

- 21 To upgrade VCS or Storage Foundation High Availability (SFHA) on the Coordination Point (CP) server systems to version 6.0.1, upgrade all the application clusters to 6.0.1. You then upgrade VCS or SFHA on the CP server systems.

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Performing a rolling upgrade of SVS using the Web-based installer

This section describes using the Veritas Web-based installer to perform a rolling upgrade. The installer detects and upgrades the product that is currently installed on the specified system or systems. If you want to upgrade to a different product, you may need to perform additional steps.

See [“About rolling upgrades”](#) on page 273.

To start the rolling upgrade—phase 1

- 1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.
- 2 Start the Web-based installer.
 See [“Starting the Veritas Web-based installer”](#) on page 172.
- 3 In the Task pull-down menu, select `Rolling Upgrade`.
 Click the **Next** button to proceed.
- 4 Enter the name of any one system in the cluster on which you want to perform a rolling upgrade. The installer identifies the cluster information of the system and displays the information.
 Click **Yes** to confirm the cluster information. The installer now displays the nodes in the cluster that will be upgraded during phase 1 of the upgrade.
- 5 Review the systems that the installer has chosen for phase 1 of the rolling upgrade. These systems are chosen to minimize downtime during the upgrade.
 Click **Yes** to proceed.
 The installer validates systems. If it throws an error, address the error and return to the installer.
- 6 Review the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.
- 7 If you have online failover service groups, the installer prompts you to choose to switch these service groups either manually or automatically. Choose any option and follow the steps to switch all the failover service groups to the other subcluster.
- 8 The installer stops all processes. Click **Next** to proceed.
 The installer removes old software and upgrades the software on the systems that you selected.
- 9 If you want to enable volume or file replication or global cluster capabilities, select from the following options:
 - Veritas Volume Replicator
 - Veritas File Replicator
 - Global Cluster Option
 Click **Register** to register the software. Click the **Next** button. The installer starts all the relevant processes and brings all the service groups online.

- 10 When prompted by the installer, reboot the nodes on the first half of the cluster.

Restart the installer.

- 11 Repeat step 5 through step 10 until the kernel packages of all the nodes are upgraded. For clusters with larger number of nodes, this process may get repeated several times. Service groups come down and are brought up to accommodate the upgrade.
- 12 When prompted, perform step 3 through step 10 on the nodes that you have not yet upgraded.
- 13 When prompted, start phase 2. Click **Yes** to continue with the rolling upgrade. You may need to restart the Web-based installer to perform phase 2. See “Starting the Veritas Web-based installer” on page 172.

To upgrade the non-kernel components—phase 2

- 1 In the Task pull-down menu, make sure that **Rolling Upgrade** is selected. Click the **Next** button to proceed.
- 2 The installer detects the information of cluster and the state of rolling upgrade. The installer validates systems. Click **Next**. If it throws an error, address the error and return to the installer.
- 3 Review the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.
- 4 The installer stops the `HAD` and `CmdServer` processes in phase 2 of the rolling upgrade process. Click **Next** to proceed.
- 5 The installer removes old software and upgrades the software on the systems that you selected. Review the output and click the **Next** button when prompted. Register the software and click **Next** to proceed. The installer starts all the relevant processes and brings all the service groups online.
- 6 If you have network connection to the Internet, the installer checks for updates. If updates are discovered, you can apply them now.
- 7 A prompt message appears to ask if the user would like to read the summary file. You can choose **y** if you want to read the install summary file.

The upgrade is complete.

Upgrading the operating system

This chapter includes the following topics:

- [Upgrading the Solaris operating system](#)

Upgrading the Solaris operating system

If you are running Symantec VirtualStore 6.0.1 with an earlier release of the Solaris operating system, you can upgrade the Solaris operating system using the following procedure.

Warning: You should only use this procedure to upgrade the Solaris operating system if you are running Symantec VirtualStore 6.0.1.

The directory `/opt` must exist, be writable, and must not be a symbolic link. This is because the volumes not temporarily converted by the `upgrade_start` are unavailable during the upgrade process. If you have a symbolic link from `/opt` to one of the unconverted volumes, the symbolic link will not function during the upgrade and items in `/opt` will not be installed.

To upgrade the Solaris operating system only

- 1 Bring the system down to single-user mode using the following command:

```
# init s
```

You must mount `/opt` manually if `/opt` is on its own partition.

- 2 Load and mount the software disc from the currently installed version of Symantec VirtualStore.

- 3 Change directory:

```
# cd /mount_point/scripts
```

- 4 Run the `upgrade_start` with the `-check` argument to detect any problems that exist which could prevent a successful upgrade. Use the `upgrade_start` script that was supplied with the currently installed SF release. If this command reports success, you can proceed with running the `upgrade_start` script, but if it reports errors, correct the problem(s) and rerun `upgrade_start -check`.

```
# ./upgrade_start -check
```

- 5 Run the `upgrade_start` script so that the system can come up with partitions. The `upgrade_start` script searches for volumes containing file systems, and if any are found, converts them to partitions:

```
# ./upgrade_start
```

- 6 Bring the system down to run level 0.

```
# init 0
```

- 7 Upgrade the operating system to a supported version of Solaris.

You should boot up the system from run level 0 depending on the Solaris upgrade procedure that you want to follow. Refer to the Solaris installation documentation for instructions on how to upgrade the Solaris operating system.

- 8 After installing the Solaris operating system, install any Solaris patches required by Symantec VirtualStore 6.0.1.

See the *Symantec VirtualStore Release Notes*.

- 9 After the system is up with the upgraded Solaris operating system, bring the system down to single-user mode by entering:

```
# init s
```

- 10 Ensure that `/opt` is mounted.

- 11 Load and mount the software disc from the currently installed version of Symantec VirtualStore.

- 12 If you upgraded to Solaris 10, you must reinstall certain Symantec VirtualStore packages in order to support Solaris 10 functionality.

To reinstall the required packages, follow the steps below:

- Remove the existing packages in the reverse order of their installation. For example, if you chose the installation of all packages then uninstall those in the following order.
- Run the following commands.
To obtain a list of recommended packages to install:

```
# ./installsvs -recpkgs
```

Or

To obtain a list of all packages to install:

```
# ./installsvs -allpkgs
```

- Change to the directory containing the appropriate packages.

```
# cd /mount_point/pkg
```

- Use the `pkgadd` command to install the packages from the list you generated.
- Reboot the system.

13 Complete the upgrade from the software disc from the currently installed version of Storage Foundation by entering:

```
# devlinks  
# ./upgrade_finish
```


Post-installation tasks

- [Chapter 21. Performing post-upgrade tasks](#)

Performing post-upgrade tasks

This chapter includes the following topics:

- [Changing root user into root role](#)
- [Re-joining the backup boot disk group into the current disk group](#)
- [Reverting to the backup boot disk group after an unsuccessful upgrade](#)
- [Register the new plugin](#)

Changing root user into root role

On Oracle Solaris 11, to perform installation, you need to create root user. This means that a local user cannot assume the root role. After installation, you may want to turn root user into root role for a local user, who can log in as root.

1. Log in as root user.
2. Change the root account into role.

```
# rolemod -K type=role root

# getent user_attr root

root:::type=role;auths=solaris.*;profiles=All;audit_flags=lo\
:no;lock_after_retries=no;min_label=admin_low;clearance=admin_high
```

3. Assign the root role to a local user who was unassigned the role.

```
# usermod -R root admin
```

For more information, see the Oracle documentation on Oracle Solaris 11 operating system.

Re-joining the backup boot disk group into the current disk group

Perform this procedure to rejoin the backup boot disk if you split the mirrored boot disk during upgrade. After a successful upgrade and reboot, you no longer need to keep the boot disk group backup.

See [“Performing a rolling upgrade using the installer”](#) on page 273.

To re-join the backup boot disk group

- ◆ Re-join the *backup_bootdg* disk group to the boot disk group.

```
# /etc/vx/bin/vxrootadm -Y join backup_bootdg
```

where the `-Y` option indicates a silent operation, and *backup_bootdg* is the name of the backup boot disk group that you created during the upgrade.

Reverting to the backup boot disk group after an unsuccessful upgrade

Perform this procedure if your upgrade was unsuccessful and you split the mirrored boot disk to back it up during upgrade. You can revert to the backup that you created when you upgraded.

See [“Performing a rolling upgrade using the installer”](#) on page 273.

To revert the backup boot disk group after an unsuccessful upgrade

- 1 To determine the boot disk groups, look for the *rootvol* volume in the output of the `vxprint` command.

```
# vxprint
```

- 2 Use the `vxdbg` command to find the boot disk group where you are currently booted.

```
# vxdbg bootdg
```


- 3 Boot the operating system from the backup boot disk group.
- 4 Join the original boot disk group to the backup disk group.

```
# /etc/vx/bin/vxrootadm -Y join original_bootdg
```

where the `-Y` option indicates a silent operation, and *original_bootdg* is the boot disk group that you no longer need.

Register the new plugin

After upgrading, need to register the new plugin.

Setting up Symantec VirtualStore

- [Chapter 22. Setting up VirtualStore](#)

Setting up VirtualStore

This chapter includes the following topics:

- [About setting up VirtualStore](#)
- [Disabling SMF for NFS daemons](#)
- [Setting up Clustered NFS](#)
- [Setting up the VirtualStore vSphere Service Console](#)
- [Registering the VirtualStore cluster](#)
- [Verifying the VirtualStore cluster](#)
- [Virtual machine customization pre-requisites](#)
- [VMware View Integration pre-requisites](#)
- [Unregistering the VirtualStore cluster](#)
- [Displays all the VMware vCenter Servers registered](#)
- [Useful links from VMware on NFS support and customization while cloning virtual machines](#)

About setting up VirtualStore

Table 22-1 VirtualStore tasks

To	Tasks
Set up VirtualStore	<p>See “Disabling SMF for NFS daemons” on page 294.</p> <p>See “Setting up Clustered NFS” on page 296.</p> <p>See “Setting up the VirtualStore vSphere Service Console” on page 299.</p> <p>See “Registering the VirtualStore cluster” on page 300.</p> <p>See “Verifying the VirtualStore cluster” on page 301.</p>
Unregister the VirtualStore cluster	<p>See “Unregistering the VirtualStore cluster” on page 302.</p> <p>See “Verifying the VirtualStore cluster” on page 301.</p>
Virtual machine customization pre-requisites	See “Virtual machine customization pre-requisites” on page 301.
VMware View Integration pre-requisites	See “VMware View Integration pre-requisites” on page 302.
View all the VMware vCenter Servers registered	See “Displays all the VMware vCenter Servers registered” on page 303.
View informational links	See “Useful links from VMware on NFS support and customization while cloning virtual machines” on page 303.

Disabling SMF for NFS daemons

You must disable the Service Management Facility (SMF) for the NFS daemons. UNIX start-up scripts and configuration files previously performed these functions. SMF maintains the Service Configuration Repository to store persistent configuration information as well as runtime data for all the services. All NFS daemons (*nfsd*, *mountd*, etc.) are now controlled by SMF. To keep these daemons under VCS control, modify the configuration repository to disable the SMF framework for NFS daemons.

You must invoke the following commands before bringing the NFS agent online or the agents returns an UNKNOWN state.

To keep nfsd and mountd daemons under VCS control, on all cluster nodes:

- 1 Set the `auto_enable` property to false.

```
# svccfg -s nfs/server setprop "application/auto_enable = false"
```

- 2 Refresh the SMF configuration repository.

```
# svcadm refresh nfs/server
```

- 3 Disable SMF.

```
# svcadm disable svc:/network/nfs/server:default
```

- 4 Run `svcs -a | grep -i nfs` command and review its output to make sure that SMF for `nfsd` and `mountd` is disabled.

```
# svcs -a | grep -i nfs
disabled May_29 svc:/network/nfs/server:default
```

To keep nfsmapid daemon under VCS control, on all cluster nodes:

- 1 Set the `auto_enable` property to false.

```
# svccfg -s nfs/mapid setprop "application/auto_enable = false"
```

- 2 Refresh the SMF configuration repository.

```
# svcadm refresh nfs/mapid
```

- 3 Disable SMF.

```
# svcadm disable svc:/network/nfs/mapid:default
```

- 4 Run `svcs -a | grep -i mapid` command and review its output to make sure that SMF for `nfsmapid` is disabled.

```
# svcs -a | grep -i mapid
disabled May_29 svc:/network/nfs/mapid:default
```

To keep the statd daemon under VCS control, on all cluster nodes:

- 1 Set the `auto_enable` property to false.

```
# svccfg -s nfs/status setprop "application/auto_enable = false"
```

- 2 Refresh the SMF configuration repository.

```
# svcadm refresh nfs/status
```

- 3 Disable SMF.

```
# svcadm disable svc:/network/nfs/status:default
```

- 4 Run `svcs -a | grep -i nfs` command and review its output to make sure that SMF for statd is disabled.

```
# svcs -a | grep -i nfs
disabled May_29 svc:/network/nfs/status:default
```

To keep lockd daemon under VCS control, on all cluster nodes:

- 1 Set the `auto_enable` property to false.

```
# svccfg -s nfs/nlockmgr setprop "application/auto_enable = false"
```

- 2 Refresh the SMF configuration repository.

```
# svcadm refresh nfs/nlockmgr
```

- 3 Disable SMF.

```
# svcadm disable svc:/network/nfs/nlockmgr:default
```

- 4 Run `svcs -a | grep -i nfs` command and review its output to make sure that SMF for nlockmgr is disabled.

```
# svcs -a | grep -i nlockmgr
disabled May_29 svc:/network/nfs/nlockmgr:default
```

Setting up Clustered NFS

To set up Cluster NFS (CNFS), create a metadata NFS share for VirtualStore.

Note: The file system must have disk layout Version 8 or later to use the FileSnaps of virtual machines.

See the `vxupgrade (1M)` and `mkfs_vxfs (1M)` manual pages.

To set up CNFS

- 1 Create a shared disk group from the Cluster Volume Manager (CVM) master:

```
# vxdbg -s init shared_disk_group disk1 disk2 disk3 ... diskn
```

For example:

```
# vxdbg -s init svsdg xiv0_0699 xiv0_0700 ...
```

- 2 Create a shared volume (around 100 MB) on the shared disk group to store the CNFS metadata, create a disk layout Version 8 or later file system on top, and add the shared volume to the configuration:

```
# vxassist -g shared_disk_group make svv_meta_vol 100m
# mkfs -F vxfs -o version=8 \
/dev/vx/rdisk/shared_disk_group/svv_meta_vol
# cfsshare config -p nfs shared_disk_group svv_meta_vol \
/svv_meta_mntpt
```

For example:

```
# vxassist -g svsdg make svv_meta_vol 100m
# mkfs -F vxfs -o version=8 /dev/vx/rdisk/svsdg/svv_meta_vol
# cfsshare config -p nfs svsdg svv_meta_vol /svv_meta_mntpt
```

- 3 Create another shared volume to store the VMware images, create a disk layout Version 8 or later file system on it, and add the shared volume to the configuration:

```
# vxassist -g shared_disk_group make svsdata size
# mkfs -F vxfs -o version=8 \
/dev/vx/rdisk/shared_disk_group/svs_data_vol
# cfsshare add -p nfs -N nfs_share_options shared_disk_group \
svs_data_vol /svs_data_mntpt all=[mount_options]
# cfsshare display
```

The example below assumes that you have no mount options:

```
# vxassist -g svsdg make svs_data_vol 2048g layout=striped ncol=120
# mkfs -F vxfs -o version=8 ,bsize=8192 \
/dev/vx/rdisk/svsdg/svs_data_vol
# cfsshare add -p nfs -N "rw,anon=0" svsdg svs_meta_vol \
/svs_data_mntpt all=
# cfsshare display
```

See the `mount_vxfs(1M)` manual page for all possible `mount_options`.

- 4 Add a virtual IP (VIP) address for NFS share on the Public Network or Bonded Interface:

```
# cfsshare addvip device vip_address subnet_mask
```

For example 1:

```
# cfsshare addvip bge0 192.168.1.60 255.255.255.0
```

For example 2:

```
# cfsshare addvip bond0 192.168.1.60 255.255.255.0
```

Symantec recommends creating a bond between multiple Network interface cards to increase throughput.

- 5 Add the CNFS share created and the VIP added in the above steps to configure an NFS datastore on all your ESX machines.
 - Create VMKernel Port to allow ESX to access NFS Datastores. For example, make ESX server an NFS client this requires an IP address per Server Chassis.
 - If you add an NFS datastore and it was unsuccessful, try using the `vmkping` command to ensure basic network connectivity.

- Add the NFS Datastore to the ESX Server using the **add storage Wizard** and provide the following parameters:
 - Storage type=Network File System
 - Server: *IP_address_of_NFS_share*
 - Folder: Export mount point (For example, the */svs_data_mntpt*)
 - Data Store name: A unique name for Datastore

Setting up the VirtualStore vSphere Service Console

This section describes how to set up the VirtualStore vSphere Service Console to host the VMware vSphere Plug-ins.

The vSphere Service Console consists of the following components:

- A VirtualStore node running `svsweb`.
`svsweb` is the Web Server which hosts the vSphere Plug-in.
- A VIP address that communicates between the vSphere Client and the Plug-in.

To set up VirtualStore vSphere Service Console

1. You can either add a new VIP in the cluster or use the same VIP address that you defined when you set up clustered NFS.

- To set up a new VIP:

```
# cfsshare addvip device vip_address subnet_mask
```

Example 1:

```
# cfsshare addvip bge0 192.168.1.60 255.255.255.0
```

Example 2:

```
# cfsshare addvip bond0 192.168.1.60 255.255.255.0
```

Symantec recommends that you create a bond between multiple Network interface cards to increase throughput.

- To use the VIP address that you set up earlier, skip this step.

See “Setting up Clustered NFS” on page 296.

- 2 On the svswab server node, configure the VirtualStore Web Server for cluster failover:

```
$ svsvmwadm -a setup -s vip_address
```

The following example uses the virtual IP (VIP) address added in step 1:

```
$ svsvmwadm -a setup -s 192.168.1.60
```

- 3 Verify that the VirtualStore vSphere Service Console is Online:

```
# /opt/VRTS/bin/hagrp -state ` /opt/VRTS/bin/hares -value svswab Group`
```

where svswab is the name of the Symantec VirtualStore web process.

- 4 Ensure port 14191 is open. It is required to serve the vCenter Plug-in.

Registering the VirtualStore cluster

This section describes how to register the VirtualStore cluster with VMware vCenter Server.

Registering the VirtualStore cluster with VMware vCenter Server enables you the following:

- To start using the storage (NFS exported from this cluster) as a VMware datastore.
- From the vSphere Client to invoke the VirtualStore FileSnap Wizard.

To register the VirtualStore cluster

- 1 Log in to the cluster using the virtual IP address used to set up the SVS vSphere Service Console.
- 2 Register the VirtualStore cluster with VMware vCenter Server:

```
$ svsvmwadm -a register -v vcenter_server_ip -u user \  
[-p password]
```

For example:

```
$ svsvmwadm -a register -v 192.168.1.55 -u admin -p xxxxxxx
```

- 3 List registered Plug-ins.

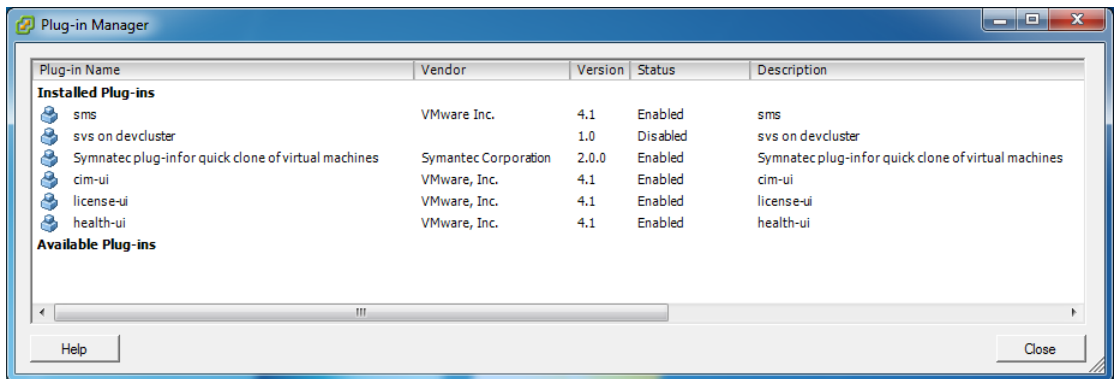
```
$ svsvmwadm -a list
```

Verifying the VirtualStore cluster

This section describes how to verify the VirtualStore cluster is installed and enabled.

To verify the VirtualStore cluster is installed and enabled

- 1 Go to vCenter VI client.
- 2 Click on **Plug-ins** and a **Plug-in Manager** window displays.
- 3 Ensure that you see **svs on *cluster_name*** in the list of installed Plug-ins.
- 4 Verify that the Plug-in is in the enabled state.



Virtual machine customization pre-requisites

Prior knowledge of VMware vSphere is required.

For more information on "Customizing Guest Operating Systems", see the *VMware vSphere Basic System Administration Guide*.

Virtual machine customization pre-requisites

- 1 VMware Tools must be installed on the virtual machine. For detailed instructions, refer to <http://kb.vmware.com/kb/1014294>.
- 2 For Windows XP, 2000 Server and 2003 Server, Microsoft Sysprep needs to be available on the vCenter Server. For detailed instructions, refer to <http://kb.vmware.com/kb/1005593>.
- 3 If customization has been applied to the virtual machine, it must be powered on in order to commit the customization changes to the guest operating system. This must be done before recustomizing.

VMware View Integration pre-requisites

Prior knowledge of VMware View is required.

For more information, see the *VMware View Administrator's Guide*.

VMware View Integration pre-requisites

- 1 VMware View Agent needs to be installed on the virtual machine.
- 2 The vCenter Server must be added to the View Connection Server. It must be added using the same address (IP or FQDN) used to login to the vCenter with the vSphere Client.

Note: Domain users which are View Administrators should not exist as local users with the same password on the View Connection Server or Active Directory Server as this may cause authentication issues.

- 3 SASL DIGEST-MD5 libraries must be installed on the VirtualStore node. The default installation of most operating systems already includes this library. If it is not installed with the OS, it should be available on the OS installation media.

```
Package name:  
RHEL: cyrus-sasl-md5  
SLES: cyrus-sasl-digestmd5
```

- 4 OpenLDAP Tools must be installed on the VirtualStore node. The default installation of most operating systems already includes this library. If it is not installed with the OS, it should be available on the OS installation media.

```
Package name: openldap-clients or openldap2-clients
```

Unregistering the VirtualStore cluster

This section describes how to unregister the VirtualStore cluster from VMware vCenter Server.

To unregister the VirtualStore cluster

- 1 Log in to the cluster using the virtual IP address used to set up the SVS vSphere Service Console.
- 2 Unregister the VirtualStore cluster from VMware vCenter Server:

```
$ svsvmwadm -a unregister -v vcenter_server_ip -u user \
[-p password]
```

For example:

```
$ svsvmwadm -a unregister -v 192.168.1.55 -u admin -p xxxxxx
```

Displays all the VMware vCenter Servers registered

This section describes how to display all the VMware vCenter Servers registered.

To display all the VMware vCenter Servers registered

- ◆ Displays all the VMware vCenter Servers registered:

```
$ svsvmwadm -a list
```

Useful links from VMware on NFS support and customization while cloning virtual machines

- Best Practices for running VMware vSphere on Network Attached Storage (White paper):
http://vmware.com/files/pdf/VMware_NFS_BestPractices_WP_EN.pdf
- VirtualCenter2 templates usage and best practices (White paper)
Best practices for setting up templates and guest customization:
http://www.vmware.com/pdf/vc_2_templates_usage_best_practices_wp.pdf

Using the extensions for Symantec VirtualStore

- [Chapter 23. Using the VirtualStore Plug-in for VMware vSphere](#)
- [Chapter 24. Using the Citrix XenDesktop extension for Symantec VirtualStore](#)

Using the VirtualStore Plug-in for VMware vSphere

This chapter includes the following topics:

- [About the VMware vSphere Plug-in for VirtualStore](#)
- [Adding storage to ESX servers](#)
- [Creating a virtual machine](#)
- [Creating virtual machine clones using Symantec FileSnap](#)
- [Specifying the number of virtual machine clones to be created](#)
- [Specifying where to create the virtual machine clones](#)
- [Specifying the guest operating system if customizing for Linux or Windows](#)
- [Specifying network customization parameters for guest operating systems if using DHCP or Static IP](#)
- [Configuring the VMware View](#)
- [Configuring Citrix XenDesktop](#)
- [Verifying the virtual machine clones](#)

About the VMware vSphere Plug-in for VirtualStore

VirtualStore provides the benefits of a highly-scalable NAS and NFS solution for VMware ESX workloads.

The VirtualStore Plug-in for VMware vSphere enables an administrator to quickly clone hundreds of virtual machines.

Adding storage to ESX servers

To add storage to ESX servers

- 1 Right-click on a datacenter, cluster, folder, or an ESX server in the **vSphere Client** window. Choose **Add storage from *clustername***, where *clustername* is the SVS cluster that has been registered with this vCenter Server, and from which you want to add storage.
- 2 In the **Add Symantec Storage** window, specify ESX server information, NFS storage, and datastore information in the appropriate fields.

ESX Servers In the **ESX Servers** table, check the ESX server(s) to which you want to add storage.

The ESX servers that are displayed under the **ESX Host Name** column depend on what entity you selected in step 1. If the entity selected is a datacenter, all the ESX servers in the datacenter are displayed. If the entity selected is a folder, all the ESX servers in the folder are displayed. If the entity selected is a cluster, then all the ESX servers in that cluster are displayed.

Basically, a datacenter, a cluster, or a folder are containers of ESX servers.

Virtual IP Address In the **NFS Storage Properties** table, in the drop-down menu, select a virtual IP address.

Share In the **NFS Storage Properties** table, in the drop-down menu, select the directory path of the NFS share.

Mount NFS Read Only In the **NFS Storage Properties** table, check if you want the mounted NFS share to be read-only.

Datastore Name A datastore name is automatically generated based on the virtual IP address and the NFS share that you selected.

You can change the datastore name to whatever you choose.

Note: The datastore name must be unique. If the datastore name is not unique, you receive an error message after clicking **Submit**.

- 3 Click **Submit**.

Creating a virtual machine

To create a virtual machine

- ◆ Create a virtual machine.

See the *VMware vSphere Virtual Machine Administration Guide*.

