

Symantec™ VirtualStore Installation and Configuration Guide

Solaris

5.1 Service Pack 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: 5.1 SP1

Document version: 5.1SP1.1

Legal Notice

Copyright © 2010 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	supportsolutions@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 website.

<http://www.symantec.com/business/support/overview.jsp?pid=15107>

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:

docs@symantec.com

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	11
Chapter 1 Symantec VirtualStore	13
About Symantec VirtualStore	13
About Symantec VirtualStore solution for VMware environment	13
Chapter 2 Before you install	15
About planning for SVS installation	15
About installation and configuration methods	16
Assessing system preparedness	17
Symantec Operations Readiness Tools	18
Prechecking your systems using the