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_vm_admin_guide.pdf

If you plan on using or integrating the virtual machine with VMware View:

See the *VMware View Administrator's Guide*.

http://www.vmware.com/pdf/view45_admin_guide.pdf

Note: If you plan to use the vApp and OVF templates, then you must disable the vApp.

See the *Symantec VirtualStore Release Notes* for more information.

MAC address conflicts may arise if static addresses are used.

See the VMware Knowledge Base Article on changing the MAC address of a hosted virtual machine for more information.

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=507

Creating virtual machine clones using Symantec FileSnap

This section describes how to create virtual machine clones using Symantec FileSnap. FileSnap is a component of Symantec VirtualStore.

Before being able to create virtual machine clones using Symantec FileSnap, you must have registered your SVS cluster with a vCenter Server using the SVS CLI. You must also have created a virtual machine.

See “[About the VMware vSphere Plug-in for VirtualStore](#)” on page 307.

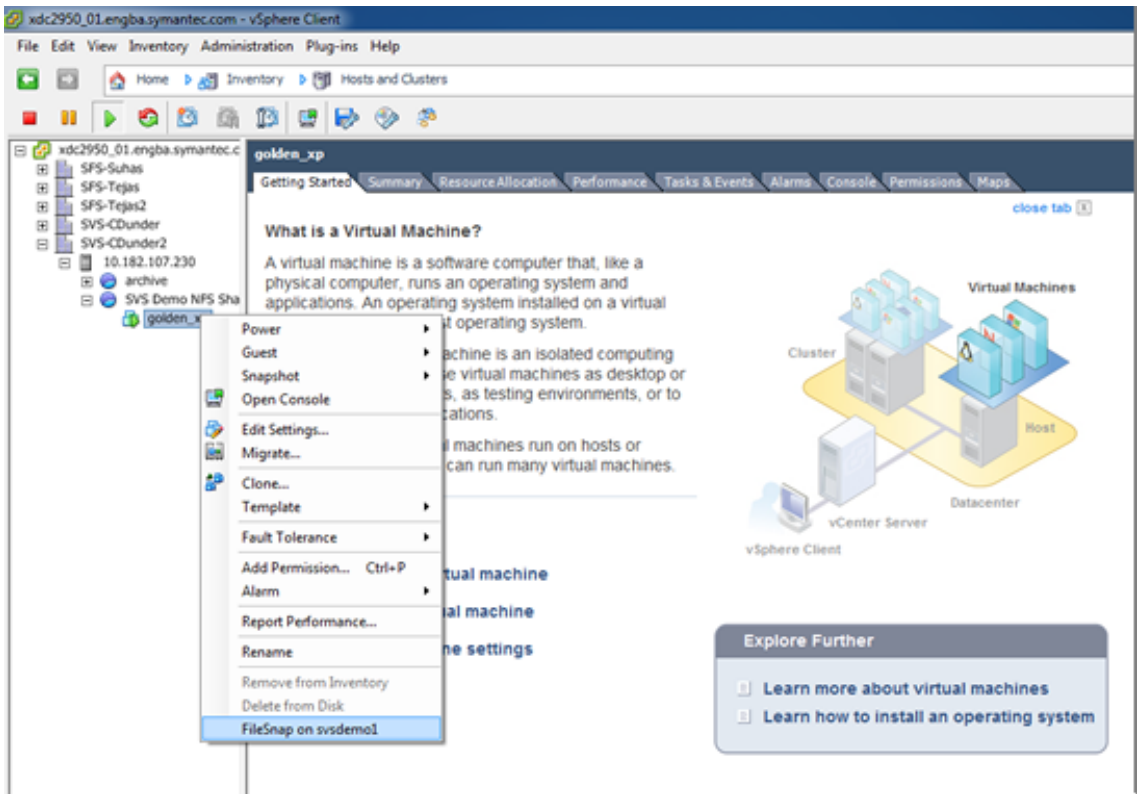
See “[Creating a virtual machine](#)” on page 309.

Note: During the use of the FileSnap wizard, if you “close” the status window this only closes the window, and does not cancel any running jobs.

To create virtual machine clones using Symantec FileSnap

- 1 Right-click on the virtual machine you want to clone, and select **FileSnap** on *clustername* in the **vSphere Client** window.

Depending upon whether the virtual disks belong to a Symantec datastore (CNFS/VirtualStore), the GUI allows or disallows the cloning operation of the virtual machine. To allow cloning, at least one virtual disk must be from a Symantec datastore. If the **NEXT** button is not displayed, then the GUI displays a message that the cloning operation is not allowed on this virtual machine.



- 2 In the **Security alert** window, click **Yes**.

Specifying the number of virtual machine clones to be created

To specify the number of virtual machine clones to be created

- 1 In the **Clone Name Pattern** window of the **Symantec Quick Clone Virtual Machine Wizard**, enter virtual machine clone information in the appropriate fields.

Number of Clones Specify the number of virtual machine clones you want to create.

Clone Name Specify the name of the virtual machine clone.
The clone name should only contain alpha-numeric characters, underscores, and or hyphens.

Start From Specify the number of the virtual machine clone that you want to start creating clones from.

- 2 Click **Next**.

Specifying where to create the virtual machine clones

To specify where to create the virtual machine clones

- 1 In the **Clone Target** window of the **Symantec Quick Clone Virtual Machine Wizard**, enter the datacenter, ESX host/cluster, and the resource pool for creating virtual machine clones in the appropriate fields.

Datacenter (required) From the drop-down menu, select the datacenter where you want the virtual machine clones to reside.

ESX Host/Cluster (required) From the drop-down menu, select the ESX host/cluster where you want the virtual machine clones to reside.

Resource Pool From the drop-down menu, select the resource pool for running the virtual machine clones.

A resource pool is a VMware term; it is a division of computing resources that are used to manage allocations between virtual machines.

Customize the guest OS and network for the virtual machine clones	If you want to customize the guest OS and network for the virtual machine clones, check the Customize the guest OS and network for the virtual machine clones checkbox.
Export virtual machines to Virtual Desktop Infrastructure (VDI)	<p>If you want to export virtual machines to Virtual Desktop Infrastructure (VDI), check the Export virtual machines to Virtual Desktop Infrastructure (VDI) checkbox.</p> <p>If you check the Export virtual machines to Virtual Desktop Infrastructure (VDI) checkbox, you can select from one of the following options:</p> <ul style="list-style-type: none">■ VMware View - allows you to configure the VMware View.■ Citrix XenDesktop (CSV file) - allows you to export a CSV file from the vCenter Server, and then download the exported CSV file to Citrix XenDesktop.

- 2 Click **Next**.

Specifying the guest operating system if customizing for Linux or Windows

To specify the guest operating system if customizing the guest operating system for Linux

- 1 In the **Guest OS Customization** window of the **Symantec Quick Clone Virtual Machine Wizard**, specify the guest operating system parameters for virtual machine clones if you want to customize the guest operating system for Linux.

Guest OS Name	Specify the guest operating system name that you want to customize.
Start From	Specify the number of the virtual machine clone that you want to start from.
Domain	Enter the active directory domain name.

- 2 Click **Next**.

To specify the guest operating system if customizing the guest operating system for Windows

- 1** In the **Guest OS Customization** window of the **Symantec Quick Clone Virtual Machine Wizard**, specify the guest operating system parameters for virtual machine clones if you want to customize the guest operating system for Windows.

Guest OS Name	Specify the guest operating system name that you want to customize. The guest OS name should only contain alpha-numeric characters and or hyphens. The full host name (concatenated Guest OS Name and Start From) cannot be greater than 63 characters.
Start From	Specify the number of the virtual machine clone that you want to start from.
Workgroup	Enter the workgroup name. If you select a domain computer (Domain), the Workgroup field is not available.
Domain	Enter the active directory domain name.
Username	Enter the domain username.
Password	Enter the domain user password.
Confirm Password	Re-enter the domain user password.
Product Key	Specify the product key for the virtual machine clone. The product key should only contain alpha-numeric characters, underscores, and or hyphens.
User Name	Specify the user name for the virtual machine clone. The user name should only contain alpha-numeric characters, underscores, and or hyphens.
Company	Specify the name of the company you are from.
Timezone	From the drop-down menu, specify the time zone for creating the virtual machine clone.

- 2** Click **Next**.

Specifying network customization parameters for guest operating systems if using DHCP or Static IP

To specify network customization parameters for guest operating systems if using DHCP

- 1 If you checked the **Customize the guest OS and network for the virtual machine clones** checkbox on the **Clone Target** window of the **Symantec Quick Clone Virtual Machine Wizard**, the **Network Customization** window appears.
Each virtual machine may have multiple network adapters.
- 2 In the **Network Customization** window, if you select **DHCP** as the **IP Assignment**, you do not need to specify values for the **IP Address**, **Netmask**, and the **Gateway** fields.
- 3 Click **Next**.

To specify network customization parameters for guest operating systems if using Static IP

- 1 If you checked the **Customize the guest OS and network for the virtual machine clones** checkbox on the **Clone Target** window of the **Symantec Quick Clone Virtual Machine Wizard**, the **Network Customization** window appears.
- 2 In the **Network Customization** window, if you select **Static IP** as the **IP Assignment**, enter information in the appropriate fields.

IP Assignment	If you select Static IP from the drop-down menu, you need to enter values for IP Address , Netmask , and Gateway fields.
IP Address	Specify a valid IP address for the network adapter card. Each virtual machine may have multiple network adapters.
Netmask	Specify a valid netmask address for the network adapter.
Gateway	Specify a valid gateway IP address for the network adapter.
Primary DNS	Enter the IP address for your primary Domain Name System (DNS) server.
Secondary DNS	Enter the IP address for your secondary Domain Name System (DNS) server.

- 3 Click **Next**.

Configuring the VMware View

To configure the VMware View

- 1 If you checked the **Export virtual machines to Virtual Desktop Infrastructure (VDI)** checkbox, and then selected the **VMware View** radio button on the **CloneTarget** window of the **Symantec Quick Clone Virtual Machine Wizard**, the **VMware View Configuration** window appears.
- 2 In the **VMware View Configuration** window, enter information in the appropriate fields to import cloned virtual machines as a new Desktop Pool in the VMware View.

Server Name/IP Address	Specify the name of the server or IP address for the server for importing cloned virtual machines. Note: You must log on to the vCenter Server using the same IP address or a fully-qualified domain name (FQDN) that the VMware View Server uses to access the vCenter Server for successful integration of the cloned virtual machines into the VMware View Server.
Username	Enter a VMware View administrator username. You must enter a username.
Password	Enter the VMware View administrator password. You must enter a password.
Domain	Enter the VMware View administrator domain name. Note: To be accessed by the VMware View Server, virtual machines must be joined to a domain. The Symantec Quick Clone Virtual Machine Wizard can automatically join virtual machine clones to the domain entered on the VMware View Configuration window.
Pool ID	Specify the pool ID for importing the cloned virtual machines. You must enter a pool ID.
Pool Persistence	Specify if you want persistent pools by checking this checkbox. Pool persistence indicates if users are allocated a dedicated desktop. This option statically assigns the desktop to a user on the first connection. All user documents, applications, and settings are retained between sessions.

- 3 Click **Next**.

Configuring Citrix XenDesktop

To configure Citrix XenDesktop

- 1 If you checked the **Customize the guest OS and network for the virtual machine clones** radio button and the **Export virtual machines to Virtual Desktop Infrastructure (VDI) - Citrix XenDesktop (CSV file)** option on the **Clone Target** window of the **Symantec Quick Clone Virtual Machine Wizard**, the **Configure Citrix XenDesktop** window appears.
- 2 In the **Configure Citrix XenDesktop** window for **Connection Name**, provide a meaningful name for this connection.

This connection name has to be same as the one created in Citrix XenDesktop.

If you click the **Details** link, you will see additional information about **Connection Name. This is the VMware vCenter connection name as provided during the XenDesktop configuration for VMware environments.**
- 3 Click **Next**.

Verifying the virtual machine clones

To verify the list of requested virtual machine clones

- 1 In the **Summary** window of the **Symantec Quick Clone Virtual Machine Wizard**, verify the list of requested virtual machine clones.
- 2 If you specified a **Connection Name** on the **Configure Citrix XenDesktop** window, you will see a message saying **The CSV file for Citrix XenDesktop will be generated.**, and the hyperlink for accessing the CSV file.
- 3 If you want to turn on the virtual machine clones after they are created, check the **Power on clones after creation** checkbox.
- 4 Click **Submit**.

Using the Citrix XenDesktop extension for Symantec VirtualStore

This chapter includes the following topics:

- [About adding virtual machine clones to Citrix XenDesktop](#)
- [Connecting Citrix XenDesktop to a vCenter Server](#)
- [Adding a connection](#)
- [Creating virtual machine clones using the Citrix XenDesktop extension](#)
- [Importing virtual machines to Citrix Desktop Studio](#)
- [Creating a desktop group and testing the deployment](#)

About adding virtual machine clones to Citrix XenDesktop

You can add virtual machine clones created on SVS to Citrix XenDesktop.

Prior to being able to use this feature, you must have already configured your VMware vCenter Server and registered your SVS cluster with the vCenter Server.

You must also have successfully installed and configured the Citrix XenDesktop controller.

Connecting Citrix XenDesktop to a vCenter Server

By default, the vCenter Server is installed with a self-signed certificate. If you are not able to replace it with a certificate issued from a certification authority, you can use the following workaround to use the self-signed certificate of the vCenter Server. On the Windows server where you installed Citrix XenDesktop, do the following.

To connect Citrix XenDesktop to a vCenter Server

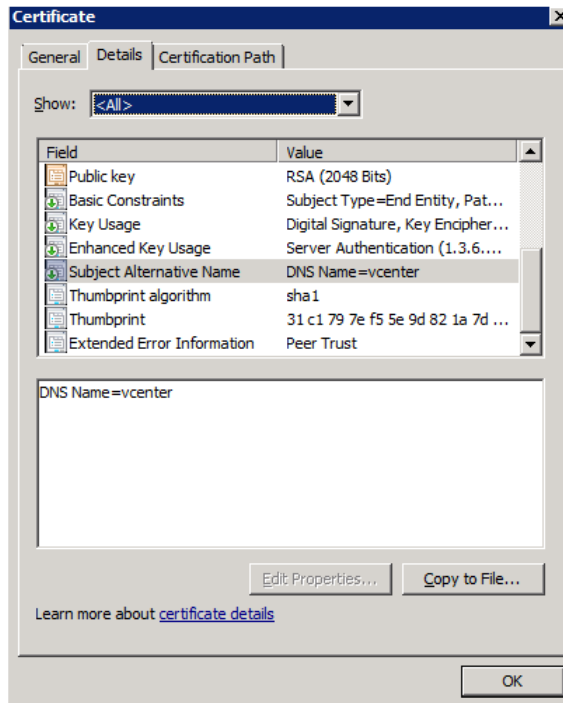
- 1 Open an Internet Explorer browser, and enter the hostname or IP address of the machine running the vCenter Server as **https://<vcenter_server>**.

You will see a certificate error.

- 2 Click the certificate error, and select **View certificate**, and click **Install certificate**.
- 3 Click the **Details** tab on the **View Certificate** dialog.

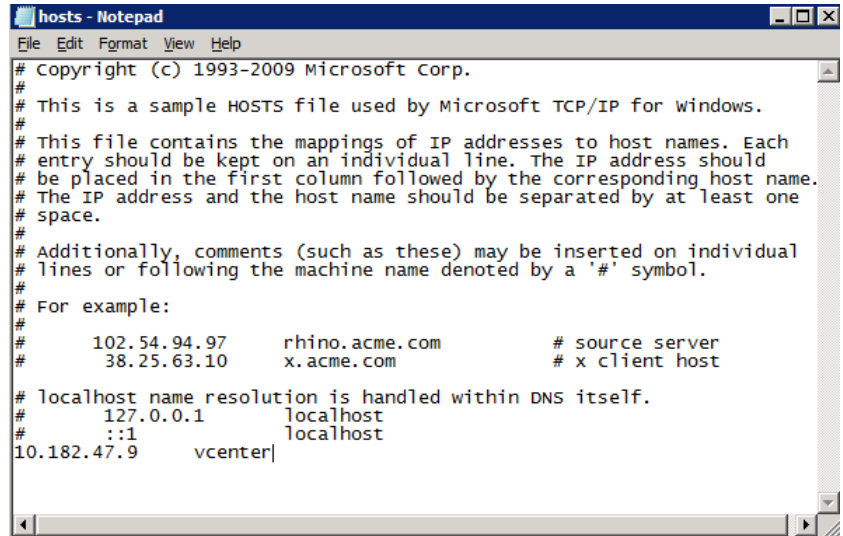
Check the DNS name in the certificate. For example, the DNS name of the vCenter Server is displayed as **vcenter**.

Make a note of the DNS name.



- 4 Open the hosts file in %SystemRoot%/WINDOWS/system32/Drivers/etc/.

Add a line with the IP address of your vCenter Server and the DNS name as displayed in the **Certificate** dialog, and save the hosts file.



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com           # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
10.182.47.9      vcenter|
```

- 5 Add a line with the IP address of your vCenter Server and the DNS name in the certificate and save the hosts file. The following is a sample.

- 6 Open a new Internet Explorer browser, and enter
`https://<vCenter_DNS_name_in_certificate>.`

If the certification error is gone, you are done, and you can move to the next step.

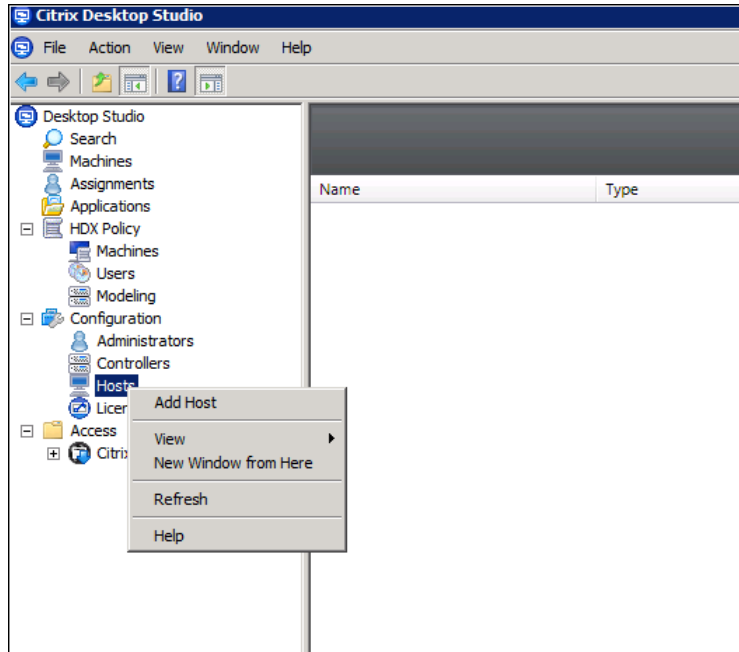
See “[Adding a connection](#)” on page 319.

Adding a connection

To add a connection

- 1 Launch **Citrix Desktop Studio** on the Windows server where you installed Citrix XenDesktop.
- 2 Select **Configuration > Hosts**.

- 3 Right-click on **Hosts**, and then select **Add Host**.



- 4 Choose **VMware virtualization** as the **Host type**.
- 5 Enter `https://<vcenter_dns_name_in_certificate>/sdk` in the **Address** text box, and enter the vCenter Server administrator's Username and Password.

- 6 Choose a **Connection name** that you like, and select **Manually create virtual machines**.

Add Host

Steps

- Host
- Summary

Host type: VMware virtualization

Address: https://vcenter/sdk

Username: administrator

Password: ●●●●●●

The Connection name will be displayed in Desktop Studio. Consider using a name that will help administrators to identify the host type and address of the deployment to which the connection relates.

Connection name: vCenter

Virtual machines:

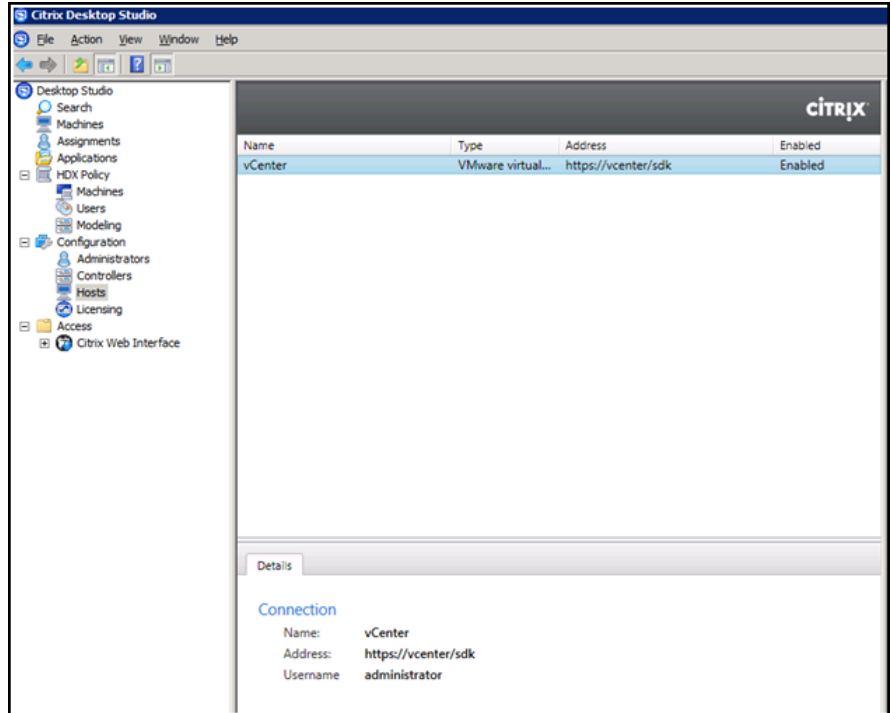
- Use XenDesktop to create virtual machines
- Manually create virtual machines

CITRIX

Back Next Cancel

7 Click **Next**.

You can see the connection name in Citrix Desktop Studio.



Creating virtual machine clones using the Citrix XenDesktop extension

This section describes how to create virtual machine clones using the Citrix XenDesktop extension with the Symantec Quick Clone Virtual Machine Wizard.

To create virtual machine clones using the Citrix XenDesktop extension

- 1 Prepare a virtual machine golden image and install Citrix XenDesktop Virtual Desktop Agent on the virtual machine.

Refer to the Citrix XenDesktop documentation for how to install the Virtual Desktop Agent.

<http://support.citrix.com/proddocs/topic/xendesktop-snma/cds-install-vda.html>

- 2 Follow the steps for creating virtual machine clones using Symantec FileSnap.

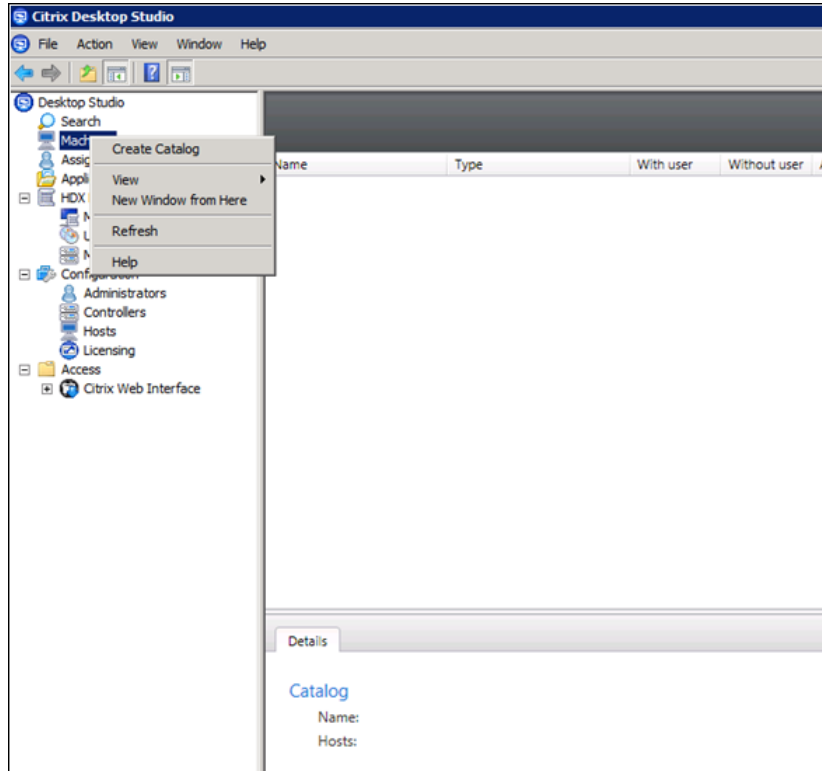
- 3 Once you have finished using the Symantec Quick Clone Virtual Machine Wizard, power on all virtual machines.
- 4 Check if the virtual machines are properly configured.

Importing virtual machines to Citrix Desktop Studio

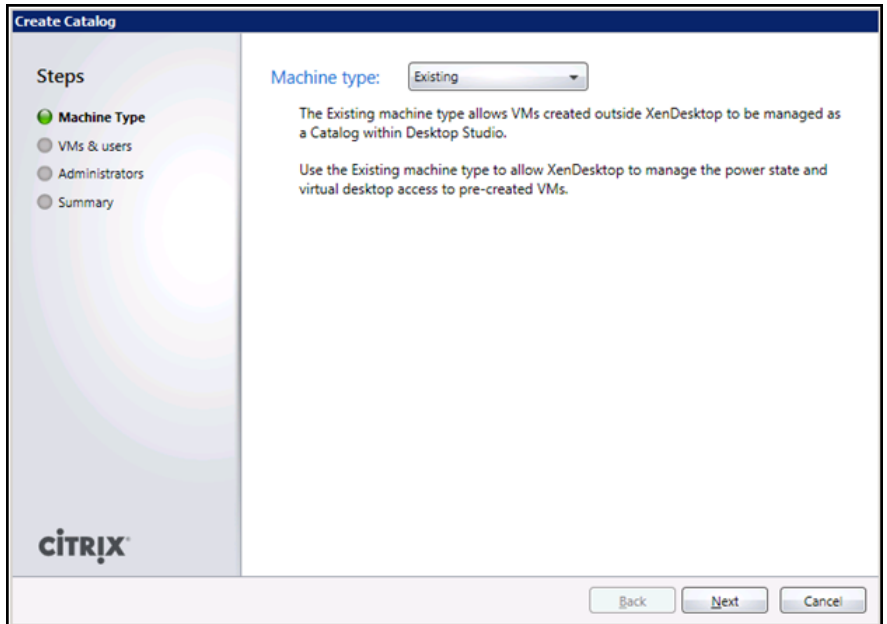
This section describes how to import virtual machines to Citrix Desktop Studio.

To import the virtual machine clones into Citrix XenDesktop

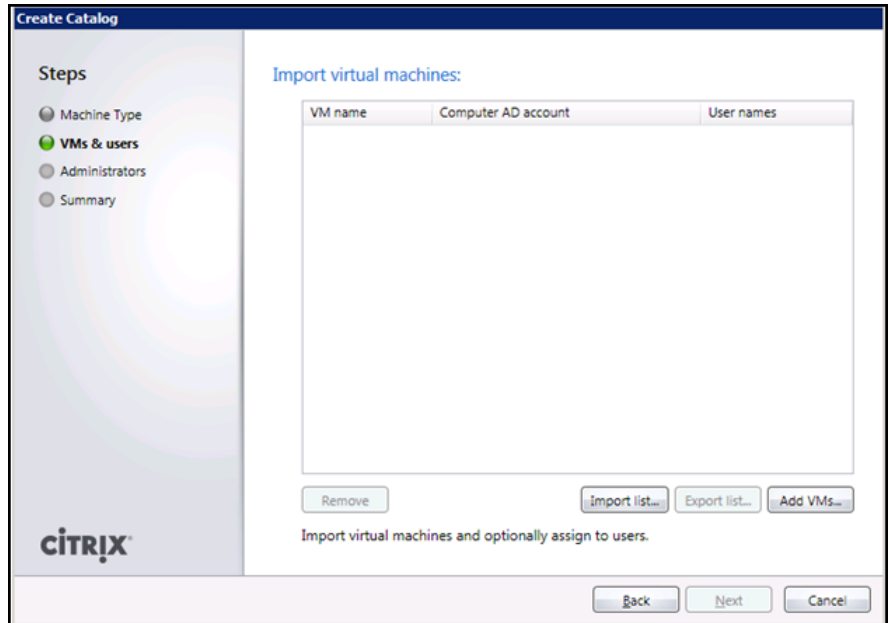
- 1 Launch Citrix Desktop Studio, and right-click **Machines**, and then select **Create Catalog**.



- 2 Select **Existing** from the **Machine type** drop-down menu.



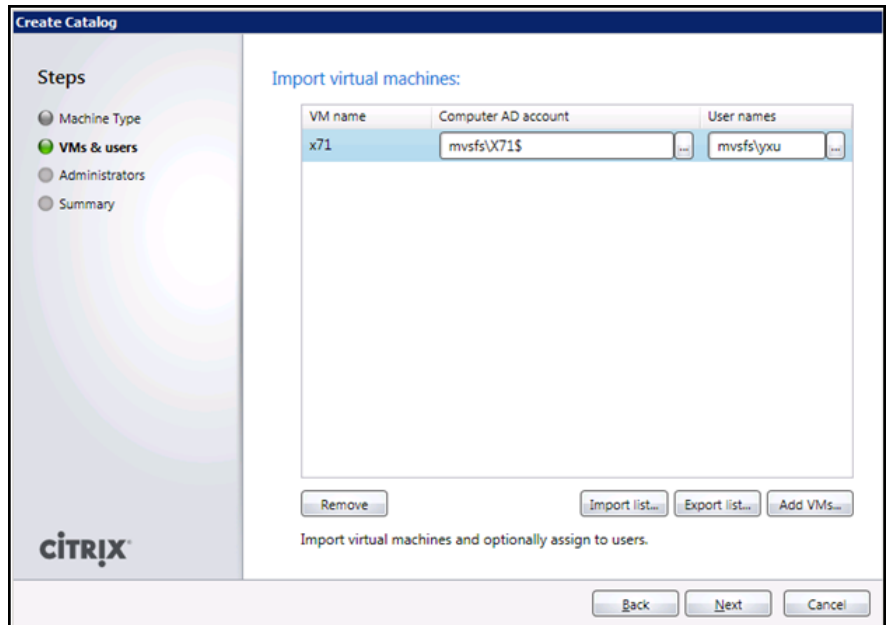
3 Click the **Import list** button.



- 4 Choose the CSV file that you saved, and click **Open**.

You will see the virtual machines listed in the CSV file.

You can change the **Computer AD** account or **User names** if you want.



- 5 Click **Next** to finish the operation.
- 6 Log into the virtual machines with the user account that you were assigned.
Verify that the virtual machines are working correctly.

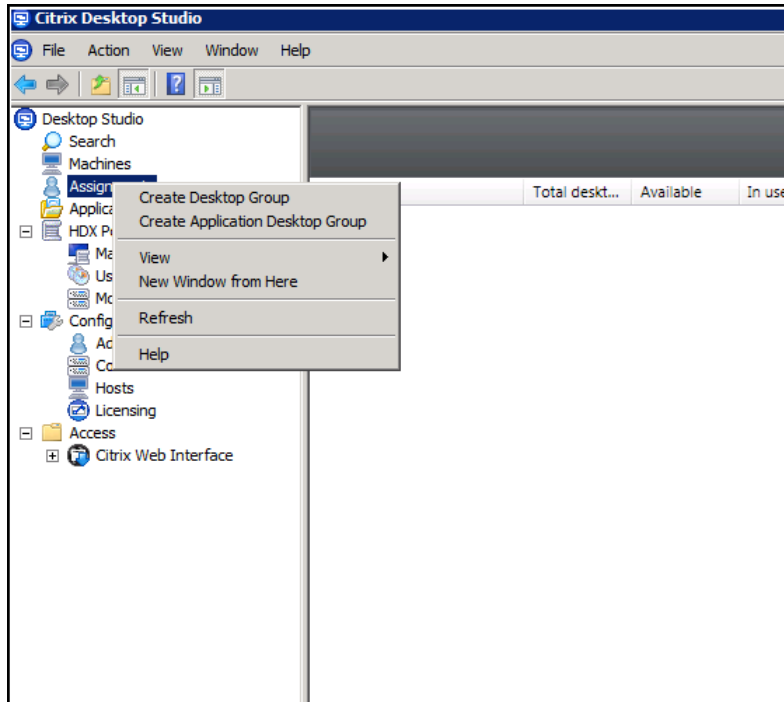
Creating a desktop group and testing the deployment

This section describes how to create a desktop group for the catalog of virtual machines that you just created.

To create a desktop group and test the deployment

- 1 At the **Citrix Desktop Studio** dialog, right-click **Assignments**, and select **Create Desktop Group**.

Follow the Wizard dialogs step-by-step.

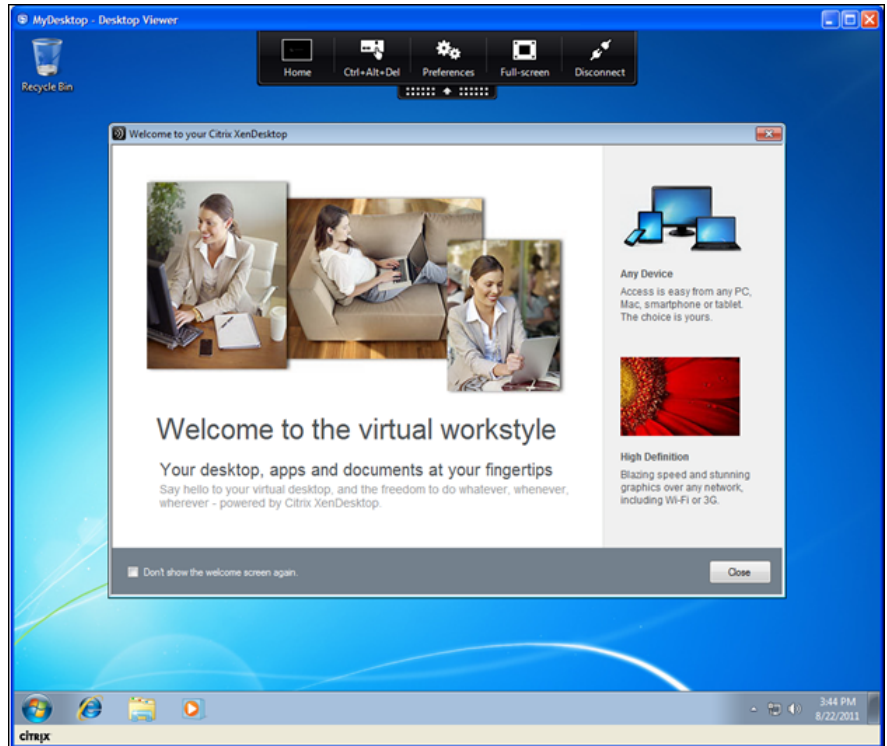


- 2 Ensure that you have installed and configured Citrix XenDesktop Virtual Desktop Agent.

See [“Creating virtual machine clones using the Citrix XenDesktop extension”](#) on page 322.

- 3 From any computer, point your browser at the controller IP address, or its fully-qualified DNS name, and authenticate it using one of the users supplied.





Adding and removing nodes

- [Chapter 25. Adding a node to a cluster](#)
- [Chapter 26. Removing a node from a cluster](#)

Adding a node to a cluster

This chapter includes the following topics:

- [About adding a node to a cluster](#)
- [Before adding a node to a cluster](#)
- [Adding a node to a cluster using the SVS installer](#)
- [Adding a node using the Web-based installer](#)
- [Adding the node to a cluster manually](#)
- [Starting Cluster Volume Manager \(CVM\) and Cluster File System \(CFS\)](#)
- [After adding the new node](#)

About adding a node to a cluster

You can add a node:

- Using the product installer
- Using the Web installer
- Manually

The following table provides a summary of the tasks required to add a node to an existing SVS cluster.

Table 25-1 Tasks for adding a node to a cluster

Step	Description
Complete the prerequisites and preparatory tasks before adding a node to the cluster.	See “Before adding a node to a cluster” on page 334.

Table 25-1 Tasks for adding a node to a cluster (*continued*)

Step	Description
Add a new node to the cluster.	See “Adding a node to a cluster using the SVS installer” on page 336. See “Adding the node to a cluster manually” on page 340.
Complete the configuration of the new node after adding it to the cluster.	See “Starting Cluster Volume Manager (CVM) and Cluster File System (CFS)” on page 350.

The example procedures describe how to add a node to an existing cluster with two nodes.

Before adding a node to a cluster

Before preparing to add the node to an existing SVS cluster, perform the required preparations.

- Verify hardware and software requirements are met.
- Set up the hardware.
- Prepare the new node.

To verify hardware and software requirements are met

- 1 Review hardware and software requirements for SVS.
- 2 Verify the new system has the same identical operating system versions and patch levels as that of the existing cluster
- 3 If the cluster is upgraded from the previous version, you must check the cluster protocol version to make sure it has the same version as the node to be added. If there is a protocol mismatch, the node is unable to join the existing cluster.

Check the cluster protocol version using:

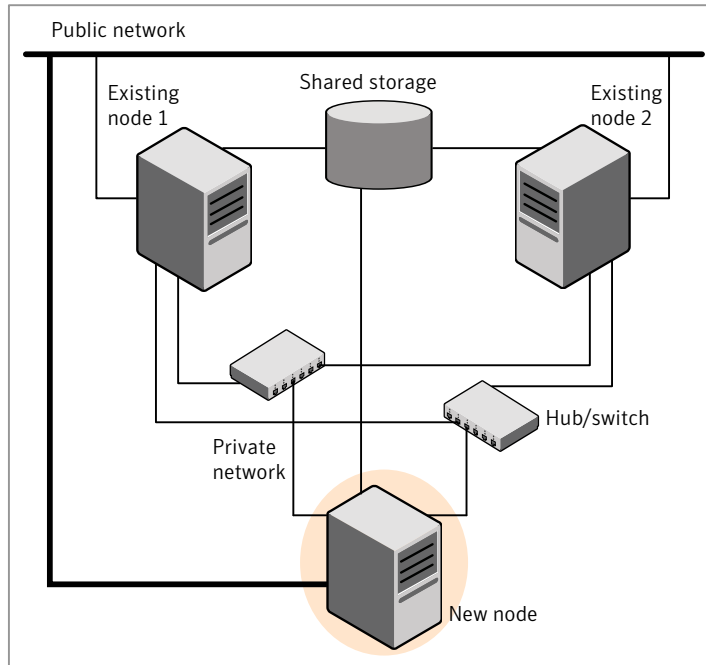
```
# vxdctl protocolversion
Cluster running at protocol 120
```

- 4 If the cluster protocol on the master node is below 120, upgrade it using:

```
# vxdctl upgrade [version]
```

Before you configure a new system on an existing cluster, you must physically add the system to the cluster as illustrated in [Figure 25-1](#).

Figure 25-1 Adding a node to a two-node cluster using two switches



To set up the hardware

1 Connect the SVS private Ethernet controllers.

Perform the following tasks as necessary:

- When you add nodes to a cluster, use independent switches or hubs for the private network connections. You can only use crossover cables for a two-node cluster, so you might have to swap out the cable for a switch or hub.
- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

[Figure 25-1](#) illustrates a new node being added to an existing two-node cluster using two independent hubs.

2 Make sure that you meet the following requirements:

- The node must be connected to the same shared storage devices as the existing nodes.

- The node must have private network connections to two independent switches for the cluster.
For more information, see the *Veritas Cluster Server Installation Guide*.
- The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster.

Complete the following preparatory steps on the new node before you add it to an existing SVS cluster.

To prepare the new node

- 1 Verify that the new node meets installation requirements.

```
# ./installsvs -precheck
```

You can also use the Web-based installer for the precheck.

- 2 Install SVS on the new system. Make sure all the VRTS packages available on the existing nodes are also available on the new node.

```
# cd /opt/VRTS/install
```

```
# ./installsvs<version>
```

Where *<version>* is the specific release version.

Do not configure SVS when prompted.

Adding a node to a cluster using the SVS installer

You can add a node to a cluster using the `-addnode` option with the SVS installer.

The SVS installer performs the following tasks:

- Verifies that the node and the existing cluster meet communication requirements.
- Verifies the products and packages installed but not configured on the new node.
- Discovers the network interfaces on the new node and checks the interface settings.
- Creates the following files on the new node:
`/etc/llttab`
`/etc/VRTSvcs/conf/sysname`
- Copies the following files on the new node:
`/etc/llthosts`


```
/etc/gabtab
/etc/VRTSvcs/conf/config/main.cf
```

- Copies the following files from the existing cluster to the new node:

```
/etc/vxfenmode
/etc/vxfendg
/etc/vx/.uuids/clusuuid
```

- Generate security credentials on the new node if the CPS server of existing cluster is secure
- Configures disk-based or server-based fencing depending on the fencing mode in use on the existing cluster.
- Adds the new node to the CVM, ClusterService, and VxSS service groups in the VCS configuration.

Note: For other service groups configured under VCS, update the configuration for the new node manually.

- Adds the new node to the CVM and ClusterService service groups in the VCS configuration.

Note: For other service groups configured under VCS, update the configuration for the new node manually.

- Starts SVS processes and configures CVM and CFS on the new node.
- Configure clustered NFS service group on the new node.

At the end of the process, the new node joins the SVS cluster.

Note: If you have configured server-based fencing on the existing cluster, make sure that the CP server does not contain entries for the new node. If the CP server already contains entries for the new node, remove these entries before adding the node to the cluster, otherwise the process may fail with an error.

To add the node to an existing cluster using the installer

- 1 Log in as the root user on one of the nodes of the existing cluster.
- 2 Run the SVS installer with the `-addnode` option.

```
# cd /opt/VRTS/install  
# ./installsvs<version> -addnode
```

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

The installer displays the copyright message and the location where it stores the temporary installation logs.

- 3 Enter the name of a node in the existing SVS cluster.

The installer uses the node information to identify the existing cluster.

```
Enter one node of the SVS cluster to which  
you would like to add one or more new nodes: sys1
```

- 4 Review and confirm the cluster information.
- 5 Enter the name of the systems that you want to add as new nodes to the cluster.

```
Enter the system names separated by spaces  
to add to the cluster: saturn
```

Confirm if the installer prompts if you want to add the node to the cluster.

The installer checks the installed products and packages on the nodes and discovers the network interfaces.

- 6 Enter the name of the network interface that you want to configure as the first private heartbeat link.

Note: The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster. The LLT configuration for the new node must be the same as that of the existing cluster.

```
Enter the NIC for the first private heartbeat
link on saturn: [b,q,?] bge1
```

```
Enter the NIC for the second private heartbeat
link on saturn: [b,q,?] bge2
```

Note: At least two private heartbeat links must be configured for high availability of the cluster.

- 7 Depending on the number of LLT links configured in the existing cluster, configure additional private heartbeat links for the new node.
 The installer verifies the network interface settings and displays the information.
- 8 Review and confirm the information.
- 9 If you have configured SMTP, SNMP, or the global cluster option in the existing cluster, you are prompted for the NIC information for the new node.

```
Enter the NIC for VCS to use on saturn: bge3
```

- 10 If the existing cluster uses server-based fencing in secure mode, the installer will configure server-based fencing in secure mode on the new nodes.
 The installer then starts all the required Veritas processes and joins the new node to cluster.
 The installer indicates the location of the log file, summary file, and response file with details of the actions performed.
- 11 Confirm that the new node has joined the SVS cluster using `lltstat -n` and `gabconfig -a` commands.
 If the new node has not joined the cluster, verify if it has been added to the `SystemList`.

Adding a node using the Web-based installer

You can use the Web-based installer to add a node to a cluster.

To add a node to a cluster using the Web-based installer

- 1 From the Task pull-down menu, select **Add a Cluster node**.

From the product pull-down menu, select the product.

Click the **Next** button.

- 2 Click **OK** to confirm the prerequisites to add a node.

- 3 In the System Names field enter a name of a node in the cluster where you plan to add the node and click **OK**.

The installer program checks inter-system communications and compatibility. If the node fails any of the checks, review the error and fix the issue.

If prompted, review the cluster's name, ID, and its systems. Click the **Yes** button to proceed.

- 4 In the System Names field, enter the names of the systems that you want to add to the cluster as nodes. Separate system names with spaces. Click the **Next** button.

The installer program checks inter-system communications and compatibility. If the system fails any of the checks, review the error and fix the issue.

Click the **Next** button. If prompted, click the **Yes** button to add the system and to proceed.

- 5 From the heartbeat NIC pull-down menus, select the heartbeat NICs for the cluster. Click the **Next** button.

- 6 Once the addition is complete, review the log files. Optionally send installation information to Symantec. Click the **Finish** button to complete the node's addition to the cluster.

Adding the node to a cluster manually

Perform this procedure after you install SVS only if you plan to add the node to the cluster manually.

Table 25-2 Procedures for adding a node to a cluster manually

Step	Description
Start the Veritas Volume Manager (VxVM) on the new node.	See “Starting Veritas Volume Manager (VxVM) on the new node” on page 341.
Configure the cluster processes on the new node.	See “Configuring cluster processes on the new node” on page 342.
If the CPS server of existing cluster is secure, generate security credentials on the new node.	See “Setting up the node to run in secure mode” on page 344.
Configure fencing for the new node to match the fencing configuration on the existing cluster. If the existing cluster is configured to use server-based I/O fencing, configure server-based I/O fencing on the new node.	See “Starting fencing on the new node” on page 349.
Start VCS.	See “To start VCS on the new node” on page 351.
Configure CVM and CFS.	
If the ClusterService group is configured on the existing cluster, add the node to the group.	See “Configuring the ClusterService group for the new node” on page 350.

Starting Veritas Volume Manager (VxVM) on the new node

Veritas Volume Manager (VxVM) uses license keys to control access. As you run the `vxinstall` utility, answer **n** to prompts about licensing. You installed the appropriate license when you ran the `installsvs` program.

To start VxVM on the new node

- 1 To start VxVM on the new node, use the `vxinstall` utility:

```
# vxinstall
```

- 2 Enter **n** when prompted to set up a system wide disk group for the system. The installation completes.

- 3 Verify that the daemons are up and running. Enter the command:

```
# vxdisk list
```

Make sure the output displays the shared disks without errors.

Configuring cluster processes on the new node

Perform the steps in the following procedure to configure cluster processes on the new node.

- 1 Edit the `/etc/llthosts` file on the existing nodes. Using `vi` or another text editor, add the line for the new node to the file. The file resembles:

```
0 sys1
1 sys2
2 sys4
```

- 2 Copy the `/etc/llthosts` file from one of the existing systems over to the new system. The `/etc/llthosts` file must be identical on all nodes in the cluster.
- 3 Create an `/etc/llttab` file on the new system. For example:

```
set-node saturn
set-cluster 101

link bge1 /dev/bge:1 - ether - -
link bge2 /dev/bge:2 - ether - -
```

Except for the first line that refers to the node, the file resembles the `/etc/llttab` files on the existing nodes. The second line, the cluster ID, must be the same as in the existing nodes.

- 4 Use `vi` or another text editor to create the file `/etc/gabtab` on the new node. This file must contain a line that resembles the following example:

```
/sbin/gabconfig -c -nN
```

Where `N` represents the number of systems in the cluster including the new node. For a three-system cluster, `N` would equal 3.

- 5 Edit the `/etc/gabtab` file on each of the existing systems, changing the content to match the file on the new system.
- 6 For the following files on the new node:

```
/etc/default/llt
/etc/default/gab
/etc/default/vxfen
/etc/default/vcs
```

Verify if the attributes in each file are set as follows before using `smf` on Solaris 10 to start the related processes and to load drivers:

```
LLT_START/LLT_STOP=1
GAB_START/GAB_STOP=1
VXFEN_START/VXFEN_STOP=1
VCS_START/VCS_STOP=1
```

- 7 Use `vi` or another text editor to create the file `/etc/VRTSvcs/conf/sysname` on the new node. This file must contain the name of the new node added to the cluster.

For example:

```
saturn
```

- 8 Create the Unique Universal Identifier file `/etc/vx/.uuids/clusuuid` on the new node:

```
# /opt/VRTSvcs/bin/uuidconfig.pl -rsh -clus -copy \
-from_sys sys1 -to_sys saturn
```

- 9 Start the LLT, GAB, and ODM drivers on the new node:

```
# svcadm enable llt
# svcadm enable gab
# svcadm restart vxodm
```

10 On the new node, verify that the GAB port memberships are a and d:

```
# gabconfig -a
GAB Port Memberships
=====
Port a gen df204 membership 012
Port b gen df20a membership 012
Port d gen df207 membership 012
```

Setting up the node to run in secure mode

You must follow this procedure only if you are adding a node to a cluster that is running in secure mode. If you are adding a node to a cluster that is not running in a secure mode, proceed with configuring LLT and GAB.

[Table 25-3](#) uses the following information for the following command examples.

Table 25-3 The command examples definitions

Name	Fully-qualified host name (FQHN)	Function
sys4	sys4.nodes.example.com	The new node that you are adding to the cluster.

Configuring the authentication broker on node sys4

To configure the authentication broker on node sys4

- 1 Extract the embedded authentication files and copy them to temporary directory:

```
# mkdir -p /var/VRTSvcs/vcsauth/bkup  
# cd /tmp; gunzip -c /opt/VRTSvcs/bin/VxAT.tar.gz | tar xvf -
```

- 2 Edit the setup file manually:

```
# cat /etc/vx/.uuids/clusuuid 2>&1
```

The output is a string denoting the UUID. This UUID (without { and }) is used as the ClusterName for the setup file.

```
{UUID}
```

```
# cat /tmp/eat_setup 2>&1
```

The file content must resemble the following example:

```
AcceptorMode=IP_ONLY  
  
BrokerExeName=vcsauthserver  
  
ClusterName=UUID  
  
DataDir=/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER  
  
DestDir=/opt/VRTSvcs/bin/vcsauth/vcsauthserver  
  
FipsMode=0  
  
IPPort=14149  
  
RootBrokerName=vcsroot_uuid  
  
SetToRBPlusABorNot=0  
  
SetupPDRs=1  
  
SourceDir=/tmp/VxAT/version
```

- 3 Set up the embedded authentication file:

```
# cd /tmp/VxAT/version/bin/edition_number; \  
./broker_setup.sh/tmp/eat_setup  
  
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssregctl -s -f  
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER/root/.VRTSat/profile \  
/VRTSatlocal.conf -b 'Security\Authentication \  
\Authentication Broker' -k UpdatedDebugLogFileName \  
-v /var/VRTSvcs/log/vcsauthserver.log -t string
```

- 4 Copy the broker credentials from one node in the cluster to sys4 by copying the entire bkup directory.

The bkup directory content resembles the following example:

```
# cd /var/VRTSvcs/vcsauth/bkup/  
  
# ls  
  
CMDSERVER  CPSADM  CPSEVER  HAD  VCS_SERVICES  WAC
```

- 5 Import the VCS_SERVICES domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atutil import -z \  
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER -f /var/VRTSvcs/vcsauth/bkup \  
/VCS_SERVICES -p password
```

- 6 Import the credentials for HAD, CMDSERVER, CPSADM, CPSEVER, and WAC.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atutil import -z \  
/var/VRTSvcs/vcsauth/data/VCS_SERVICES -f /var/VRTSvcs/vcsauth/bkup \  
/HAD -p password
```

- 7 Start the vcsauthserver process on sys4.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh
```

8 Perform the following tasks:

```
# mkdir /var/VRTSvcs/vcsauth/data/CLIENT
# mkdir /var/VRTSvcs/vcsauth/data/TRUST
# export EAT_DATA_DIR='/var/VRTSvcs/vcsauth/data/TRUST'
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat setuptrust -b \
localhost:14149 -s high
```

9 Create the `/etc/VRTSvcs/conf/config/.secure` file:

```
# touch /etc/VRTSvcs/conf/config/.secure
```

Configuring server-based fencing on the new node

This section describes the procedures to configure server-based fencing on a new node. Depending on whether server-based fencing is configured in secure or non-secure mode on the existing cluster, perform the tasks in one of the following procedures:

■ Server-based fencing in non-secure mode:

[To configure server-based fencing in non-secure mode on the new node](#)

■ Server-based fencing in secure mode:

[To configure server-based fencing with security on the new node](#)

To configure server-based fencing in non-secure mode on the new node

- 1 Log in to each CP server as the root user.
- 2 Update each CP server configuration with the new node information:

```
# cpsadm -s cps1.symantecexample.com \
-a add_node -c clus1 -h sys4 -n2
```

```
Node 2 (sys4) successfully added
```

- 3 Verify that the new node is added to the CP server configuration:

```
# cpsadm -s cps1.symantecexample.com \  
-a list_nodes
```

The new node must be listed in the command output.

- 4 Add the VCS user cpsclient@sys4 to each CP server:

```
# cpsadm -s cps1.symantecexample.com \  
-a add_user -e cpsclient@sys4 \  
-f cps_operator -g vx
```

```
User cpsclient@sys4 successfully added
```

To configure server-based fencing with security on the new node

- 1 Log in to each CP server as the root user.
- 2 Update each CP server configuration with the new node information:

```
# cpsadm -s cps1.symantecexample.com \  
-a add_node -c clus1 -h sys4 -n2
```

```
Node 2 (sys4) successfully added
```

- 3 Verify that the new node is added to the CP server configuration:

```
# cpsadm -s cps1.symantecexample.com -a list_nodes
```

The new node must be listed in the output.

Adding the new node to the vxfen service group

Perform the steps in the following procedure to add the new node to the vxfen service group.

To add the new node to the vxfen group using the CLI

- 1 On one of the nodes in the existing SVS cluster, set the cluster configuration to read-write mode:

```
# haconf -makerw
```

- 2 Add the node sys4 to the existing vxfen group.

```
# hagrps -modify vxfen SystemList -add sys4 2
```

- 3 Save the configuration by running the following command from any node in the SVS cluster:

```
# haconf -dump -makero
```

Starting fencing on the new node

Perform the following steps to start fencing on the new node.

To start fencing on the new node

- 1 For disk-based fencing on at least one node, copy the following files from one of the nodes in the existing cluster to the new node:

```
/etc/default/vxfen
/etc/vxfendg
/etc/vxfenmode
```

If you are using pure CP server-based fencing on the existing cluster, then only the /etc/vxfenmode file needs to be copied on the new node.

- 2 Start fencing on the new node:

```
# svcadm enable vxfen
```

- 3 On the new node, verify that the GAB port memberships are a, b, and d:

```
# gabconfig -a
```

```
GAB Port Memberships
```

```
=====
```

```
Port a gen      df204 membership 012
Port b gen      df20d membership 012
Port d gen      df20a membership 012
```

Configuring the ClusterService group for the new node

If the ClusterService group is configured on the existing cluster, add the node to the group by performing the steps in the following procedure on one of the nodes in the existing cluster.

To configure the ClusterService group for the new node

- 1 On an existing node, for example sys1, write-enable the configuration:

```
# haconf -makerw
```

- 2 Add the node saturn to the existing ClusterService group.

```
# hagrps -modify ClusterService SystemList -add saturn 2
```

```
# hagrps -modify ClusterService AutoStartList -add saturn
```

- 3 Modify the IP address and NIC resource in the existing group for the new node.

```
# hares -modify gcoip Device bge0 -sys saturn
```

```
# hares -modify gconic Device bge0 -sys saturn
```

- 4 Save the configuration by running the following command from any node.

```
# haconf -dump -makero
```

Starting Cluster Volume Manager (CVM) and Cluster File System (CFS)

Bring the CVM group online to start CVM and CFS on the new node.

To start CVM and CFS

- 1 Log onto one of the nodes in the existing cluster.
- 2 Bring the CVM group online on the new node:

```
# hagrps -online cvm -sys saturn
```

- 3 Verify that the CVM and CFS groups are online:

```
# hagrps -state
```

- 4 Configure cluster NFS on the new nodes. On each new node, run the command:

```
# cfsshare addnode <saturn>
```

After adding the new node

Start VCS on the new node.

To start VCS on the new node

- ◆ Start VCS on the new node:

```
# hastart
```


Removing a node from a cluster

This chapter includes the following topics:

- [Removing a node from a SVS cluster](#)

Removing a node from a SVS cluster

[Table 26-1](#) specifies the tasks that are involved in removing a node from a cluster. In the example procedure, the cluster consists of nodes sys1, sys2, and sys4; node sys4 is to leave the cluster.

Table 26-1 Tasks that are involved in removing a node

Task	Reference
<ul style="list-style-type: none"> ■ Back up the configuration file. ■ Check the status of the nodes and the service groups. 	See “Verifying the status of nodes and service groups” on page 354.
<ul style="list-style-type: none"> ■ Switch or remove any SVS service groups on the node departing the cluster. ■ Delete the node from SVS configuration. 	See “Deleting the departing node from SVS configuration” on page 355.
Modify the llthosts(4) and gabtab(4) files to reflect the change.	
If the existing cluster is configured to use server-based I/O fencing, remove the node configuration from the CP server.	See “Removing the node configuration from the CP server” on page 359.

Table 26-1 Tasks that are involved in removing a node (*continued*)

Task	Reference
For a cluster that is running in a secure mode, remove the security credentials from the leaving node.	See “Removing security credentials from the leaving node” on page 358.
On the node departing the cluster: <ul style="list-style-type: none">■ Modify startup scripts for LLT, GAB, and SVS to allow reboot of the node without affecting the cluster.■ Unconfigure and unload the LLT and GAB utilities.■ Remove the SVS packages.	See “Unloading LLT and GAB and removing VCS on the departing node” on page 359.

Verifying the status of nodes and service groups

Start by issuing the following commands from one of the nodes to remain in the cluster node sys1 or node sys2 in our example.

To verify the status of the nodes and the service groups

- 1 Make a backup copy of the current configuration file, main.cf.

```
# cp -p /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.goodcopy
```

- 2 Check the status of the systems and the service groups.

```
# hastatus -summary

-- SYSTEM STATE
-- System      State          Frozen
A sys1        RUNNING        0
A sys2        RUNNING        0
A sys4        RUNNING        0

-- GROUP STATE
-- Group       System        Probed   AutoDisabled  State
B grp1        sys1          Y        N              ONLINE
B grp1        sys2          Y        N              OFFLINE
B grp2        sys1          Y        N              ONLINE
B grp3        sys2          Y        N              OFFLINE
B grp3        sys4          Y        N              ONLINE
B grp4        sys4          Y        N              ONLINE
```

The example output from the `hastatus` command shows that nodes `sys1`, `sys2`, and `sys4` are the nodes in the cluster. Also, service group `grp3` is configured to run on node `sys2` and node `sys4`, the departing node. Service group `grp4` runs only on node `sys4`. Service groups `grp1` and `grp2` do not run on node `sys4`.

Deleting the departing node from SVS configuration

Before you remove a node from the cluster you need to identify the service groups that run on the node.

You then need to perform the following actions:

- Remove the service groups that other service groups depend on, or
- Switch the service groups to another node that other service groups depend on.

To remove or switch service groups from the departing node

- 1 Switch failover service groups from the departing node. You can switch grp3 from node sys4 to node sys2.

```
# hagrps -switch grp3 -to sys2
```

- 2 Check for any dependencies involving any service groups that run on the departing node; for example, grp4 runs only on the departing node.

```
# hagrps -dep
```

- 3 If the service group on the departing node requires other service groups—if it is a parent to service groups on other nodes—unlink the service groups.

```
# haconf -makerw  
# hagrps -unlink grp4 grp1
```

These commands enable you to edit the configuration and to remove the requirement grp4 has for grp1.

- 4 Stop SVS on the departing node:

```
# hastop -sys sys4
```

To stop VCS using SMF, run the following command:

```
# svcadm disable vcs
```

- 5 Check the status again. The state of the departing node should be EXITED. Make sure that any service group that you want to fail over is online on other nodes.

```
# hastatus -summary

-- SYSTEM STATE
-- System      State          Frozen
A sys1        RUNNING        0
A sys2        RUNNING        0
A sys4        EXITED         0

-- GROUP STATE
-- Group       System      Probed   AutoDisabled   State
B grp1        sys1        Y        N               ONLINE
B grp1        sys2        Y        N               OFFLINE
B grp2        sys1        Y        N               ONLINE
B grp3        sys2        Y        N               ONLINE
B grp3        sys4        Y        Y               OFFLINE
B grp4        sys4        Y        N               OFFLINE
```

- 6 Delete the departing node from the SystemList of service groups grp3 and grp4.

```
# haconf -makerw
# hagr -modify grp3 SystemList -delete sys4
# hagr -modify grp4 SystemList -delete sys4
```

Note: If sys4 was in the autostart list, then you need to manually add another system in the autostart list so that after reboot, the group comes online automatically.

- 7 For the service groups that run only on the departing node, delete the resources from the group before you delete the group.

```
# hagr -resources grp4
    processx_grp4
    processy_grp4
# hares -delete processx_grp4
# hares -delete processy_grp4
```

- 8 Delete the service group that is configured to run on the departing node.

```
# hagrps -delete grp4
```

- 9 Check the status.

```
# hastatus -summary
-- SYSTEM STATE
-- System      State          Frozen
A sys1        RUNNING        0
A sys2        RUNNING        0
A sys4        EXITED         0

-- GROUP STATE
-- Group       System      Probed   AutoDisabled  State
B grp1        sys1       Y        N              ONLINE
B grp1        sys2       Y        N              OFFLINE
B grp2        sys1       Y        N              ONLINE
B grp3        sys2       Y        N              ONLINE
```

- 10 Delete the node from the cluster.

```
# hasys -delete sys4
```

- 11 Save the configuration, making it read only.

```
# haconf -dump -makero
```

Removing security credentials from the leaving node

If the leaving node is part of a cluster that is running in a secure mode, you must remove the security credentials from node sys4. Perform the following steps.

To remove the security credentials

- 1 Stop the AT process.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh \
stop
```

- 2 Remove the credentials.

```
# rm -rf /var/VRTSvcs/vcsauth/data/
```

Removing the node configuration from the CP server

After removing a node from a SVS cluster, perform the steps in the following procedure to remove that node's configuration from the CP server.

Note: The `cpsadm` command is used to perform the steps in this procedure. For detailed information about the `cpsadm` command, see the *Symantec VirtualStore Administrator's Guide*.

To remove the node configuration from the CP server

- 1 Log into the CP server as the root user.
- 2 View the list of VCS users on the CP server, using the following command:

```
# cpsadm -s cp_server -a list_users
```

Where `cp_server` is the virtual IP/ virtual hostname of the CP server.

- 3 Remove the VCS user associated with the node you previously removed from the cluster.

For CP server in non-secure mode:

```
# cpsadm -s cp_server -a rm_user \  
-e cpsclient@sys4 -f cps_operator -g vx
```

- 4 Remove the node entry from the CP server:

```
# cpsadm -s cp_server -a rm_node -h sys4 -c clus1 -n 2
```

- 5 View the list of nodes on the CP server to ensure that the node entry was removed:

```
# cpsadm -s cp_server -a list_nodes
```

Unloading LLT and GAB and removing VCS on the departing node

Perform the tasks on the node that is departing the cluster.

You can use script-based installer to uninstall VCS on the departing node or perform the following manual steps.

If you have configured Symantec VirtualStore as part of the Storage Foundation and High Availability products, you may have to delete other dependent packages before you can delete all of the following ones.

To unconfigure and unload LLT and GAB and remove SVS

- 1 If you had configured I/O fencing in enabled mode, then stop I/O fencing.

```
# svcadm disable -t vxfen
```

- 2 Unconfigure GAB and LLT:

```
# /sbin/gabconfig -U  
# /sbin/lltconfig -U
```

- 3 Unload the GAB and LLT modules from the kernel.

- Determine the kernel module IDs:

```
# modinfo | grep gab  
# modinfo | grep llc
```

The module IDs are in the left-hand column of the output.

- Unload the module from the kernel:

```
# modunload -i gab_id  
# modunload -i llt_id
```

- 4 Disable the startup files to prevent LLT, GAB, or SVS from starting up:

```
# /usr/sbin/svcadm disable -t llc  
# /usr/sbin/svcadm disable -t gab  
# /usr/sbin/svcadm disable -t vcs
```

- 5 To determine the packages to remove, enter:

```
# pkginfo | grep VRTS
```


- 6 To permanently remove the SVS packages from the system, use the `pkgrm` command. Start by removing the following packages, which may have been optionally installed, in the order shown below.

On Solaris10:

```
# pkgrm VRTSvcsea
# pkgrm VRTSat
# pkgrm VRTSvcstag
# pkgrm VRTScps
# pkgrm VRTSvc
# pkgrm VRTSamf
# pkgrm VRTSvxfen
# pkgrm VRTSgab
# pkgrm VRTSllt
# pkgrm VRTSspt
# pkgrm VRTSsfcp601
# pkgrm VRTSperl
# pkgrm VRTSvlic
```

On Solaris 11:

```
# pkg uninstall VRTSvcsea VRTSsat VRTSvcstag
VRTScps VRTSvc VRTSamf VRTSvxfen VRTSgab VRTSllt VRTSspt
VRTSsfcp601 VRTSperl VRTSvlic
```

- 7 Remove the LLT and GAB configuration files.

```
# rm /etc/llttab
# rm /etc/gabtab
# rm /etc/llthosts
```

- 8 Remove the language packages and patches.

Uninstallation of Symantec VirtualStore

- [Chapter 27. Uninstalling Symantec VirtualStore](#)

Uninstalling Symantec VirtualStore

This chapter includes the following topics:

- [About removing Symantec VirtualStore](#)
- [Shutting down cluster operations](#)
- [Disabling the agents on a system](#)
- [Removing the Replicated Data Set](#)
- [Uninstalling SVS packages using the script-based installer](#)
- [Uninstalling SVS with the Veritas Web-based installer](#)
- [Removing the CP server configuration using the installer program](#)

About removing Symantec VirtualStore

This section covers uninstallation requirements and steps to uninstall the Veritas software.

Only users with superuser privileges can uninstall Symantec VirtualStore.

Warning: Failure to follow the instructions in the following sections may result in unexpected behavior.

Preparing to uninstall

Review the following removing the Veritas software.

Remote uninstallation

You must configure remote communication to uninstall SVS on remote systems. In a High Availability environment, you must meet the prerequisites to uninstall on all nodes in the cluster at one time.

The following prerequisites are required for remote uninstallation:

- Communication protocols must exist between systems. By default, the uninstall scripts use ssh.
- You must be able to execute ssh or rsh commands as superuser on all systems.
- The ssh or rsh must be configured to operate without requests for passwords or passphrases.

See [“About configuring secure shell or remote shell communication modes before installing products”](#) on page 415.

Preparing to remove Veritas Volume Manager

This section describes the steps you need to take before removing Veritas Volume Manager (VxVM) to preserve the contents of the volumes.

Warning: Failure to follow the preparations in this section might result in unexpected behavior.

Moving volumes from an encapsulated root disk

Use the following procedure to move volumes from an encapsulated root disk.

To uninstall VxVM if root, swap, usr, or var is a volume under Volume Manager control

- 1 Ensure that the `rootvol`, `swapvol`, `usr`, and `var` volumes have only one associated plex each.

The plex must be contiguous, non-striped, non-spanned, and non-sparse. To obtain this information, enter the following:

```
# vxprint -ht rootvol swapvol usr var
```

If any of these volumes have more than one associated plex, remove the unnecessary plexes using the following command:

```
# vxplex -o rm dis plex_name
```

- 2 Run the `vxunroot` command:

```
# /etc/vx/bin/vxunroot
```

The `vxunroot` command changes the volume entries in `/etc/vfstab` to the underlying disk partitions for `rootvol`, `swapvol`, `usr`, and `var`. It also modifies `/etc/system` and prompts for a reboot so that disk partitions are mounted instead of volumes for `root`, `swap`, `usr`, and `var`.

- 3 Once you have changed the `root`, `swap`, `usr`, and `var` volumes, move all remaining volumes to disk partitions.

You can do this using one of the following procedures:

- Back up the entire system to tape and then recover from tape.
- Back up each file system individually and then recover them all after creating new file systems on disk partitions.
- Move volumes incrementally to disk partitions.
See [“Moving volumes to disk partitions”](#) on page 367.
Otherwise, shut down VxVM.

Moving volumes to disk partitions

Use the following procedure to move volumes incrementally to disk partitions.

To move volumes incrementally to disk partitions

- 1 Evacuate disks using `vxdiskadm`, the VOM GUI, or the `vxevac` utility.

Evacuation moves subdisks from the specified disks to target disks. The evacuated disks provide the initial free disk space for volumes to be moved to disk partitions.

- 2 Remove the evacuated disks from VxVM control by entering:

```
# vxdg rmdisk diskname  
# vxdisk rm devname
```

- 3 Decide which volume to move first, and if the volume is mounted, unmount it.
- 4 If the volume is being used as a raw partition for database applications, make sure that the application is not updating the volume and that you have applied the `sync` command to the data on the volume.
- 5 Create a partition on free disk space of the same size as the volume using the `format` command.

If there is not enough free space for the partition, add a new disk to the system for the first volume removed. Subsequent volumes can use the free space generated by the removal of this first volume.

- 6 Copy the data on the volume onto the newly created disk partition using a command such as `dd`.

```
# dd if=/dev/vx/dsk/diskgroup/lhome of=/dev/dsk/c2t2d2s7
```

where `c2t2d2` is the disk outside of Volume Manager and `s7` is the newly created partition.

- 7 Replace the entry for that volume (if present) in `/etc/vfstab` with an entry for the newly created partition.
- 8 Mount the disk partition if the corresponding volume was previously mounted.
- 9 Stop and remove the volume from VxVM using the commands.

```
# vxvol -g diskgroup stop volume_name  
# vxedit -rf rm volume_name
```


- 10** Remove any free disks (those having no subdisks defined on them) by removing the volumes from VxVM control.

To check if there are still some subdisks remaining on a particular disk, use the `vxprint` command.

```
# vxprint -g diskgroup -F '%sdnum' diskname
```

If the output is not 0, there are still some subdisks on this disk that you need to remove. If the output is 0, remove the disk from VxVM control.

```
# vxdg rmdisk diskname
# vxdisk rm devname
```

Use the free space created for adding the data from the next volume you want to remove.

- 11** After you successfully convert all volumes into disk partitions, reboot the system.
- 12** After the reboot, make sure none of the volumes are open by using the `vxprint` command.

```
# vxprint -Aht -e v_open
```

- 13** If any volumes remain open, repeat the steps listed above.

Example of moving volumes to disk partitions on Solaris

This example shows how to move the data on a volume to a disk partition. In the example, there are three disks: `disk1` and `disk2` are subdisks on volume `vol101` and `disk3` is a free disk. The data on `vol101` is copied to `disk3` using `vxevac`.

These are the contents of the disk group `voldg` before the data on `vol101` is copied to `disk3`.

```
# vxprint -g voldg -ht
DG NAME  NCONFIG  NLOG      MINORS    GROUP-ID
DM NAME  DEVICE   TYPE      PRIVLEN   PUBLN     STATE
RV NAME  RLINK_CNT KSTATE    STATE     PRIMARY   DATAVOLS  SRL
RL NAME  RVG      KSTATE    STATE     REM_HOST  REM_DG     REM_RLNK
V  NAME  RVG      KSTATE    STATE     LENGTH    READPOL    PREFPLEX  UTYPE
PL NAME  VOLUME   KSTATE    STATE     LENGTH    LAYOUT     NCOL/WID  MODE
SD NAME  PLEX     DISK      DISKOFFS  LENGTH    [COL/]OFF  DEVICE    MODE
SV NAME  PLEX     VOLNAME   NVOLLAYR  LENGTH    [COL/]OFF  AM/NM     MODE
DC NAME  PARENTVOL LOGVOL
SP NAME  SNAPVOL  DCO
```

```
dg voldg default    default 115000
1017856044.1141.hostname.veritas.com
```

```
dm disk1 c1t12d0s2 sliced 2591    17900352 -
dm disk2 c1t14d0s2 sliced 2591    17899056 -
dm disk3 c1t3d0s2  sliced 2591    17899056 -
```

```
v  vol1 -          ENABLED ACTIVE  4196448 ROUND    -          fsgen
pl pl1  vol1      ENABLED ACTIVE  4196448 CONCAT   -          RW
sd sd1  pl1       disk1  0          2098224  0          c1t12d0  ENA
sd sd2  pl1       disk2  0          2098224  2098224   c1t14d0  ENA
```

Evacuate disk1 to disk3.

```
# /etc/vx/bin/vxevac -g voldg disk1 disk3
# vxprint -g voldg -ht
```

```
DG NAME  NCONFIG  NLOG    MINORS  GROUP-ID
DM NAME  DEVICE   TYPE    PRIVLEN PUBLEN  STATE
RV NAME  RLINK_CNT KSTATE  STATE   PRIMARY DATAVOLS  SRL
RL NAME  RVG      KSTATE  STATE   REM_HOST REM_DG     REM_RLNK
V  NAME  RVG      KSTATE  STATE   LENGTH  READPOL   PREFPLEX  UTYPE
PL NAME  VOLUME   KSTATE  STATE   LENGTH  LAYOUT    NCOL/WID  MODE
SD NAME  PLEX     DISK    DISKOFFS LENGTH  [COL/]OFF DEVICE    MODE
SV NAME  PLEX     VOLNAME NVOLLAYR LENGTH  [COL/]OFF AM/NM    MODE
DC NAME  PARENTVOL LOGVOL
SP NAME  SNAPVOL  DCO
```

```
dg voldg default    default 115000
1017856044.1141.hostname.veritas.com
```

```
dm disk1 c1t12d0s2 sliced 2591    17900352 -
dm disk2 c1t14d0s2 sliced 2591    17899056 -
dm disk3 c1t3d0s2  sliced 2591    17899056 -
```

```
v  vol1 -          ENABLED ACTIVE  4196448 ROUND    -          fsgen
pl pl1  vol1      ENABLED ACTIVE  4196448 CONCAT   -          RW
sd disk3-0111 disk3  0          2098224  0          c1t3d0  ENA
sd sd2  pl1       disk2  0          2098224  2098224   c1t14d0  ENA
```

Evacuate disk2 to disk3.

```
# /etc/vx/bin/vxevac -g voldg disk2 disk3
# vxprint -g voldg -ht
```

```
DG NAME      NCONFIG  NLOG      MINORS     GROUP-ID
DM NAME      DEVICE   TYPE      PRIVLEN    PUBLLEN    STATE
RV NAME      RLINK_CNT KSTATE    STATE      PRIMARY    DATAVOL    SRL
RL NAME      RVG      KSTATE    STATE      REM_HOST   REM_DG      REM_RLNK
V  NAME      RVG      KSTATE    STATE      LENGTH     READPOL     PREFPLEX    UTYPE
PL NAME      VOLUME   KSTATE    STATE      LENGTH     LAYOUT      NCOL/WID    MODE
SD NAME      PLEX     DISK      DISKOFFS   LENGTH     [COL/]OFF  DEVICE      MODE
SV NAME      PLEX     VOLNAME   NVOLLAYR   LENGTH     [COL/]OFF  AM/NM      MODE
DC NAME      PARENTVOL LOGVOL
SP NAME      SNAPVOL  DCO
```

```
dg voldg      default    default    115000
1017856044.1141.hostname.veritas.com
```

```
dm disk1     c1t12d0s2 sliced    2591     17900352 -
dm disk2     c1t14d0s2 sliced    2591     17899056 -
dm disk3     c1t3d0s2  sliced    2591     17899056 -
```

```
v  vol1      -          ENABLED  ACTIVE   4196448  ROUND    -          fsgen
pl  pl1      vol1      ENABLED  ACTIVE   4196448  CONCAT   -          RW
sd  disk3-01 pl1       disk3     0        2098224  0        c1t3d0    ENA
sd  disk3-02 pl1       disk3     2098224  2098224  2098224  c1t3d0    ENA
```

Remove the evacuated disks from VxVM control.

```
# vxdisk -g voldg list
```

```
DEVICE      TYPE      DISK      GROUP      STATUS
c1t3d0s2    sliced    disk3     voldg      online
c1t12d0s2    sliced    disk1     voldg      online
c1t14d0s2    sliced    disk2     voldg      online
```

```
# vxdg rmdisk disk1
```

```
# vxdg rmdisk disk2
```

```
# vxdisk rm c1t12d0
```

```
# vxdisk rm c1t14d0
```

Verify that the evacuated disks have been removed from VxVM control.

```
# vxdisk -g voldg list
```

```
DEVICE      TYPE      DISK      GROUP      STATUS
c1t3d0s2    sliced    disk3     voldg      online
```

Check to see whether the volume you want to move first is mounted.

```
# mount | grep voll
/voll on /dev/vx/dsk/voldg/voll
read/write/setuid/log/nolargefiles/dev=12dc138 on Wed Apr
3 10:13:11 2002
```

Create a partition on free disk space of the same size as the volume. In this example, a 2G partition is created on `disk1` (`clt12d0s1`).

```
# format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
  0. c0t0d0 <SUN9.0G cyl 4924 alt 2 hd 27 sec 133>
    /sbus@1f,0/SUNW,fas@e,8800000/sd@0,0
  1. clt3d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
    /sbus@1f,0/SUNW,fas@2,8800000/sd@3,0
  2. clt9d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
    /sbus@1f,0/SUNW,fas@2,8800000/sd@9,0
  3. clt10d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
    /sbus@1f,0/SUNW,fas@2,8800000/sd@a,0
  4. clt11d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
    /sbus@1f,0/SUNW,fas@2,8800000/sd@b,0
  5. clt12d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
    /sbus@1f,0/SUNW,fas@2,8800000/sd@c,0
  6. clt14d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
    /sbus@1f,0/SUNW,fas@2,8800000/sd@e,0
  7. clt15d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
    /sbus@1f,0/SUNW,fas@2,8800000/sd@f,0

Specify disk (enter its number): 5
selecting clt12d0
[disk formatted]

FORMAT MENU:
disk          - select a disk
type          - select (define) a disk type
partition    - select (define) a partition table
current      - describe the current disk
format       - format and analyze the disk
repair       - repair a defective sector
label        - write label to the disk
analyze      - surface analysis
defect       - defect list management
```

```
backup      - search for backup labels
verify     - read and display labels
save       - save new disk/partition definitions
inquiry    - show vendor, product and revision
volname    - set 8-character volume name
!<cmd>    - execute <cmd>, then return
quit

format> p

PARTITION MENU:
0      - change '0' partition
1      - change '1' partition
2      - change '2' partition
3      - change '3' partition
4      - change '4' partition
5      - change '5' partition
6      - change '6' partition
7      - change '7' partition
select  - select a predefined table
modify  - modify a predefined partition table
name    - name the current table
print   - display the current table
label   - write partition map and label to the disk
!<cmd> - execute <cmd>, then return
quit

partition> 1
Part      Tag      Flag      Cylinders      Size      Blocks
   1 unassigned  wm         0              0      (0/0/0)         0
Enter partition id tag[unassigned]:
Enter partition permission flags[wm]:
Enter new starting cyl[0]:
Enter partition size[0b, 0c, 0.00mb, 0.00gb]: 2.00gb
partition> 1
Ready to label disk, continue? y

partition> p
Current partition table (unnamed):
Total disk cylinders available: 13814 + 2 (reserved cylinders)
Part      Tag      Flag      Cylinders      Size      Blocks
   0 unassigned  wm         0              0      (0/0/0)         0
   1 unassigned  wm         0 - 3236      2.00GB  (3237/0/0)    4195152
partition> q
```

Copy the data on `vol01` to the newly created disk partition.

```
# dd if=/dev/vx/dsk/voldg/vol01 of=/dev/dsk/c1t12d0s1
```

In the `/etc/vfstab` file, remove the following entry.

```
/dev/vx/dsk/voldg/vol1 /dev/vx/rdisk/voldg/vol1 /vol1 vxfs 4 yes rw
```

Replace it with an entry for the newly created partition.

```
/dev/dsk/c1t12d0s1 /dev/rdsk/c1t12d0s1 /vol01 vxfs 4 yes rw
```

Mount the disk partition.

```
# mount -F vxfs /dev/dsk/c1t12d0s1 /vol01
```

Remove `vol01` from VxVM.

```
# vxedit -rf rm /dev/vx/dsk/voldg/vol01
```

To complete the procedure, follow the remaining steps.

Shutting down VERITAS Volume Manager (inset)

File text inset name: `zz_shutting_down_volume_manager.fm`

Preparing to remove Veritas File System

The `VRTSvxfs` package cannot be removed if there are any mounted VxFS file systems or Storage Checkpoints. Unmount the VxFS file systems and Storage Checkpoints before uninstalling Veritas Storage Foundation. After you remove the `VRTSvxfs` package, VxFS file systems are not mountable or accessible until another `VRTSvxfs` package is installed.

To unmount a file system

- 1 Check if any VxFS file systems are mounted.

```
# cat /etc/mnttab | grep vxfs
```

- 2 Unmount any file systems.

```
# umount special | mount_point
```

Specify the file system to be unmounted as a *mount_point* or *special* (the device on which the file system resides). See the `umount_vxfs(1M)` manual page for more information about this command and its available options.

You can use the `-a` option to unmount all file systems except `/`, `/usr`, `/usr/kvm`, `/var`, `/proc`, `/dev/fd`, and `/tmp`.

To unmount a Storage Checkpoint

- 1 Check if any Storage Checkpoints are mounted.

```
# cat /etc/mnttab | grep vxfs
```

- 2 Unmount any Storage Checkpoints.

```
# umount /checkpoint_name
```

Shutting down cluster operations

If the systems are running as an HA cluster, you have to take all service groups offline and shutdown VCS.

To take all service groups offline and shutdown VCS

- ◆ Use the `hastop` command as follows:

```
# /opt/VRTSvcs/bin/hastop -all
```

Warning: Do not use the `-force` option when executing `hastop`. This will leave all service groups online and shut down VCS, causing undesired results during uninstallation of the packages.

Disabling the agents on a system

This section explains how to disable a VCS agent for VVR on a system. To disable an agent, you must change the service group containing the resource type of the agent to an OFFLINE state. Then, you can stop the application or switch the application to another system.

To disable the agents

- 1 Check whether any service group containing the resource type of the agent is online by typing the following command:

```
# hagrps -state service_group -sys system_name
```

If none of the service groups is online, skip to 3.

- 2 If the service group is online, take it offline.

To take the service group offline without bringing it online on any other system in the cluster, enter:

```
# hagrps -offline service_group -sys system_name
```

- 3 Stop the agent on the system by entering:

```
# haagent -stop agent_name -sys system_name
```

When you get the message `Please look for messages in the log file,` check the file `/var/VRTSvcs/log/engine_A.log` for a message confirming that each agent has stopped.

You can also use the `ps` command to confirm that the agent is stopped.

- 4 Remove the system from the `SystemList` of the service group. If you disable the agent on all the systems in the `SystemList`, you can also remove the service groups and resource types from the VCS configuration.

Read information on administering VCS from the command line.

Refer to the *Veritas Cluster Server User's Guide*.

Removing the Replicated Data Set

If you use VVR, you need to perform the following steps. This section gives the steps to remove a Replicated Data Set (RDS) when the application is either active or stopped.

To remove the Replicated Data Set

- 1 Verify that all RLINKs are up-to-date:

```
# vxrlink -g diskgroup status rlink_name
```

If the Secondary is not required to be up-to-date, proceed to [2](#) and stop replication using the `-f` option with the `vradmin stoprep` command.

- 2 Stop replication to the Secondary by issuing the following command on any host in the RDS:

The `vradmin stoprep` command fails if the Primary and Secondary RLINKs are not up-to-date. Use the `-f` option to stop replication to a Secondary even when the RLINKs are not up-to-date.

```
# vradmin -g diskgroup stoprep local_rvgname sec_hostname
```

The argument `local_rvgname` is the name of the RVG on the local host and represents its RDS.

The argument `sec_hostname` is the name of the Secondary host as displayed in the output of the `vradmin printrvg` command.

- 3 Remove the Secondary from the RDS by issuing the following command on any host in the RDS:

```
# vradmin -g diskgroup delsec local_rvgname sec_hostname
```

The argument `local_rvgname` is the name of the RVG on the local host and represents its RDS.

The argument `sec_hostname` is the name of the Secondary host as displayed in the output of the `vradmin printrvg` command.

- 4 Remove the Primary from the RDS by issuing the following command on the Primary:

```
# vradmin -g diskgroup delpri local_rvgname
```

When used with the `-f` option, the `vradmin delpri` command removes the Primary even when the application is running on the Primary.

The RDS is removed.

- 5 If you want to delete the SRLs from the Primary and Secondary hosts in the RDS, issue the following command on the Primary and all Secondaries:

```
# vxedit -r -g diskgroup rm srl_name
```

Uninstalling SVS packages using the script-based installer

Use the following procedure to remove SVS products.

Not all packages may be installed on your system depending on the choices that you made when you installed the software.

Note: After you uninstall the product, you cannot access any file systems you created using the default disk layout version in SVS 6.0.1 with a previous version of SVS.

Language packages are uninstalled when you uninstall the English language packages.

To shut down and remove the installed SVS packages

- 1 Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/vfstab`. Failing to remove these entries could result in system boot problems later.
- 2 Unmount all mount points for VxFS file systems.
- 3 If the VxVM package (`VRTSVxvm`) is installed, read and follow the uninstallation procedures for VxVM.
See [“Preparing to remove Veritas Volume Manager”](#) on page 366.
- 4 Make sure you have performed all of the prerequisite steps.
- 5 Move to the `/opt/VRTS/install` directory and run the uninstall script.

```
# cd /opt/VRTS/install
# ./uninstallsvs<version>
```

Where `<version>` is the specific release version.

Or, if you are using ssh or rsh, use one of the following:

```
■ # ./uninstallsvs<version> -rsh
■ # ./uninstallsvs<version> -ssh
```

See [“About the Veritas installer”](#) on page 41.

- 6 The uninstall script prompts for the system name. Enter one or more system names, separated by a space, from which to uninstall SVS, for example, `sys1`:

```
Enter the system names separated by spaces: [q?] sys1 sys2
```

- 7 The uninstall script prompts you to stop the product processes. If you respond yes, the processes are stopped and the packages are uninstalled.

The uninstall script creates log files and displays the location of the log files.

- 8 Most packages have kernel components. In order to ensure complete removal, a system reboot is recommended after all packages have been removed.
- 9 To verify the removal of the packages, use the `pkginfo` command.

```
# pkginfo | grep VRTS
```

Uninstalling SVS with the Veritas Web-based installer

This section describes how to uninstall using the Veritas Web-based installer.

Note: After you uninstall the product, you cannot access any file systems you created using the default disk layout Version in SVS 6.0.1 with a previous version of SVS.

To uninstall SVS

- 1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.
- 2 Start the Web-based installer.
See [“Starting the Veritas Web-based installer”](#) on page 172.
- 3 On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.
- 4 Select **Symantec VirtualStore** from the Product drop-down list, and click **Next**.
- 5 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Next**.
- 6 After the validation completes successfully, click **Next** to uninstall SVS on the selected system.
- 7 If there are any processes running on the target system, the installer stops the processes. Click **Next**.

- 8 After the installer stops the processes, the installer removes the products from the specified system.

Click **Next**.

- 9 After the uninstall completes, the installer displays the location of the summary, response, and log files. If required, view the files to confirm the status of the removal.

- 10 Click **Finish**.

Most RPMs have kernel components. In order to ensure their complete removal, a system reboot is recommended after all the RPMs have been removed.

Removing the CP server configuration using the installer program

This section describes how to remove the CP server configuration from a node or a cluster that hosts the CP server.

Warning: Ensure that no SVS cluster (application cluster) uses the CP server that you want to unconfigure.

To remove the CP server configuration

- 1 To run the configuration removal script, enter the following command on the node where you want to remove the CP server configuration:

```
root@cps1.symantecexample.com
# /opt/VRTS/install/installvcsversion -configcps
```

- 2 Select option 3 from the menu to unconfigure the CP server.

```
VERITAS COORDINATION POINT SERVER CONFIGURATION UTILITY
=====
```

Select one of the following:

- ```
[1] Configure Coordination Point Server on single node VCS system
[2] Configure Coordination Point Server on SFHA cluster
[3] Unconfigure Coordination Point Server
```

**3 Review the warning message and confirm that you want to unconfigure the CP server.**

```
WARNING: Unconfiguring Coordination Point Server stops the
vxcpserv process. VCS clusters using this server for
coordination purpose will have one less coordination point.
```

```
Are you sure you want to bring down the cp server? (y/n)
(Default:n) :y
```

**4 Review the screen output as the script performs the following steps to remove the CP server configuration:**

- Stops the CP server
- Removes the CP server from VCS configuration
- Removes resource dependencies
- Takes the the CP server service group (CPSSG) offline, if it is online
- Removes the CPSSG service group from the VCS configuration
- Successfully unconfigured the Veritas Coordination Point Server

```
The CP server database is not being deleted on the shared storage.
It can be re-used if CP server is reconfigured on the cluster.
The same database location can be specified during CP server configurat.
```

**5 Decide if you want to delete the CP server configuration file.**

```
Do you want to delete the CP Server configuration file (/etc/vxcps.conf)
and log files (in /var/VRTScps)? [y,n,q] (n) y
```

```
Deleting /etc/vxcps.conf and log files on sys1.... Done
Deleting /etc/vxcps.conf and log files on sys2... Done
```

**6 Confirm if you want to send information about this installation to Symantec to help improve installation in the future.**

```
Would you like to send the information about this installation
to Symantec to help improve installation in the future? [y,n,q,?] (y)
```

Upload completed successfully.



# Installation reference

- [Appendix A. Tunable files for installation](#)
- [Appendix B. Installation scripts](#)
- [Appendix C. Configuration files](#)
- [Appendix D. Response files](#)
- [Appendix E. Configuring the secure shell or the remote shell for communications](#)
- [Appendix F. SVS components](#)
- [Appendix G. Sample SVS cluster setup diagrams for CP server-based I/O fencing](#)
- [Appendix H. Configuring LLT over UDP using IPv6](#)
- [Appendix I. Configuring LLT over UDP using IPv4](#)
- [Appendix J. Compatibility issues when installing Symantec VirtualStore with other products](#)





# Tunable files for installation

This appendix includes the following topics:

- [About setting tunable parameters using the installer or a response file](#)
- [Setting tunables for an installation, configuration, or upgrade](#)
- [Setting tunables with no other installer-related operations](#)
- [Setting tunables with an un-integrated response file](#)
- [Preparing the tunables file](#)
- [Setting parameters for the tunables file](#)
- [Tunables value parameter definitions](#)

## About setting tunable parameters using the installer or a response file

You can set non-default product and system tunable parameters using a tunables file. With the file, you can set tunables such as the I/O policy or toggle native multi-pathing. The tunables file passes arguments to the installer script to set tunables. With the file, you can set the tunables for the following operations:

- When you install, configure, or upgrade systems.

```
./installer -tunablesfile tunables_file_name
```

See “[Setting tunables for an installation, configuration, or upgrade](#)” on page 386.

- When you apply the tunables file with no other installer-related operations.

```
./installer -tunablesfile tunables_file_name -setttunables [
system1 system2 ...]
```

See [“Setting tunables with no other installer-related operations”](#) on page 387.

- When you apply the tunables file with an un-integrated response file.

```
./installer -responsefile response_file_name -tunablesfile
tunables_file_name
```

See [“Setting tunables with an un-integrated response file”](#) on page 388.

You must select the tunables that you want to use from this guide.

See [“Tunables value parameter definitions”](#) on page 390.

## Setting tunables for an installation, configuration, or upgrade

You can use a tunables file for installation procedures to set non-default tunables. You invoke the installation script with the `tunablesfile` option. The tunables file passes arguments to the script to set the selected tunables. You must select the tunables that you want to use from this guide.

See [“Tunables value parameter definitions”](#) on page 390.

---

**Note:** Certain tunables only take effect after a system reboot.

---

### To set the non-default tunables for an installation, configuration, or upgrade

- 1 Prepare the tunables file.  
See [“Preparing the tunables file”](#) on page 389.
- 2 Make sure the systems where you want to install SVS meet the installation requirements.
- 3 Complete any preinstallation tasks.
- 4 Copy the tunables file to one of the systems where you want to install, configure, or upgrade the product.
- 5 Mount the product disc and navigate to the directory that contains the installation program.
- 6 Start the installer for the installation, configuration, or upgrade. For example:

```
./installer -tunablesfile /tmp/tunables_file
```

Where `/tmp/tunables_file` is the full path name for the tunables file.

- 7 Proceed with the operation. When prompted, accept the tunable parameters. Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.
- 8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

## Setting tunables with no other installer-related operations

You can use the installer to set tunable parameters without any other installer-related operations. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See [“Tunables value parameter definitions”](#) on page 390.

---

**Note:** Certain tunables only take effect after a system reboot.

---

### To set tunables with no other installer-related operations

- 1 Prepare the tunables file.  
See [“Preparing the tunables file”](#) on page 389.
- 2 Make sure the systems where you want to install SVS meet the installation requirements.
- 3 Complete any preinstallation tasks.
- 4 Copy the tunables file to one of the systems that you want to tune.
- 5 Mount the product disc and navigate to the directory that contains the installation program.
- 6 Start the installer with the `-setttunables` option.

```
./installer -tunablesfile tunables_file_name -setttunables [
sys123 sys234 ...]
```

Where `/tmp/tunables_file` is the full path name for the tunables file.

- 7 Proceed with the operation. When prompted, accept the tunable parameters. Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.
- 8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

## Setting tunables with an un-integrated response file

You can use the installer to set tunable parameters with an un-integrated response file. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See [“Tunables value parameter definitions”](#) on page 390.

---

**Note:** Certain tunables only take effect after a system reboot.

---

### To set tunables with an un-integrated response file

- 1 Make sure the systems where you want to install SVS meet the installation requirements.
- 2 Complete any preinstallation tasks.
- 3 Prepare the tunables file.  
See [“Preparing the tunables file”](#) on page 389.
- 4 Copy the tunables file to one of the systems that you want to tune.
- 5 Mount the product disc and navigate to the directory that contains the installation program.
- 6 Start the installer with the `-responsefile` and `-tunablesfile` options.

```
./installer -responsefile response_file_name -tunablesfile
tunables_file_name
```

Where *response\_file\_name* is the full path name for the response file and *tunables\_file\_name* is the full path name for the tunables file.

- 7 Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.
- 8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

## Preparing the tunables file

A tunables file is a Perl module and consists of an opening and closing statement, with the tunables defined between. Use the hash symbol at the beginning of the line to comment out the line. The tunables file opens with the line "our %TUN;" and ends with the return true "1;" line. The final return true line only needs to appear once at the end of the file. Define each tunable parameter on its own line.

You can use the installer to create a tunables file template, or manually format tunables files you create.

### To create a tunables file template

- ◆ Start the installer with the `-tunables` option. Enter the following:

```
./installer -tunables
```

You see a list of all supported tunables, and the location of the tunables file template.

### To manually format tunables files

- ◆ Format the tunable parameter as follows:

```
$TUN{"tunable_name"}{"system_name"|"*" }=value_of_tunable;
```

For the *system\_name*, use the name of the system, its IP address, or a wildcard symbol. The *value\_of\_tunable* depends on the type of tunable you are setting. End the line with a semicolon.

The following is an example of a tunables file.

```

Tunable Parameter Values:

our %TUN;

$TUN{"tunable1"}{"*" }=1024;
$TUN{"tunable3"}{"sys123" }="SHA256";

1;
```

## Setting parameters for the tunables file

Each tunables file defines different tunable parameters. The values that you can use are listed in the description of each parameter. Select the tunables that you want to add to the tunables file and then configure each parameter.

See [“Tunables value parameter definitions”](#) on page 390.

Each line for the parameter value starts with \$TUN. The name of the tunable is in curly brackets and double-quotes. The system name is enclosed in curly brackets and double-quotes. Finally define the value and end the line with a semicolon, for example:

```
$TUN{"dmp_daemon_count"}{"node123"}=16;
```

In this example, you are changing the dmp\_daemon\_count value from its default of 10 to 16. You can use the wildcard symbol "\*" for all systems. For example:

```
$TUN{"dmp_daemon_count"}{"*"}=16;
```

## Tunables value parameter definitions

When you create a tunables file for the installer you can only use the parameters in the following list.

Prior to making any updates to the tunables, refer to the *Veritas Storage Foundation and High Availability Solutions Tuning Guide* for detailed information on product tunable ranges and recommendations .

[Table A-1](#) describes the supported tunable parameters that can be specified in a tunables file.

**Table A-1** Supported tunable parameters

| Tunable             | Description                                                                                                                                                                                        |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dmp_cache_open      | (Veritas Dynamic Multi-Pathing) Whether the first open on a device performed by an array support library (ASL) is cached. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_daemon_count    | (Veritas Dynamic Multi-Pathing) The number of kernel threads for DMP administrative tasks. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                |
| dmp_delayq_interval | (Veritas Dynamic Multi-Pathing) The time interval for which DMP delays the error processing if the device is busy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.        |

**Table A-1** Supported tunable parameters (*continued*)

| Tunable                 | Description                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dmp_fast_recovery       | (Veritas Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Veritas Dynamic Multi-Pathing is started.             |
| dmp_health_time         | (Veritas Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                  |
| dmp_log_level           | (Veritas Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                         |
| dmp_low_impact_probe    | (Veritas Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                  |
| dmp_lun_retry_timeout   | (Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                          |
| dmp_monitor_fabric      | (Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_monitor_osevent     | (Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                |
| dmp_monitor_ownership   | (Veritas Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                |
| dmp_native_multipathing | (Veritas Dynamic Multi-Pathing) Whether DMP will intercept the I/Os directly on the raw OS paths or not. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                 |

**Table A-1** Supported tunable parameters (*continued*)

| Tunable                   | Description                                                                                                                                                                                                                         |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dmp_native_support        | (Veritas Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                                         |
| dmp_path_age              | (Veritas Dynamic Multi-Pathing) The time for which an intermittently failing path needs to be monitored before DMP marks it as healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                    |
| dmp_pathswitch_blks_shift | (Veritas Dynamic Multi-Pathing) The default number of contiguous I/O blocks sent along a DMP path to an array before switching to the next available path. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_probe_idle_lun        | (Veritas Dynamic Multi-Pathing) Whether the path restoration kernel thread probes idle LUNs. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                               |
| dmp_probe_threshold       | (Veritas Dynamic Multi-Pathing) The number of paths will be probed by the restore daemon. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                                  |
| dmp_restore_cycles        | (Veritas Dynamic Multi-Pathing) The number of cycles between running the check_all policy when the restore policy is check_periodic. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                       |
| dmp_restore_interval      | (Veritas Dynamic Multi-Pathing) The time interval in seconds the restore daemon analyzes the condition of paths. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                           |
| dmp_restore_policy        | (Veritas Dynamic Multi-Pathing) The policy used by DMP path restoration thread. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                                            |
| dmp_restore_state         | (Veritas Dynamic Multi-Pathing) Whether kernel thread for DMP path restoration is started. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                                 |



**Table A-1** Supported tunable parameters (*continued*)

| Tunable           | Description                                                                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dmp_retry_count   | (Veritas Dynamic Multi-Pathing) The number of times a path reports a path busy error consecutively before DMP marks the path as failed. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_scsi_timeout  | (Veritas Dynamic Multi-Pathing) The timeout value for any SCSI command sent via DMP. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                    |
| dmp_sfg_threshold | (Veritas Dynamic Multi-Pathing) The status of the subpaths failover group (SFG) feature. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                |
| dmp_stat_interval | (Veritas Dynamic Multi-Pathing) The time interval between gathering DMP statistics. This tunable must be set after Veritas Dynamic Multi-Pathing is started.                                                     |



# Installation scripts

This appendix includes the following topics:

- [Installation script options](#)
- [Restarting the installer after a failed connection](#)
- [Starting and stopping processes for the Veritas products](#)
- [Installation program has improved failure handling](#)

## Installation script options

[Table B-1](#) shows command line options for the installation script. For an initial install or upgrade, options are not usually required. The installation script options apply to all Veritas Storage Foundation product scripts, except where otherwise noted.

See [“About the Veritas installer”](#) on page 41.

**Table B-1** Available command line options

| Commandline Option | Function                                                                                                                                                                                                                  |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -addnode           | Adds a node to a high availability cluster.                                                                                                                                                                               |
| -allpkgs           | Displays all packages required for the specified product. The packages are listed in correct installation order. The output can be used to create scripts for command line installs, or for installations over a network. |

**Table B-1** Available command line options (*continued*)

| Commandline Option                 | Function                                                                                                                                                                                                                                                     |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -comcleanup                        | The <code>-comcleanup</code> option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated. |
| -configcps                         | The <code>-configcps</code> option is used to configure CP server on a running system or cluster.                                                                                                                                                            |
| -configure                         | Configures the product after installation.                                                                                                                                                                                                                   |
| -fencing                           | Configures I/O fencing in a running cluster.                                                                                                                                                                                                                 |
| -fips                              | The <code>-fips</code> option is used to enable or disable security with fips mode on a running VCS cluster. It could only be used together with <code>-security</code> or <code>-securityonnode</code> option.                                              |
| -hostfile <i>full_path_to_file</i> | Specifies the location of a file that contains a list of hostnames on which to install.                                                                                                                                                                      |
| -installallpkgs                    | The <code>-installallpkgs</code> option is used to select all packages.                                                                                                                                                                                      |
| -installrecpkgs                    | The <code>-installrecpkgs</code> option is used to select the recommended packages set.                                                                                                                                                                      |
| -installminpkgs                    | The <code>-installminpkgs</code> option is used to select the minimum packages set.                                                                                                                                                                          |
| -ignorepatchreqs                   | The <code>-ignorepatchreqs</code> option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.                                                                                                   |
| -jumpstart <i>dir_path</i>         | Produces a sample finish file for Solaris JumpStart installation. The <i>dir_path</i> indicates the path to the directory in which to create the finish file.                                                                                                |
| -keyfile <i>ssh_key_file</i>       | Specifies a key file for secure shell (SSH) installs. This option passes <code>-i ssh_key_file</code> to every SSH invocation.                                                                                                                               |
| -license                           | Registers or updates product licenses on the specified systems.                                                                                                                                                                                              |

**Table B-1** Available command line options (*continued*)

| Commandline Option           | Function                                                                                                                                                                                                                                                                                |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -logpath <i>log_path</i>     | Specifies a directory other than /opt/VRTS/install/logs as the location where installer log files, summary files, and response files are saved.                                                                                                                                         |
| -makeresponsefile            | Use the -makeresponsefile option only to generate response files. No actual software installation occurs when you use this option.                                                                                                                                                      |
| -minpkgs                     | Displays the minimal packages required for the specified product. The packages are listed in correct installation order. Optional packages are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See allpkgs option. |
| -nolic                       | Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.                                                                                                                         |
| -pkginfo                     | Displays a list of packages and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the -pkginfo option with the installvcs script to display VCS packages.                                 |
| -pkgpath <i>package_path</i> | Designates the path of a directory that contains all packages to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.                                                                                              |
| -pkgset                      | Discovers and displays the package group (minimum, recommended, all) and packages that are installed on the specified systems.                                                                                                                                                          |
| -pkgtable                    | Displays product's packages in correct installation order by group.                                                                                                                                                                                                                     |
| -postcheck                   | Checks for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups.                                                                                                                                 |

**Table B-1** Available command line options (*continued*)

| Commandline Option                 | Function                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -precheck                          | Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.                                                                                                                                                                             |
| -recpkgs                           | Displays the recommended packages required for the specified product. The packages are listed in correct installation order. Optional packages are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See <code>allpkgs</code> option.                                   |
| -redirect                          | Displays progress details without showing the progress bar.                                                                                                                                                                                                                                                                                |
| -requirements                      | The <code>-requirements</code> option displays required OS version, required packages and patches, file system space, and other system requirements in order to install the product.                                                                                                                                                       |
| -responsefile <i>response_file</i> | Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The <i>response_file</i> must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. |
| -rolling_upgrade                   | Starts a rolling upgrade. Using this option, the installer detects the rolling upgrade status on cluster systems automatically without the need to specify rolling upgrade phase 1 or phase 2 explicitly.                                                                                                                                  |
| -rollingupgrade_phase1             | The <code>-rollingupgrade_phase1</code> option is used to perform rolling upgrade Phase-I. In the phase, the product kernel packages get upgraded to the latest version.                                                                                                                                                                   |
| -rollingupgrade_phase2             | The <code>-rollingupgrade_phase2</code> option is used to perform rolling upgrade Phase-II. In the phase, VCS and other agent packages upgrade to the latest version. Product kernel drivers are rolling-upgraded to the latest protocol version.                                                                                          |

**Table B-1** Available command line options (*continued*)

| Commandline Option         | Function                                                                                                                                                                                                                                                                  |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -rootpath <i>root_path</i> | Specifies an alternative root directory on which to install packages.<br><br>On Solaris operating systems, -rootpath passes -R <i>path</i> to pkgadd command.                                                                                                             |
| -rsh                       | Specify this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.<br><br>See <a href="#">“About configuring secure shell or remote shell communication modes before installing products”</a> on page 415.        |
| -security                  | The -security option is used to convert a running VCS cluster between secure and non-secure modes of operation.                                                                                                                                                           |
| -securityonnode            | The -securityonnode option is used to configure a secure cluster node by node.                                                                                                                                                                                            |
| -securitytrust             | The -securitytrust option is used to setup trust with another broker.                                                                                                                                                                                                     |
| -serial                    | Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems.                                         |
| -settunables               | Specify this option when you want to set tunable parameters after you install and configure a product. You may need to restart processes of the product for the tunable parameter values to take effect. You must use this option together with the -tunablesfile option. |
| -start                     | Starts the daemons and processes for the specified product.                                                                                                                                                                                                               |
| -stop                      | Stops the daemons and processes for the specified product.                                                                                                                                                                                                                |

**Table B-1** Available command line options (*continued*)

| Commandline Option                  | Function                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -timeout                            | The <code>-timeout</code> option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the <code>-timeout</code> option overrides the default value of 1200 seconds. Setting the <code>-timeout</code> option to 0 prevents the script from timing out. The <code>-timeout</code> option does not work with the <code>-serial</code> option. |
| -tmppath <i>tmp_path</i>            | Specifies a directory other than <code>/var/tmp</code> as the working directory for the installation scripts. This destination is where initial logging is performed and where packages are copied on remote systems before installation.                                                                                                                                                                           |
| -tunables                           | Lists all supported tunables and create a tunables file template.                                                                                                                                                                                                                                                                                                                                                   |
| -tunables_file <i>tunables_file</i> | Specify this option when you specify a tunables file. The tunables file should include tunable parameters.                                                                                                                                                                                                                                                                                                          |
| -upgrade                            | Specifies that an existing version of the product exists and you plan to upgrade it.                                                                                                                                                                                                                                                                                                                                |
| -upgrade_kernelpkgs                 | The <code>-upgrade_kernelpkgs</code> option has been renamed to <code>-rollingupgrade_phase1</code> .                                                                                                                                                                                                                                                                                                               |
| -upgrade_nonkernelpkgs              | The <code>-upgrade_nonkernelpkgs</code> option has been renamed to <code>-rollingupgrade_phase2</code> .                                                                                                                                                                                                                                                                                                            |
| -version                            | Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.         |



## Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

## Starting and stopping processes for the Veritas products

After the installation and configuration is complete, the Veritas product installer starts the processes that are used by the installed products. You can use the product installer to stop or start the processes, if required.

### To stop the processes

- ◆ Use the `-stop` option to stop the product installation script.

For example, to stop the product's processes, enter the following command:

```
./installer -stop
```

or

```
/opt/VRTS/install/installsvs<version> -stop
```

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

### To start the processes

- ◆ Use the `-start` option to start the product installation script.

For example, to start the product's processes, enter the following command:

```
./installer -start
```

or

```
/opt/VRTS/install/installsvs<version> -start
```

Where `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

## Installation program has improved failure handling

The product installer has improved ability to recover from failed installations, as follows:

- A recovery file is created if an installation fails due to a failed network connection. This file enables the install program to resume from the point where the installation failed.
- New options are available to start or stop the Veritas processes without requiring a full installation or configuration.

# Configuration files

This appendix includes the following topics:

- [About I/O fencing configuration files](#)

## About I/O fencing configuration files

[Table C-1](#) lists the I/O fencing configuration files.

**Table C-1** I/O fencing configuration files

| File               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /etc/default/vxfen | <p>This file stores the start and stop environment variables for I/O fencing:</p> <ul style="list-style-type: none"><li>■ VXFEN_START—Defines the startup behavior for the I/O fencing module after a system reboot. Valid values include:<ul style="list-style-type: none"><li>1—Indicates that I/O fencing is enabled to start up.</li><li>0—Indicates that I/O fencing is disabled to start up.</li></ul></li><li>■ VXFEN_STOP—Defines the shutdown behavior for the I/O fencing module during a system shutdown. Valid values include:<ul style="list-style-type: none"><li>1—Indicates that I/O fencing is enabled to shut down.</li><li>0—Indicates that I/O fencing is disabled to shut down.</li></ul></li></ul> <p>The installer sets the value of these variables to 1 at the end of Symantec VirtualStore configuration.</p> |
| /etc/vxfendg       | <p>This file includes the coordinator disk group information.</p> <p>This file is not applicable for server-based fencing.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table C-1** I/O fencing configuration files (*continued*)

| File           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /etc/vxfenmode | <p>This file contains the following parameters:</p> <ul style="list-style-type: none"> <li>■ <b>vxfen_mode</b> <ul style="list-style-type: none"> <li>■ <b>scsi3</b>—For disk-based fencing</li> <li>■ <b>customized</b>—For server-based fencing</li> <li>■ <b>disabled</b>—To run the I/O fencing driver but not do any fencing operations.</li> </ul> </li> <li>■ <b>vxfen_mechanism</b><br/>This parameter is applicable only for server-based fencing. Set the value as cps.</li> <li>■ <b>scsi3_disk_policy</b> <ul style="list-style-type: none"> <li>■ <b>dmp</b>—Configure the vxfen module to use DMP devices<br/>The disk policy is dmp by default. If you use iSCSI devices, you must set the disk policy as dmp.</li> <li>■ <b>raw</b>—Configure the vxfen module to use the underlying raw character devices</li> </ul> </li> </ul> <p><b>Note:</b> You must use the same SCSI-3 disk policy on all the nodes.</p> <ul style="list-style-type: none"> <li>■ <b>security</b><br/>This parameter is applicable only for server-based fencing.<br/>1—Indicates that communication with the CP server is in secure mode. This setting is the default.<br/>0—Indicates that communication with the CP server is in non-secure mode.</li> <li>■ <b>List of coordination points</b><br/>This list is required only for server-based fencing configuration.<br/>Coordination points in server-based fencing can include coordinator disks, CP servers, or both. If you use coordinator disks, you must create a coordinator disk group containing the individual coordinator disks.<br/>Refer to the sample file /etc/vxfen.d/vxfenmode_cps for more information on how to specify the coordination points and multiple IP addresses for each CP server.</li> <li>■ <b>single_cp</b><br/>This parameter is applicable for server-based fencing which uses a single highly available CP server as its coordination point. Also applicable for when you use a coordinator disk group with single disk.</li> <li>■ <b>autoseed_gab_timeout</b><br/>This parameter enables GAB automatic seeding of the cluster even when some cluster nodes are unavailable. This feature requires that I/O fencing is enabled.<br/>0—Turns the GAB auto-seed feature on. Any value greater than 0 indicates the number of seconds that GAB must delay before it automatically seeds the cluster.<br/>-1—Turns the GAB auto-seed feature off. This setting is the default.</li> </ul> |

**Table C-1** I/O fencing configuration files (*continued*)

| File          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /etc/vxfentab | <p>When I/O fencing starts, the vxfen startup script creates this /etc/vxfentab file on each node. The startup script uses the contents of the /etc/vxfendg and /etc/vxfenmode files. Any time a system is rebooted, the fencing driver reinitializes the vxfentab file with the current list of all the coordinator points.</p> <p><b>Note:</b> The /etc/vxfentab file is a generated file; do not modify this file.</p> <p>For disk-based I/O fencing, the /etc/vxfentab file on each node contains a list of all paths to each coordinator disk along with its unique disk identifier. A space separates the path and the unique disk identifier. An example of the /etc/vxfentab file in a disk-based fencing configuration on one node resembles as follows:</p> <ul style="list-style-type: none"> <li>■ Raw disk:           <pre style="margin-left: 2em;">/dev/rdisk/c1t1d0s2 HITACHI%5F1724-100%20%20FASTT%5FDISKS%5F6 00A0B8000215A5D000006804E795D075 /dev/rdisk/c2t1d0s2 HITACHI%5F1724-100%20%20FASTT%5FDISKS%5F6 00A0B8000215A5D000006814E795D076 /dev/rdisk/c3t1d2s2 HITACHI%5F1724-100%20%20FASTT%5FDISKS%5F6 00A0B8000215A5D000006824E795D077</pre> </li> <li>■ DMP disk:           <pre style="margin-left: 2em;">/dev/vx/rdmp/c1t1d0s2 HITACHI%5F1724-100%20%20FASTT%5FDISKS%5F6 00A0B8000215A5D000006804E795D075 /dev/vx/rdmp/c2t1d0s2 HITACHI%5F1724-100%20%20FASTT%5FDISKS%5F6 00A0B8000215A5D000006814E795D076 /dev/vx/rdmp/c3t1d0s2 HITACHI%5F1724-100%20%20FASTT%5FDISKS%5F6 00A0B8000215A5D000006824E795D077</pre> </li> </ul> <p>For server-based fencing, the /etc/vxfentab file also includes the security settings information.</p> <p>For server-based fencing with single CP server, the /etc/vxfentab file also includes the single_cp settings information.</p> |



# Response files

This appendix includes the following topics:

- [About response files](#)
- [Upgrading SVS using response files](#)
- [Uninstalling SVS using response files](#)
- [Syntax in the response file](#)
- [Response file variables to install, upgrade, or uninstall Symantec VirtualStore](#)
- [Sample response file for Symantec VirtualStore installation](#)
- [Sample response file for Symantec VirtualStore configuration](#)

## About response files

The installer or product installation script generates a response file during any installation, configuration, upgrade (except rolling upgrade), or uninstall procedure. The response file contains the configuration information that you entered during the procedure. When the procedure completes, the installation script displays the location of the response files.

You can use the response file for future installation procedures by invoking an installation script with the `-responsefile` option. The response file passes arguments to the script to automate the installation of that product. You can edit the file to automate installation and configuration of additional systems.

You can generate a response file using the `-makeresponsefile` option.

See [“Installation script options”](#) on page 395.

## Upgrading SVS using response files

Typically, you can use the response file that the installer generates after you perform SVS upgrade on one system to upgrade SVS on other systems. You can also create a response file using the `makeresponsefile` option of the installer.

### To perform automated SVS upgrade

- 1 Make sure the systems where you want to upgrade SVS meet the upgrade requirements.
- 2 Make sure the pre-upgrade tasks are completed.
- 3 Copy the response file to one of the systems where you want to upgrade SVS.
- 4 Edit the values of the response file variables as necessary.
- 5 Mount the product disc and navigate to the folder that contains the installation program.
- 6 Start the upgrade from the system to which you copied the response file. For example:

```
./installer -responsefile /tmp/response_file
./installsvs<version> -responsefile /tmp/response_file
```

Where `/tmp/response_file` is the response file's full path name and `<version>` is the specific release version.

See [“About the Veritas installer”](#) on page 41.

## Uninstalling SVS using response files

Typically, you can use the response file that the installer generates after you perform SVS uninstallation on one cluster to uninstall SVS on other clusters.

### To perform an automated uninstallation

- 1 Make sure that you meet the prerequisites to uninstall SVS.
- 2 Copy the response file to the system where you want to uninstall SVS.
- 3 Edit the values of the response file variables as necessary.



- 4 Start the uninstallation from the system to which you copied the response file. For example:

```
/opt/VRTS/install/uninstallsvs<version>
 -responsefile /tmp/response_file
```

Where *<version>* is the specific release version, and */tmp/response\_file* is the response file's full path name.

See [“About the Veritas installer”](#) on page 41.

## Syntax in the response file

The syntax of the Perl statements that are included in the response file variables varies. It can depend on whether the variables require scalar or list values.

For example, in the case of a string value:

```
$CFG{Scalar_variable}="value";
```

or, in the case of an integer value:

```
$CFG{Scalar_variable}=123;
```

or, in the case of a list:

```
$CFG{List_variable}=["value", "value", "value"];
```

## Response file variables to install, upgrade, or uninstall Symantec VirtualStore

[Table D-1](#) lists the response file variables that you can define to configure SVS.

**Table D-1**

| Variable          | Description                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CFG{opt}{install} | Installs SVS packages. Configuration can be performed at a later time using the <code>-configure</code> option.<br><br>List or scalar: scalar<br><br>Optional or required: optional |

**Table D-1** (continued)

| Variable              | Description                                                                                                                                                                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CFG{accepteula}       | Specifies whether you agree with the EULA.pdf file on the media.<br><br>List or scalar: scalar<br><br>Optional or required: required                                                                                                          |
| \$CFG{opt}{vxkeyless} | Installs the product with keyless license.<br><br>List or scalar: scalar<br><br>Optional or required: optional                                                                                                                                |
| CFG{systems}          | List of systems on which the product is to be installed or uninstalled.<br><br>List or scalar: list<br><br>Optional or required: required                                                                                                     |
| CFG{prod}             | Defines the product to be installed or uninstalled.<br><br>List or scalar: scalar<br><br>Optional or required: required                                                                                                                       |
| CFG{opt}{keyfile}     | Defines the location of an ssh keyfile that is used to communicate with all remote systems.<br><br>List or scalar: scalar<br><br>Optional or required: optional                                                                               |
| CFG{opt}{pkgpath}     | Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems.<br><br>List or scalar: scalar<br><br>Optional or required: optional          |
| CFG{opt}{tmppath}     | Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp.<br><br>List or scalar: scalar<br><br>Optional or required: optional |

Table D-1 (continued)

| Variable                  | Description                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CFG{opt}{rsh}             | Defines that <i>rsh</i> must be used instead of <i>ssh</i> as the communication method between systems.<br><br>List or scalar: scalar<br>Optional or required: optional     |
| CFG{opt}{logpath}         | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.<br><br>List or scalar: scalar<br>Optional or required: optional |
| \$CFG{opt}{prodmode}      | List of modes for product<br><br>List or scalar: list<br>Optional or required: optional                                                                                     |
| CFG{opt}{uninstall}       | Uninstalls SVS packages.<br><br>List or scalar: scalar<br>Optional or required: optional                                                                                    |
| CFG{mirrordgname}{system} | Splits the target disk group name for a system.<br><br>List or scalar: scalar<br>Optional or required: optional                                                             |
| CFG{splitmirror}{system}  | Indicates the system where you want a split mirror backup disk group created.<br><br>List or scalar: scalar<br>Optional or required: optional                               |

## Sample response file for Symantec VirtualStore installation

The following example shows a response file for installing Symantec VirtualStore.

```
#####
#Auto generated svcs responsefile #
#####
```

**Sample response file for Symantec VirtualStore configuration**

```
our %CFG;
$CFG{accepteula}=1;
$CFG{opt}{rsh}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vr}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{prod}="SVS60";
$CFG{systems}=[qw(sys1 sys2)];
```

```
1;
```

## Sample response file for Symantec VirtualStore configuration

The following example shows a response file for configuring Symantec VirtualStore.

```
#####
#Auto generated svcs responsefile #
#####
```

```
our %CFG;
$CFG{accepteula}=1;
$CFG{fencingenabled}="0";
$CFG{lltoverudp}="0";
$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vr}=1;
$CFG{opt}{installrecpkgs}=1;
$CFG{opt}{vxkeyless}=1;
$CFG{prod}="SVS60";
$CFG{reconfigurevcs}=1;
$CFG{systems}=[qw(sys1 sys2)];
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=127;
$CFG{vcs_clustername}="uxrt_sol";
$CFG{vcs_lltlink1}{"sys1"}="bge1";
$CFG{vcs_lltlink1}{"sys2"}="bge1";
$CFG{vcs_lltlink2}{"sys1"}="bge2";
```

```
$CFG{vcs_lltlink2}{"sys2"}="bge2";
$CFG{vcs_userenpw}=[qw(JlmElgLimHmKumGlj)];
$CFG{vcs_username}=[qw(admin)];
$CFG{vcs_userpriv}=[qw(Administrators)];
$CFG{opt}{logpath}="/tmp/log";
```

```
1;
```

**Sample response file for Symantec VirtualStore configuration**

# Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

- [About configuring secure shell or remote shell communication modes before installing products](#)
- [Manually configuring and passwordless ssh](#)
- [Restarting the ssh session](#)
- [Enabling and disabling rsh for Solaris](#)

## About configuring secure shell or remote shell communication modes before installing products

You can install products to remote systems using either secure shell (ssh) or remote shell (rsh). Symantec recommends that you use ssh as it is more secure than rsh.

This section contains an example of how to set up ssh password free communication. The example sets up ssh between a source system (system1) that contains the installation directories, and a target system (system2). This procedure also applies to multiple target systems.

---

**Note:** The script- and Web-based installers support establishing passwordless communication for you.

---

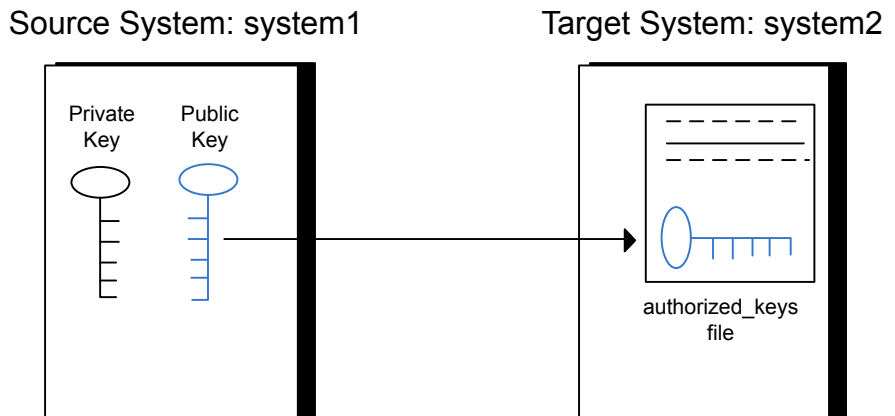
## Manually configuring and passwordless ssh

The ssh program enables you to log into and execute commands on a remote system. ssh enables encrypted communications and an authentication process between two untrusted hosts over an insecure network.

In this procedure, you first create a DSA key pair. From the key pair, you append the public key from the source system to the `authorized_keys` file on the target systems.

Figure E-1 illustrates this procedure.

**Figure E-1** Creating the DSA key pair and appending it to target systems



Read the ssh documentation and online manual pages before enabling ssh. Contact your operating system support provider for issues regarding ssh configuration.

Visit the OpenSSH website that is located at: <http://openssh.org> to access online manuals and other resources.



### To create the DSA key pair

- 1 On the source system (system1), log in as root, and navigate to the root directory.

```
system1 # cd /
```

- 2 Make sure the `/.ssh` directory is on all the target installation systems (system2 in this example). If that directory is not present, create it on all the target systems and set the write permission to root only:

Solaris 10:

```
system2 # mkdir /.ssh
```

Solaris 11:

```
system2 # mkdir /root/.ssh
```

Change the permissions of this directory, to secure it.

Solaris 10:

```
system2 # chmod go-w /.ssh
```

Solaris 11:

```
system2 # chmod go-w /root/.ssh
```

- 3 To generate a DSA key pair on the source system, type the following command:

```
system1 # ssh-keygen -t dsa
```

System output similar to the following is displayed:

```
Generating public/private dsa key pair.
Enter file in which to save the key (//.ssh/id_dsa):
```

For Solaris 11:

```
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
```

- 4 Press Enter to accept the default location of `/.ssh/id_dsa`.
- 5 When the program asks you to enter the passphrase, press the Enter key twice.

Enter passphrase (empty for no passphrase):

Do not enter a passphrase. Press Enter.

Enter same passphrase again:

Press Enter again.

**To append the public key from the source system to the `authorized_keys` file on the target system, using secure file transfer**

- 1 Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems (system2 in this example).

To enable SFTP, the `/etc/ssh/sshd_config` file must contain the following two lines:

```
PermitRootLogin yes
Subsystem sftp /usr/lib/ssh/sftp-server
```

- 2 If the lines are not there, add them and restart ssh.

To restart ssh on Solaris 10 and Solaris 11, type the following command:

```
system1 # svcadm restart ssh
```

- 3 From the source system (system1), move the public key to a temporary file on the target system (system2).

Use the secure file transfer program.

In this example, the file name `id_dsa.pub` in the root directory is the name for the temporary file for the public key.

Use the following command for secure file transfer:

```
system1 # sftp system2
```

If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

```
Connecting to system2 ...
The authenticity of host 'system2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

- 4 Enter `yes`.

Output similar to the following is displayed:

```
Warning: Permanently added 'system2,10.182.00.00'
(DSA) to the list of known hosts.
root@system2 password:
```

- 5 Enter the root password of system2.
- 6 At the `sftp` prompt, type the following command:

```
sftp> put /.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /.ssh/id_dsa.pub to /id_dsa.pub
```

- 7 To quit the SFTP session, type the following command:

```
sftp> quit
```

- 8 To begin the `ssh` session on the target system (system2 in this example), type the following command on system1:

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

- 9 After you log in to system2, enter the following command to append the `id_dsa.pub` file to the `authorized_keys` file:

```
system2 # cat /id_dsa.pub >> /.ssh/authorized_keys
```

- 10 After the `id_dsa.pub` public key file is copied to the target system (system2), and added to the authorized keys file, delete it. To delete the `id_dsa.pub` public key file, enter the following command on system2:

```
system2 # rm /id_dsa.pub
```

- 11 To log out of the `ssh` session, enter the following command:

```
system2 # exit
```

- 12 When you install from a source system that is also an installation target, also add the local system `id_dsa.pub` key to the local `authorized_keys` file. The installation can fail if the installation source system is not authenticated.

To add the local system `id_dsa.pub` key to the local `authorized_keys` file, enter the following command:

```
system1 # cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys
```

- 13 Run the following commands on the source installation system. If your `ssh` session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and make the key globally available to the user `root`:

```
system1 # exec /usr/bin/ssh-agent $SHELL
```

```
system1 # ssh-add
```

```
Identity added: //./ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

### To verify that you can connect to a target system

- 1 On the source system (system1), enter the following command:

```
system1 # ssh -l root system2 uname -a
```

where system2 is the name of the target system.

- 2 The command should execute from the source system (system1) to the target system (system2) without the system requesting a passphrase or password.
- 3 Repeat this procedure for each target system.

## Restarting the ssh session

After you complete this procedure, ssh can be restarted in any of the following scenarios:

- After a terminal session is closed
- After a new terminal session is opened
- After a system is restarted
- After too much time has elapsed, to refresh ssh

### To restart ssh

- 1 On the source installation system (system1), bring the private key into the shell environment.

```
system1 # exec /usr/bin/ssh-agent $SHELL
```

- 2 Make the key globally available for the user root

```
system1 # ssh-add
```

## Enabling and disabling rsh for Solaris

The following section describes how to enable remote shell on Solaris system.

Veritas recommends configuring a secure shell environment for Veritas product installations.

See [“Manually configuring and passwordless ssh”](#) on page 416.

See the operating system documentation for more information on configuring remote shell.

### To enable rsh

- 1 To determine the current status of `rsh` and `rlogin`, type the following command:

```
inetadm | grep -i login
```

If the service is enabled, the following line is displayed:

```
enabled online svc:/network/login:rlogin
```

If the service is not enabled, the following line is displayed:

```
disabled disabled svc:/network/login:rlogin
```

- 2 To enable a disabled `rsh/rlogin` service, type the following command:

```
inetadm -e rlogin
```

- 3 To disable an enabled `rsh/rlogin` service, type the following command:

```
inetadm -d rlogin
```

- 4 Modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. This file must be modified for each user who remotely accesses the system using `rsh`. Each line of the `.rhosts` file contains a fully qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access `system1` from `system2`, you must add an entry for `system2.companyname.com` in the `.rhosts` file on `system1`.

```
echo "system2.companyname.com" >> $HOME/.rhosts
```

- 5 After you complete an installation procedure, delete the `.rhosts` file from each user's `$HOME` directory to ensure security:

```
rm -f $HOME/.rhosts
```

# SVS components

This appendix includes the following topics:

- [Symantec VirtualStore installation packages](#)
- [Veritas Cluster Server installation packages](#)
- [Veritas Cluster File System installation packages](#)
- [Chinese language packages](#)
- [Japanese language packages](#)
- [Veritas Storage Foundation obsolete and reorganized installation packages](#)

## Symantec VirtualStore installation packages

[Table F-1](#) shows the package name and contents for each English language package for Symantec VirtualStore. The table also gives you guidelines for which packages to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Symantec VirtualStore and Veritas Cluster Server (VCS) packages, the combined functionality is called Symantec VirtualStore and High Availability.

See [“Veritas Cluster Server installation packages”](#) on page 426.

**Table F-1** Symantec VirtualStore packages

| packages   | Contents                                                                                                                                                                                                                                                | Configuration |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| VRTSaslapm | Veritas Array Support Library (ASL) and Array Policy Module(APM) binaries<br><br>Required for the support and compatibility of various storage arrays.                                                                                                  | Minimum       |
| VRTSperl   | Perl 5.14.2 for Veritas                                                                                                                                                                                                                                 | Minimum       |
| VRTSsvs    | Symantec VirtualStore                                                                                                                                                                                                                                   | Minimum       |
| VRTSvlic   | Veritas License Utilities<br><br>Installs the license key layout files required to decode the Storage Foundation license keys. Provides the standard license key utilities vxlicrep, vxlicinst, and vxlictest.                                          | Minimum       |
| VRTSvxfs   | Veritas File System binaries<br><br>Required for VxFS file system support.                                                                                                                                                                              | Minimum       |
| VRTSvxvm   | Veritas Volume Manager binaries, scripts, and utilities. Required for VxVM volume manager support.                                                                                                                                                      | Minimum       |
| VRTSdbed   | Veritas Storage Foundation for Databases                                                                                                                                                                                                                | Recommended   |
| VRTSob     | Veritas Enterprise Administrator                                                                                                                                                                                                                        | Recommended   |
| VRTSodm    | Veritas ODM Driver for VxFS<br><br>Veritas Extension for Oracle Disk Manager is a custom storage interface designed specifically for Oracle9i and 10g. Oracle Disk Manager allows Oracle 9i and 10g to improve performance and manage system bandwidth. | Recommended   |



**Table F-1** Symantec VirtualStore packages (*continued*)

| packages    | Contents                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Configuration |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| VRTSsfcp601 | <p>Veritas Storage Foundation Common Product Installer</p> <p>The Storage Foundation Common Product installer package contains the installer libraries and product scripts that perform the following:</p> <ul style="list-style-type: none"> <li>■ installation</li> <li>■ configuration</li> <li>■ upgrade</li> <li>■ uninstallation</li> <li>■ adding nodes</li> <li>■ removing nodes</li> <li>■ etc.</li> </ul> <p>You can use these script to simplify the native operating system installations, configurations, and upgrades.</p> | Minimum       |
| VRTSsfmh    | <p>Veritas Storage Foundation Managed Host</p> <p>Discovers configuration information on a Storage Foundation managed host. This information is stored on a central database, which is not part of this release. You must download the database separately at:</p>                                                                                                                                                                                                                                                                       | Minimum       |
| VRTSspt     | Veritas Software Support Tools                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Recommended   |
| VRTSfsadv   | Minimum Veritas File System Advanced Solutions by Symantec (Solaris SPARC only).                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Minimum       |
| VRTSfssdk   | <p>Veritas File System Software Developer Kit</p> <p>For VxFS APIs, the package contains the public Software Developer Kit (headers, libraries, and sample code). It is required if some user programs use VxFS APIs.</p>                                                                                                                                                                                                                                                                                                                | All           |

## Veritas Cluster Server installation packages

[Table F-2](#) shows the package name and contents for each English language package for Veritas Cluster Server (VCS). The table also gives you guidelines for which packages to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Storage Foundation and VCS packages, the combined functionality is called Storage Foundation and High Availability.

See [“Symantec VirtualStore installation packages”](#) on page 423.

**Table F-2** VCS installation packages

| package   | Contents                                                                                                                                                                                                                                | Configuration |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| VRTSgab   | Veritas Cluster Server group membership and atomic broadcast services                                                                                                                                                                   | Minimum       |
| VRTSllt   | Veritas Cluster Server low-latency transport                                                                                                                                                                                            | Minimum       |
| VRTSamf   | Veritas Cluster Server Asynchronous Monitoring Framework                                                                                                                                                                                | Minimum       |
| VRTSvcS   | Veritas Cluster Server                                                                                                                                                                                                                  | Minimum       |
| VRTSvcSag | Veritas Cluster Server Bundled Agents                                                                                                                                                                                                   | Minimum       |
| VRTSvxfen | Veritas I/O Fencing                                                                                                                                                                                                                     | Minimum       |
| VRTSvcsea | Consolidated database and enterprise agent packages                                                                                                                                                                                     | Recommended   |
| VRTScps   | Veritas Coordination Point Server<br><br>The Coordination Point Server is an alternate mechanism for I/O fencing. It implements I/O fencing through a client/server architecture and can provide I/O fencing for multiple VCS clusters. | All           |

## Veritas Cluster File System installation packages

[Table F-3](#) shows the package name and contents for each English language package for Veritas Cluster File System (CFS). The table also gives you guidelines for which

packages to install based whether you want the minimum, recommended, or advanced configuration.

When you install all CFS packages and all the packages that comprise Storage Foundation and Veritas Cluster Server, the resulting functionality is called Storage Foundation Cluster File System.

See “[Symantec VirtualStore installation packages](#)” on page 423.

See “[Veritas Cluster Server installation packages](#)” on page 426.

**Table F-3** CFS installation packages

| package  | Contents                                                                    | Configuration |
|----------|-----------------------------------------------------------------------------|---------------|
| VRTScavf | Veritas Cluster Server Agents for Storage Foundation Cluster File System    | Minimum       |
| VRTSglm  | Veritas Group Lock Manager for Storage Foundation Cluster File System       | Minimum       |
| VRTSgms  | Veritas Group Messaging Services for Storage Foundation Cluster File System | Recommended   |

## Chinese language packages

The following table shows the package name and contents for each Chinese language package.

**Table F-4** Chinese language packages

| package  | Contents                                                                       |
|----------|--------------------------------------------------------------------------------|
| VRTSzhvm | Chinese Veritas Volume Manager by Symantec – Message Catalogs and Manual Pages |

## Japanese language packages

The following table show the package name and contents for each Japanese language package.

**Table F-5** Japanese language packages

| package   | Contents                                                                                                                          |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------|
| VRTSjacav | Japanese Veritas Cluster Server Agents for Storage Foundation Cluster File System – Manual Pages and Message Catalogs by Symantec |

**Table F-5** Japanese language packages (*continued*)

| package   | Contents                                                                          |
|-----------|-----------------------------------------------------------------------------------|
| VRTSjacs  | Veritas Cluster Server Japanese Message Catalogs by Symantec                      |
| VRTSjacse | Japanese Veritas High Availability Enterprise Agents by Symantec                  |
| VRTSjadba | Japanese Veritas Oracle Real Application Cluster Support package by Symantec      |
| VRTSjadbe | Japanese Veritas Storage Foundation for Oracle from Symantec – Message Catalogs   |
| VRTSjafs  | Japanese Veritas File System – Message Catalog and Manual Pages                   |
| VRTSjaodm | Veritas Oracle Disk Manager Japanese Message Catalog and Manual Pages by Symantec |
| VRTSjavm  | Japanese Veritas Volume Manager by Symantec – Message Catalogs and Manual Pages   |
| VRTSmulic | Multi-language Symantec License Utilities                                         |

## Veritas Storage Foundation obsolete and reorganized installation packages

[Table F-6](#) lists the packages that are obsolete or reorganized for Symantec VirtualStore.

**Table F-6** Veritas Storage Foundation obsolete and reorganized packages

| package                            | Description          |
|------------------------------------|----------------------|
| Obsolete and reorganized for 6.0.1 |                      |
| VRTSat                             | Obsolete             |
| VRTSatZH                           | Obsolete             |
| VRTSatJA                           | Obsolete             |
| Obsolete and reorganized for 5.1   |                      |
| Infrastructure                     |                      |
| SYMClma                            | Obsolete             |
| VRTSaa                             | Included in VRTSsfmh |

**Table F-6** Veritas Storage Foundation obsolete and reorganized packages  
(continued)

| package          | Description                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VRTSccg          | Included in VRTSsfmh                                                                                                                                                                                                                                                                                                                                                                                                |
| VRTSdbms3        | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSicsco        | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSjre          | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSjre15        | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSmh           | Included in VRTSsfmh                                                                                                                                                                                                                                                                                                                                                                                                |
| VRTSobc33        | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSobweb        | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSobgui        | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSpbx          | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSsfm          | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTSweb          | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| Product packages |                                                                                                                                                                                                                                                                                                                                                                                                                     |
| VRTSacclib       | <p>Obsolete</p> <p>The following information is for installations, upgrades, and uninstalls using the script- or Web-based installer.</p> <ul style="list-style-type: none"> <li>■ For fresh installations VRTSacclib is not installed.</li> <li>■ For upgrades, the existing VRTSacclib is uninstalled and a new VRTSacclib is installed.</li> <li>■ For uninstallation, VRTSacclib is not uninstalled.</li> </ul> |
| VRTSalloc        | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTScmccc        | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTScmcm         | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRTScmcs         | Obsolete                                                                                                                                                                                                                                                                                                                                                                                                            |

**Table F-6** Veritas Storage Foundation obsolete and reorganized packages  
*(continued)*

| package   | Description                             |
|-----------|-----------------------------------------|
| VRTScscm  | Obsolete                                |
| VRTScscw  | Obsolete                                |
| VRTScsocw | Obsolete                                |
| VRTScssim | Obsolete                                |
| VRTScutil | Obsolete                                |
| VRTSd2gui | Included in VRTSdbed                    |
| VRTSdb2ed | Included in VRTSdbed                    |
| VRTSdbcom | Included in VRTSdbed                    |
| VRTSdbed  | Included in VRTSdbed                    |
| VRTSdcli  | Obsolete                                |
| VRTSddlpr | Obsolete                                |
| VRTSdsa   | Obsolete                                |
| VRTSfas   | Obsolete                                |
| VRTSfasag | Obsolete                                |
| VRTSfsman | Included in the product's main package. |
| VRTSfsmnd | Included in the product's main package. |
| VRTSfspro | Included in VRTSsfmh                    |
| VRTSgapms | Obsolete                                |
| VRTSmapro | Included in VRTSsfmh                    |
| VRTSorgui | Obsolete                                |
| VRTSsybed | Included in VRTSdbed                    |
| VRTSvail  | Obsolete                                |
| VRTSvcsdb | Included in VRTSvcsea                   |
| VRTSvcsmn | Included in VRTSvcs                     |

**Table F-6** Veritas Storage Foundation obsolete and reorganized packages  
(continued)

| package       | Description                             |
|---------------|-----------------------------------------|
| VRTSvcsor     | Included in VRTSvcssea                  |
| VRTSvcssy     | Included in VRTSvcssea                  |
| VRTSvcsvr     | Included in VRTSvcs                     |
| VRTSvdid      | Obsolete                                |
| VRTSvmman     | Included in the product's main package. |
| VRTSvmpro     | Included in VRTSsfmh                    |
| VRTSvrpro     | Included in VRTSob                      |
| VRTSvrw       | Obsolete                                |
| VRTSvxmsa     | Obsolete                                |
| Documentation | All Documentation packages obsolete     |

**Veritas Storage Foundation obsolete and reorganized installation packages**



# Sample SVS cluster setup diagrams for CP server-based I/O fencing

This appendix includes the following topics:

- [Configuration diagrams for setting up server-based I/O fencing](#)

## Configuration diagrams for setting up server-based I/O fencing

The following CP server configuration diagrams can be used as guides when setting up CP server within your configuration:

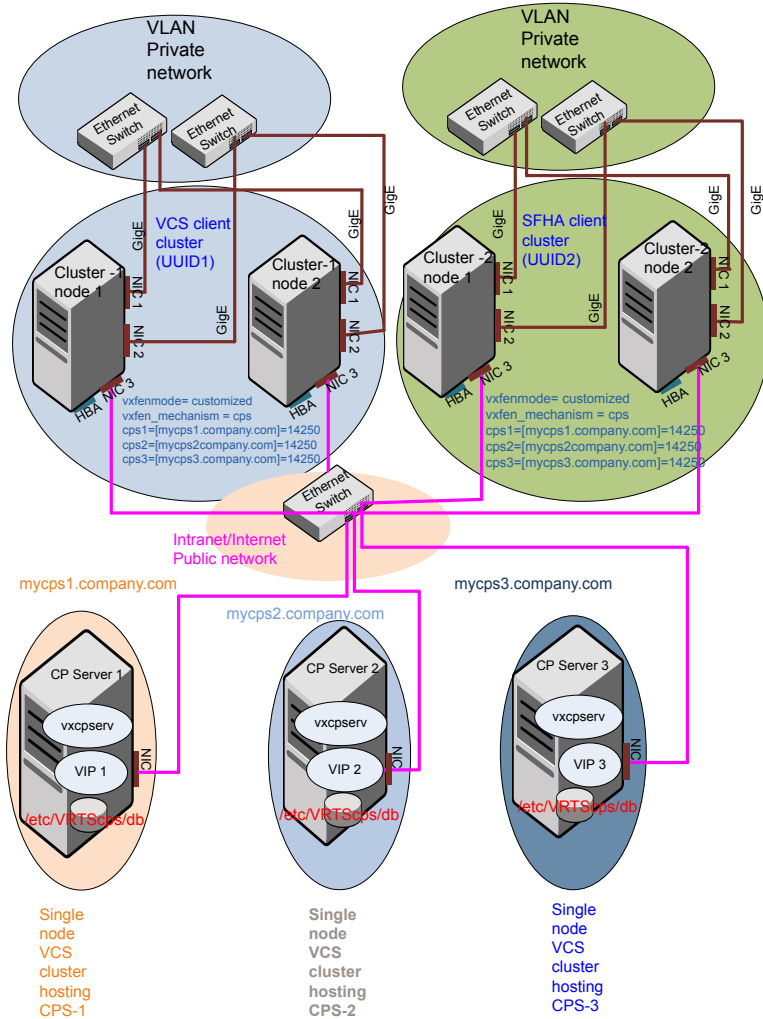
- Two unique client clusters that are served by 3 CP servers:  
See [Figure G-1](#) on page 434.
- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:
- Two node campus cluster that is served by remote CP server and 2 SCSI-3 disks:
- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:

### Two unique client clusters served by 3 CP servers

[Figure G-1](#) displays a configuration where two unique client clusters are being served by 3 CP servers (coordination points). Each client cluster has its own unique user ID (UUID1 and UUID2).

In the `vxfenmode` file on the client nodes, `vxfenmode` is set to `customized` with `vxfen` mechanism set to `cps`.

**Figure G-1** Two unique client clusters served by 3 CP servers



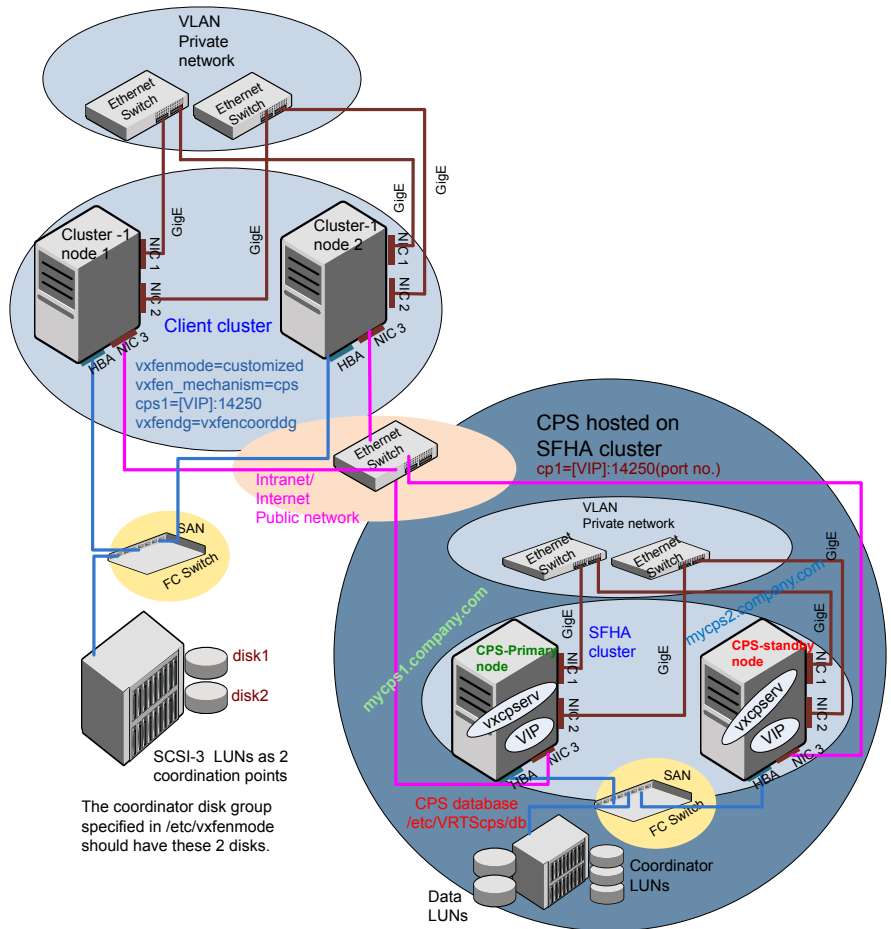
## Client cluster served by highly available CPS and 2 SCSI-3 disks

Figure G-2 displays a configuration where a client cluster is served by one highly available CP server and 2 local SCSI-3 LUNs (disks).

In the `vxfenmode` file on the client nodes, `vxfenmode` is set to customized with `vxfen` mechanism set to `cps`.

The two SCSI-3 disks are part of the disk group `vxencoorddg`. The third coordination point is a CP server hosted on an SFHA cluster, with its own shared database and coordinator disks.

**Figure G-2** Client cluster served by highly available CP server and 2 SCSI-3 disks



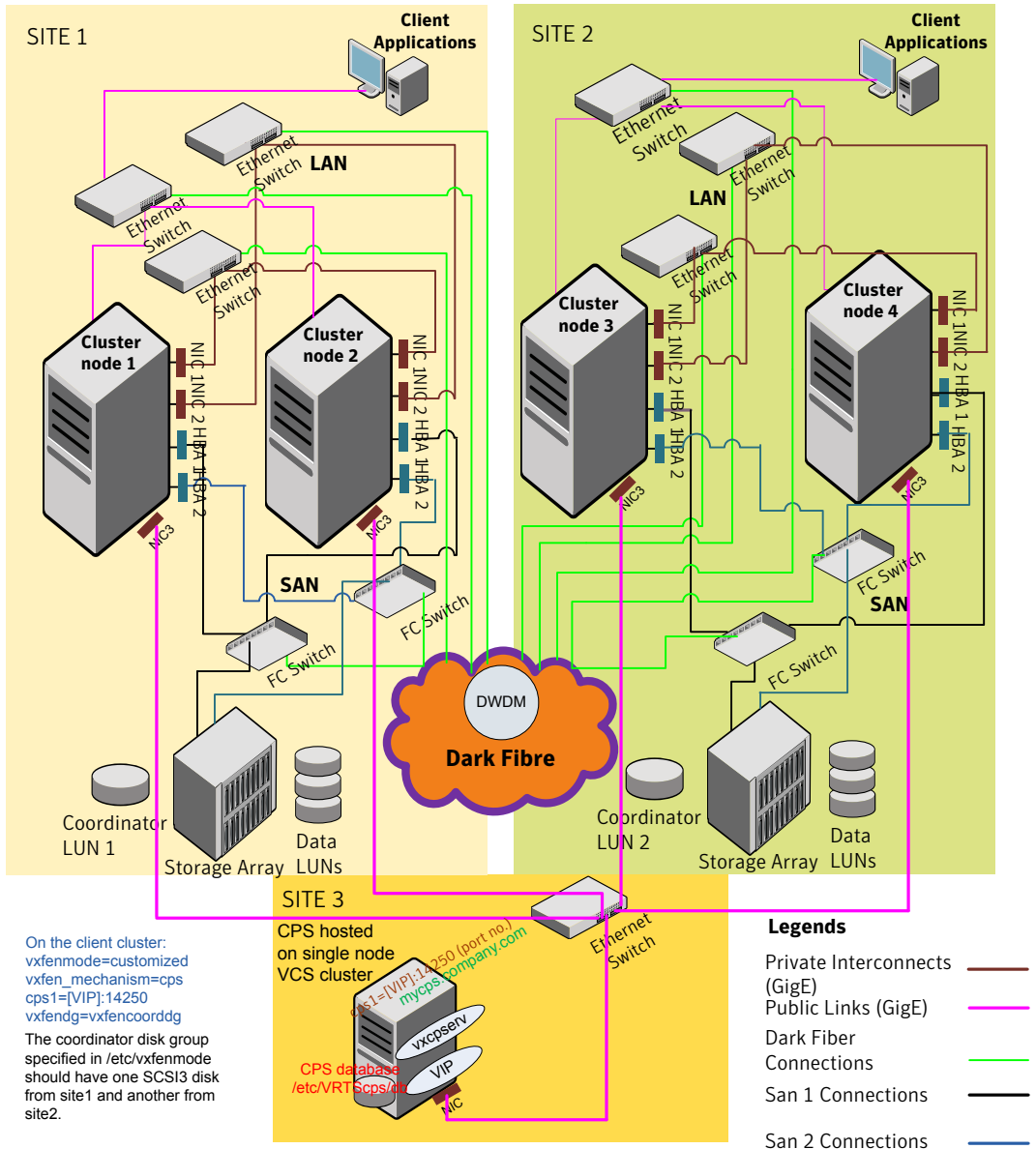
## Two node campus cluster served by remote CP server and 2 SCSI-3 disks

[Figure G-3](#) displays a configuration where a two node campus cluster is being served by one remote CP server and 2 local SCSI-3 LUN (disks).

In the `vxfenmode` file on the client nodes, `vxfenmode` is set to `customized` with `vxfen` mechanism set to `cps`.

The two SCSI-3 disks (one from each site) are part of disk group `vxfencoorddg`. The third coordination point is a CP server on a single node VCS cluster.

**Figure G-3** Two node campus cluster served by remote CP server and 2 SCSI-3



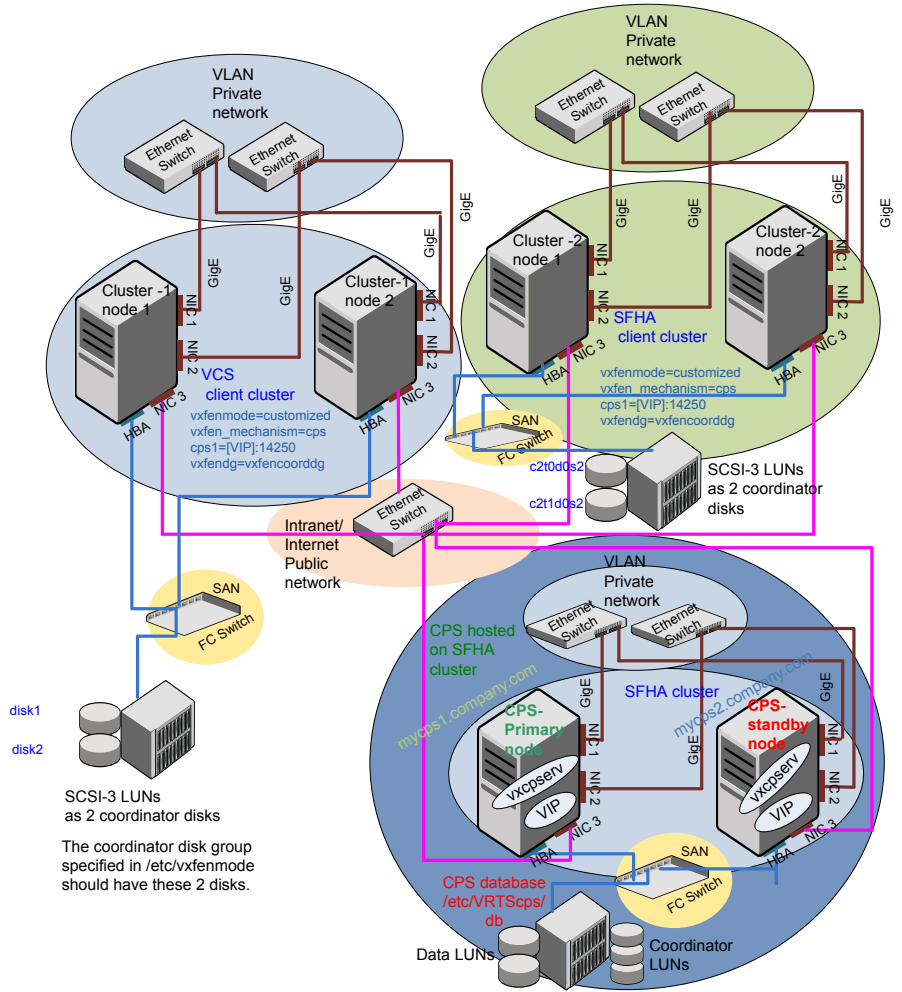
## Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

[Figure G-4](#) displays a configuration where multiple client clusters are being served by one highly available CP server and 2 local SCSI-3 LUNS (disks).

In the `vxfenmode` file on the client nodes, `vxfenmode` is set to `customized` with `vxfen` mechanism set to `cps`.

The two SCSI-3 disks are part of the disk group `vxfencoorddg`. The third coordination point is a CP server, hosted on an SFHA cluster, with its own shared database and coordinator disks.

**Figure G-4** Multiple client clusters served by highly available CP server and 2 SCSI-3 disks







# Configuring LLT over UDP using IPv6

This appendix includes the following topics:

- [Using the UDP layer of IPv6 for LLT](#)
- [Manually configuring LLT over UDP using IPv6](#)

## Using the UDP layer of IPv6 for LLT

6.0.1 provides the option of using LLT over the UDP (User Datagram Protocol) layer for clusters using wide-area networks and routers. UDP makes LLT packets routable and thus able to span longer distances more economically.

### When to use LLT over UDP

Use LLT over UDP in the following situations:

- LLT must be used over WANs
- When hardware, such as blade servers, do not support LLT over Ethernet

## Manually configuring LLT over UDP using IPv6

The following checklist is to configure LLT over UDP:

- For UDP6, the multicast address is set to "-".
- Make sure that each NIC has an IPv6 address that is configured before configuring LLT.
- Make sure the IPv6 addresses in the `/etc/llttab` files are consistent with the IPv6 addresses of the network interfaces.

- Make sure that each link has a unique not well-known UDP port.  
 See [“Selecting UDP ports”](#) on page 443.
- For the links that cross an IP router, disable multicast features and specify the IPv6 address of each link manually in the /etc/llttab file.  
 See [“Sample configuration: links crossing IP routers”](#) on page 446.

## The link command in the /etc/llttab file

Review the link command information in this section for the /etc/llttab file. See the following information for sample configurations:

- See [“Sample configuration: direct-attached links”](#) on page 444.
- See [“Sample configuration: links crossing IP routers”](#) on page 446.

Note that some of the fields in [Table H-1](#) differ from the command for standard LLT links.

[Table H-1](#) describes the fields of the link command that are shown in the /etc/llttab file examples.

**Table H-1** Field description for link command in /etc/llttab

| Field                | Description                                                                                                                                                                                  |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>tag-name</i>      | A unique string that is used as a tag by LLT; for example link1, link2,....                                                                                                                  |
| <i>device</i>        | The device path of the UDP protocol; for example /dev/udp6.                                                                                                                                  |
| <i>node-range</i>    | Nodes using the link. "-" indicates all cluster nodes are to be configured for this link.                                                                                                    |
| <i>link-type</i>     | Type of link; must be "udp6" for LLT over UDP.                                                                                                                                               |
| <i>udp-port</i>      | Unique UDP port in the range of 49152-65535 for the link.<br>See <a href="#">“Selecting UDP ports”</a> on page 443.                                                                          |
| <i>MTU</i>           | "-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the <code>lltstat -l</code> command to display the current value. |
| <i>IPv6 address</i>  | IPv6 address of the link on the local node.                                                                                                                                                  |
| <i>mcast-address</i> | "-" is the default for clusters spanning routers.                                                                                                                                            |

## The set-addr command in the /etc/llttab file

The `set-addr` command in the `/etc/llttab` file is required when the multicast feature of LLT is disabled, such as when LLT must cross IP routers.

See “[Sample configuration: links crossing IP routers](#)” on page 446.

[Table H-2](#) describes the fields of the `set-addr` command.

**Table H-2** Field description for `set-addr` command in `/etc/llttab`

| Field                | Description                                                                  |
|----------------------|------------------------------------------------------------------------------|
| <i>node-id</i>       | The ID of the cluster node; for example, 0.                                  |
| <i>link tag-name</i> | The string that LLT uses to identify the link; for example link1, link2,.... |
| <i>address</i>       | IPv6 address assigned to the link for the peer node.                         |

## Selecting UDP ports

When you select a UDP port, select an available 16-bit integer from the range that follows:

- Use available ports in the private range 49152 to 65535
- Do not use the following ports:
  - Ports from the range of well-known ports, 0 to 1023
  - Ports from the range of registered ports, 1024 to 49151

To check which ports are defined as defaults for a node, examine the file `/etc/services`. You should also use the `netstat` command to list the UDP ports currently in use. For example:

```
netstat -a | more
```

```
UDP: IPv4
 Local Address Remote Address State

 *.sunrpc Idle
 . Unbound
 *.32772 Idle
 . Unbound
 *.32773 Idle
 *.lockd Idle
 *.32777 Idle
```

```
*.32778 Idle
*.32779 Idle
*.32780 Idle
*.servicetag Idle
*.syslog Idle
*.16161 Idle
*.32789 Idle
*.177 Idle
*.32792 Idle
*.32798 Idle
*.snmpd Idle
*.32802 Idle
. Unbound
. Unbound
. Unbound
```

UDP: IPv6

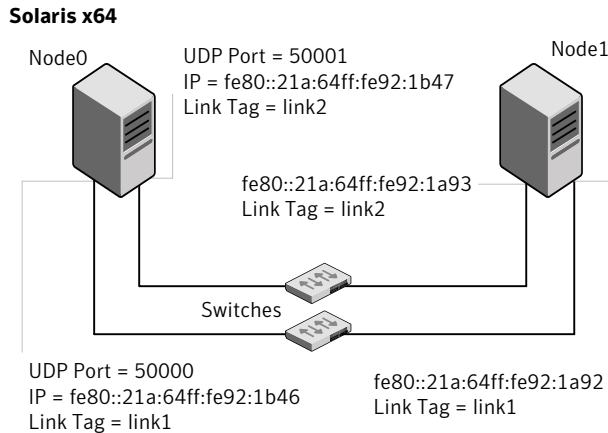
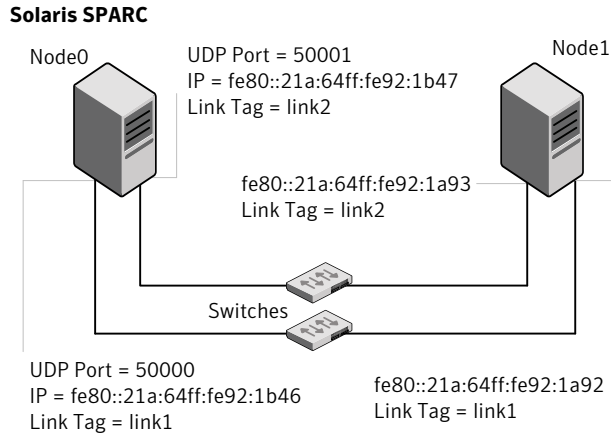
| Local Address | Remote Address | State | If |
|---------------|----------------|-------|----|
| *.servicetag  |                | Idle  |    |
| *.177         |                | Idle  |    |

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the /etc/services file, its associated name is displayed rather than the port number in the output.

## Sample configuration: direct-attached links

[Figure H-1](#) depicts a typical configuration of direct-attached links employing LLT over UDP.

**Figure H-1** A typical configuration of direct-attached links that use LLT over UDP



The configuration that the `/etc/llttab` file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT uses IPv6 multicast requests for peer node address discovery. So the addresses of peer nodes do not need to be specified in the `/etc/llttab` file using the `set-addr` command. Use the `ifconfig -a` command to verify that the IPv6 address is set correctly.

```
set-node Node0
set-cluster 1
```

```
#configure Links
#link tag-name device node-range link-type udp port MTU \
 IP-address mcast-address
link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -
```

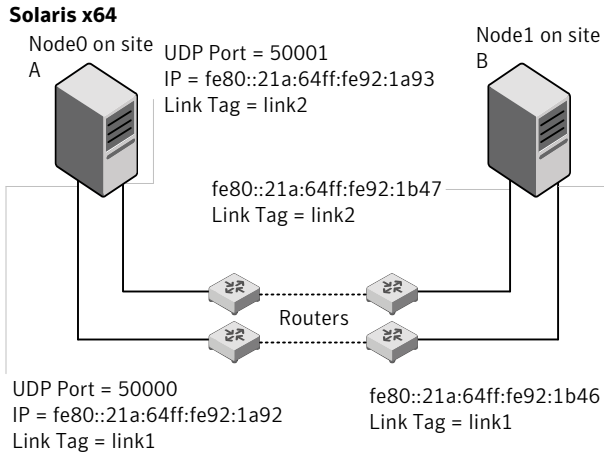
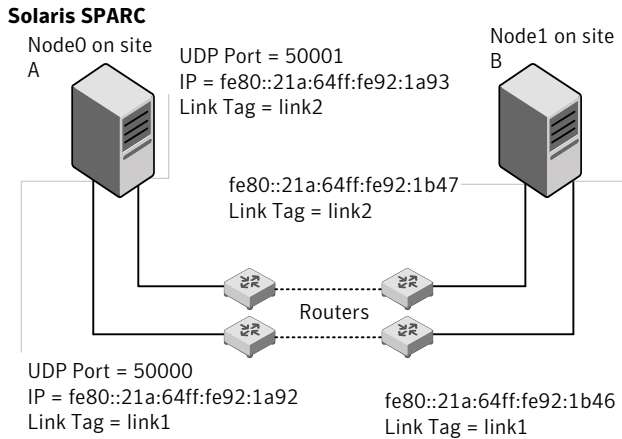
The file for Node 1 resembles:

```
set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
 IP-address mcast-address
link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -
```

## Sample configuration: links crossing IP routers

**Figure H-2** depicts a typical configuration of links crossing an IP router employing LLT over UDP. The illustration shows two nodes of a four-node cluster.

**Figure H-2** A typical configuration of links crossing an IP router



The configuration that the following `/etc/llttab` file represents for Node 1 has links crossing IP routers. Notice that IPv6 addresses are shown for each link on each peer node. In this configuration multicasts are disabled.

```
set-node Node1
set-cluster 1

link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -

#set address of each link for all peer nodes in the cluster
```

```
#format: set-addr node-id link tag-name address
set-addr 0 link1 fe80::21a:64ff:fe92:1b46
set-addr 0 link2 fe80::21a:64ff:fe92:1b47
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb 0
set-arp 0
```

**The /etc/llttab file on Node 0 resembles:**

```
set-node Node0
set-cluster 1

link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -
link link2 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 1 link1 fe80::21a:64ff:fe92:1a92
set-addr 1 link2 fe80::21a:64ff:fe92:1a93
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb 0
set-arp 0
```



## Configuring LLT over UDP using IPv4

This appendix includes the following topics:

- [Using the UDP layer for LLT](#)
- [Manually configuring LLT over UDP using IPv4](#)

### Using the UDP layer for LLT

SVS provides the option of using LLT over the UDP (User Datagram Protocol) layer for clusters using wide-area networks and routers. UDP makes LLT packets routable and thus able to span longer distances more economically.

#### When to use LLT over UDP

Use LLT over UDP in the following situations:

- LLT must be used over WANs
- When hardware, such as blade servers, do not support LLT over Ethernet

LLT over UDP is slower than LLT over Ethernet. Use LLT over UDP only when the hardware configuration makes it necessary.

### Manually configuring LLT over UDP using IPv4

The following checklist is to configure LLT over UDP:

- Make sure that the LLT private links are on separate subnets. Set the broadcast address in `/etc/l1ttab` explicitly depending on the subnet for each link. See [“Broadcast address in the `/etc/l1ttab` file”](#) on page 450.

- Make sure that each NIC has an IP address that is configured before configuring LLT.
- Make sure the IP addresses in the `/etc/llttab` files are consistent with the IP addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port. See “[Selecting UDP ports](#)” on page 452.
- Set the broadcast address correctly for direct-attached (non-routed) links. See “[Sample configuration: direct-attached links](#)” on page 454.
- For the links that cross an IP router, disable broadcast features and specify the IP address of each link manually in the `/etc/llttab` file. See “[Sample configuration: links crossing IP routers](#)” on page 455.

## Broadcast address in the `/etc/llttab` file

The broadcast address is set explicitly for each link in the following example.

- Display the content of the `/etc/llttab` file on the first node `sys1`:

```
sys1 # cat /etc/llttab

set-node sys1
set-cluster 1
link link1 /dev/udp - udp 50000 - 192.168.9.1 192.168.9.255
link link2 /dev/udp - udp 50001 - 192.168.10.1 192.168.10.255
```

Verify the subnet mask using the `ifconfig` command to ensure that the two links are on separate subnets.

- Display the content of the `/etc/llttab` file on the second node `sys2`:

```
sys2 # cat /etc/llttab

set-node sys2
set-cluster 1
link link1 /dev/udp - udp 50000 - 192.168.9.2 192.168.9.255
link link2 /dev/udp - udp 50001 - 192.168.10.2 192.168.10.255
```

Verify the subnet mask using the `ifconfig` command to ensure that the two links are on separate subnets.

## The link command in the `/etc/llttab` file

Review the link command information in this section for the `/etc/llttab` file. See the following information for sample configurations:

- See “[Sample configuration: direct-attached links](#)” on page 454.
- See “[Sample configuration: links crossing IP routers](#)” on page 455.

[Table I-1](#) describes the fields of the link command that are shown in the /etc/llttab file examples. Note that some of the fields differ from the command for standard LLT links.

**Table I-1** Field description for link command in /etc/llttab

| Field                | Description                                                                                                                                                                                               |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>tag-name</i>      | A unique string that is used as a tag by LLT; for example link1, link2,....                                                                                                                               |
| <i>device</i>        | The device path of the UDP protocol; for example /dev/udp.                                                                                                                                                |
| <i>node-range</i>    | Nodes using the link. "-" indicates all cluster nodes are to be configured for this link.                                                                                                                 |
| <i>link-type</i>     | Type of link; must be "udp" for LLT over UDP.                                                                                                                                                             |
| <i>udp-port</i>      | Unique UDP port in the range of 49152-65535 for the link.<br>See “ <a href="#">Selecting UDP ports</a> ” on page 452.                                                                                     |
| <i>MTU</i>           | "-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the <code>lltstat -l</code> command to display the current value.              |
| <i>IP address</i>    | IP address of the link on the local node.                                                                                                                                                                 |
| <i>bcast-address</i> | <ul style="list-style-type: none"> <li>■ For clusters with enabled broadcasts, specify the value of the subnet broadcast address.</li> <li>■ "-" is the default for clusters spanning routers.</li> </ul> |

## The set-addr command in the /etc/llttab file

The `set-addr` command in the /etc/llttab file is required when the broadcast feature of LLT is disabled, such as when LLT must cross IP routers.

See “[Sample configuration: links crossing IP routers](#)” on page 455.

[Table I-2](#) describes the fields of the set-addr command.

**Table I-2** Field description for set-addr command in /etc/llttab

| Field          | Description                                 |
|----------------|---------------------------------------------|
| <i>node-id</i> | The ID of the cluster node; for example, 0. |

**Table I-2** Field description for set-addr command in /etc/llttab (continued)

| Field                | Description                                                                  |
|----------------------|------------------------------------------------------------------------------|
| <i>link tag-name</i> | The string that LLT uses to identify the link; for example link1, link2,.... |
| <i>address</i>       | IP address assigned to the link for the peer node.                           |

## Selecting UDP ports

When you select a UDP port, select an available 16-bit integer from the range that follows:

- Use available ports in the private range 49152 to 65535
- Do not use the following ports:
  - Ports from the range of well-known ports, 0 to 1023
  - Ports from the range of registered ports, 1024 to 49151

To check which ports are defined as defaults for a node, examine the file /etc/services. You should also use the `netstat` command to list the UDP ports currently in use. For example:

```
netstat -a | more
UDP
 Local Address Remote Address State

 *.sunrpc Idle
 *. * Unbound
 *.32771 Idle
 *.32776 Idle
 *.32777 Idle
 *.name Idle
 *.biff Idle
 *.talk Idle
 *.32779 Idle
 .
 .
 .
 *.55098 Idle
 *.syslog Idle
 *.58702 Idle
 *. * Unbound
```

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the `/etc/services` file, its associated name is displayed rather than the port number in the output.

## Configuring the netmask for LLT

For nodes on different subnets, set the netmask so that the nodes can access the subnets in use. Run the following command and answer the prompt to set the netmask:

```
ifconfig interface_name netmask netmask
```

For example:

- For the first network interface on the node `sys1`:

```
IP address=192.168.9.1, Broadcast address=192.168.9.255,
Netmask=255.255.255.0
```

For the first network interface on the node `sys2`:

```
IP address=192.168.9.2, Broadcast address=192.168.9.255,
Netmask=255.255.255.0
```

- For the second network interface on the node `sys1`:

```
IP address=192.168.10.1, Broadcast address=192.168.10.255,
Netmask=255.255.255.0
```

For the second network interface on the node `sys2`:

```
IP address=192.168.10.2, Broadcast address=192.168.10.255,
Netmask=255.255.255.0
```

## Configuring the broadcast address for LLT

For nodes on different subnets, set the broadcast address in `/etc/llttab` depending on the subnet that the links are on.

An example of a typical `/etc/llttab` file when nodes are on different subnets. Note the explicitly set broadcast address for each link.

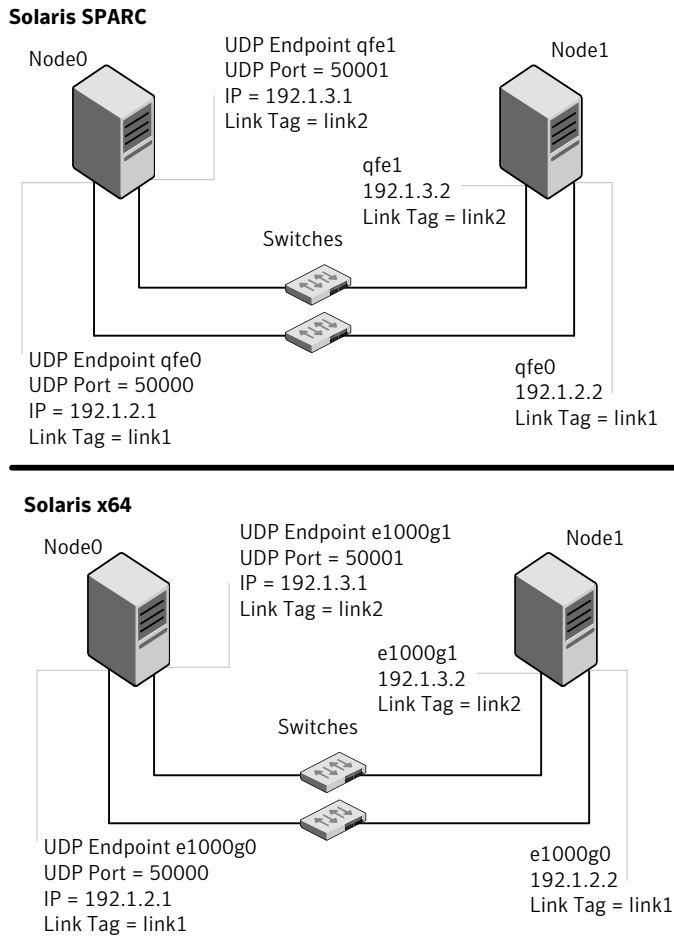
```
cat /etc/llttab
set-node nodexyz
set-cluster 100
```

```
link link1 /dev/udp - udp 50000 - 192.168.30.1 192.168.30.255
link link2 /dev/udp - udp 50001 - 192.168.31.1 192.168.31.255
```

## Sample configuration: direct-attached links

Figure I-1 depicts a typical configuration of direct-attached links employing LLT over UDP.

Figure I-1 A typical configuration of direct-attached links that use LLT over UDP



The configuration that the `/etc/llttab` file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT broadcasts requests peer nodes to discover their addresses. So the addresses of peer nodes do not need to be specified in the `/etc/llttab` file using the `set-addr` command. For direct attached links, you do need to set the broadcast address of the links in the `/etc/llttab` file. Verify that the IP addresses and broadcast addresses are set correctly by using the `ifconfig -a` command.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.1 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.1 192.1.3.255
```

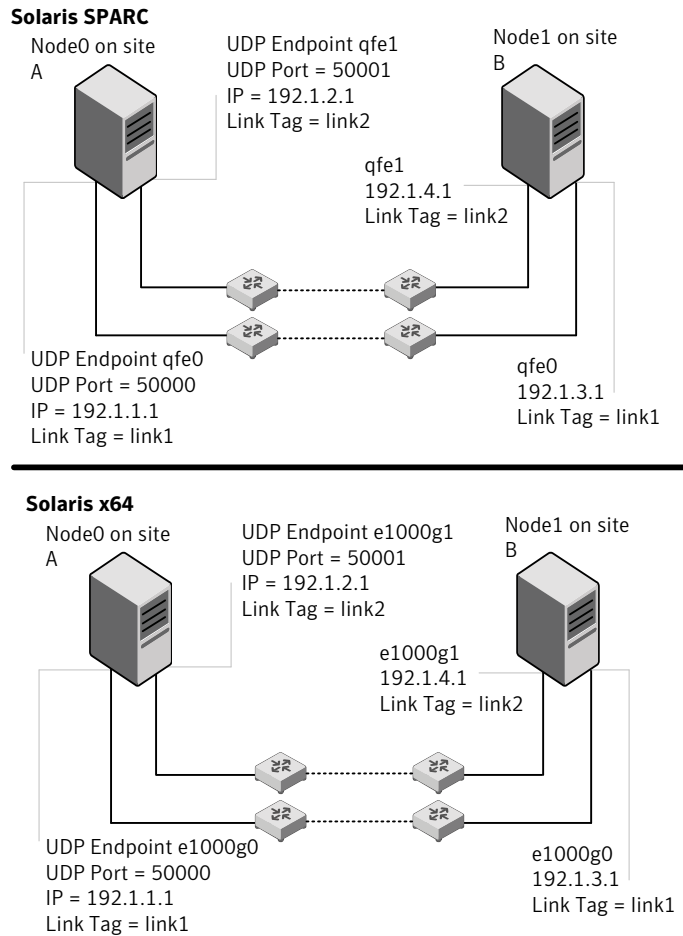
The file for Node 1 resembles:

```
set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.2 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.2 192.1.3.255
```

## Sample configuration: links crossing IP routers

[Figure I-2](#) depicts a typical configuration of links crossing an IP router employing LLT over UDP. The illustration shows two nodes of a four-node cluster.

Figure I-2 A typical configuration of links crossing an IP router



The configuration that the following `/etc/llttab` file represents for Node 1 has links crossing IP routers. Notice that IP addresses are shown for each link on each peer node. In this configuration broadcasts are disabled. Hence, the broadcast address does not need to be set in the `link` command of the `/etc/llttab` file.

```
set-node Node1
set-cluster 1
```



```

link link1 /dev/udp - udp 50000 - 192.1.3.1 -
link link2 /dev/udp - udp 50001 - 192.1.4.1 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 0 link1 192.1.1.1
set-addr 0 link2 192.1.2.1
set-addr 2 link1 192.1.5.2
set-addr 2 link2 192.1.6.2
set-addr 3 link1 192.1.7.3
set-addr 3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb 0
set-arp 0

```

**The /etc/llttab file on Node 0 resembles:**

```

set-node Node0
set-cluster 1

link link1 /dev/udp - udp 50000 - 192.1.1.1 -
link link2 /dev/udp - udp 50001 - 192.1.2.1 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 1 link1 192.1.3.1
set-addr 1 link2 192.1.4.1
set-addr 2 link1 192.1.5.2
set-addr 2 link2 192.1.6.2
set-addr 3 link1 192.1.7.3
set-addr 3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb 0
set-arp 0

```



# Compatibility issues when installing Symantec VirtualStore with other products

This appendix includes the following topics:

- [Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present](#)
- [Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present](#)
- [Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present](#)

## Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.

## Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host packages as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

## Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSspb and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSspb, VRTSicsco, and VRTSat.

# Index

## A

- about
  - Symantec VirtualStore 21
- Adding
  - connection to Citrix Desktop Studio 319
- adding
  - users 114
- agents
  - disabling 376
- applications, stopping 250
- attributes
  - UseFence 135

## B

- backup boot disk group 288
  - rejoining 288

## C

- cables
  - cross-over Ethernet 335
- Citrix Desktop Studio
  - adding a connection to 319
- Citrix XenDesktop
  - about adding virtual machine clones 317
  - connecting to a vCenter Server 318
- Citrix XenDesktop extension
  - creating virtual machine clones 322
- cluster
  - removing a node from 353
- Clustered NFS
  - setting up 296
- commands
  - format 51
  - hacf 258
  - vxdisksetup (initializing disks) 123
  - vxlicinst 121
  - vxlicrep 120
- configuring
  - rsh 48
  - ssh 48

- configuring (*continued*)
  - VirtualStore Web Server for cluster failover 299
  - VMware View 315
- configuring Symantec VirtualStore
  - script-based installer 101
- configuring VCS
  - adding users 114
  - event notification 115–116
  - global clusters 118
  - starting 102
- controllers
  - SCSI 48
- coordinator disks
  - DMP devices 25
  - for I/O fencing 25
  - setting up 133
- creating
  - Flash archive 223
  - post-deployment scripts 224
- creating virtual machine clones
  - specifying where to create 311
  - using Citrix XenDesktop 322
  - using Symantec FileSnap 309

## D

- data disks
  - for I/O fencing 25
- deployment
  - testing desktop group 327
- desktop group
  - testing the deployment 327
- disabling the agents 376
- disks
  - adding and initializing 123
  - coordinator 133
  - testing with vxfentsthdw 127
  - verifying node access 129

## E

- ESX servers
  - adding storage to 308

Ethernet controllers 335

## F

FC-AL controllers 51  
 Fibre Channel fabric 54  
 flarcreate 223  
 Flash archive 223  
   post-deployment scripts 224  
 freezing service groups 250

## G

global clusters  
   configuration 118  
 guest operating system  
   specifying if customizing for Linux or  
   Windows 312

## H

hubs  
   independent 335

## I

I/O fencing  
   checking disks 127  
   setting up 132  
   shared storage 127  
 I/O fencing requirements  
   non-SCSI-3 34  
 installer  
   Symantec VirtualStore 67  
 Installing  
   SVS with the Web-based installer 175  
   Symantec VirtualStore using the installer 67  
 installing  
   JumpStart 219  
   post 119

## J

JumpStart  
   installing 219

## L

license keys  
   adding with vxlicinst 121  
   replacing demo key 121  
 licenses  
   information about 120

## LLT

  interconnects 47  
 localized environment settings for using VVR  
   settings for using VVR in a localized  
   environment 247

## M

media speed 47  
   optimizing 47

## N

network customization parameters  
   specifying for guest operating systems if using  
   DHCP or Static IP 314  
 nodes  
   adding application nodes  
   configuring GAB 342  
   configuring LLT 342  
   configuring VXFEN 342  
   starting Volume Manager 341  
 non-SCSI-3 fencing  
   manual configuration 160  
   setting up 160  
 non-SCSI-3 I/O fencing  
   requirements 34  
 non-SCSI3 fencing  
   setting up 146  
   using installsvs 146  
 number of virtual machines to be created  
   specifying 311

## O

optimizing  
   media speed 47

## P

persistent reservations  
   SCSI-3 48  
 planning to upgrade VVR 244  
 post-deployment scripts 224  
 pre-requisites  
   virtual machine customization 301  
   VMware View Integration 302  
 preinstallation 244  
 preparing to upgrade VVR 250

**R**

- registered
    - VMware vCenter Servers 303
  - Registering
    - VirtualStore cluster 300
  - rejoining
    - backup boot disk group 288
  - removing
    - the Replicated Data Set 376
  - removing a system from a cluster 353
  - Replicated Data Set
    - removing the 376
  - rolling upgrade 273, 276
    - versions 273
  - rsh 103
    - configuration 48
- S**
- SAN
    - see Storage Area Network 54
  - script-based installer
    - Symantec VirtualStore configuration overview 101
  - SCSI-3
    - persistent reservations 48
  - SCSI-3 persistent reservations
    - verifying 132
  - service groups
    - freezing 250
  - setting up
    - Clustered NFS 296
    - VirtualStore vSphere Service Console 299
  - settings for using VVR in a localized environment
    - localized environment settings for using VVR 247
  - shared storage
    - Fibre Channel
      - setting up 51
  - SMTP email notification 115
  - SNMP trap notification 116
  - Solution
    - Symantec VirtualStore 21
  - specifying
    - number of virtual machine clones to be created 311
  - specifying guest operating system
    - if customizing for Linux or Windows 312

- specifying network customization parameters for guest operating systems
  - if customizing for DHCP or Static IP 314
- ssh 103
  - configuration 48
- starting configuration
  - installvcs program 103
  - Veritas product installer 102
- stopping
  - applications 250
- storage
  - adding to ESX servers 308
  - setting up shared fibre 51
- Storage Area Network 54
- SVS
  - coordinator disks 133
- Symantec FileSnap
  - creating virtual machine clones with 309
- Symantec VirtualStore
  - about 21
  - configuring 101
  - installer 67
  - solution 21

**T**

- tunables file
  - about setting parameters 385
  - parameter definitions 390
  - preparing 389
  - setting for configuration 386
  - setting for installation 386
  - setting for upgrade 386
  - setting parameters 389
  - setting with no other operations 387
  - setting with un-integrated response file 388

**U**

- unregistering
  - VirtualStore cluster 302
- unsuccessful upgrade 288
- upgrading
  - rolling 273
- upgrading VVR
  - from 4.1 245
  - planning 244
  - preparing 250
- Useful links
  - VMware 303

## Using

- VirtualStore Plug-in for VMware vSphere 307

**V**

## vCenter Server

- connecting to Citrix XenDesktop 318

## verifying

- virtual machine clones 316

- VirtualStore cluster 301

## virtual machine clones

- adding to Citrix XenDesktop 317

- specifying where to create 311

- verifying 316

## virtual machine customization

- pre-requisites 301

## VirtualStore

- VMware Vsphere environment 21

## VirtualStore cluster

- registering 300

- unregistering 302

- verifying 301

## VirtualStore Plug-in for VMware vSphere

- using 307

## VirtualStore vSphere Service Console

- configure 299

## VirtualStore Web Server for cluster failover

- configure 299

## VMotion 22

## VMware 21

- useful links 303

## VMware vCenter Servers

- registered 303

## VMware View

- configuring 315

## VMware View Integration

- pre-requisites 302

## Volume Manager

- Fibre Channel 51

## vradmin

- delpri 377

- stoprep 377

## VVR 4.1

- planning an upgrade from 245

## vxdisksetup command 123

## vxlincst command 121

## vxlcrep command 120

**W**

- Web-based installer 175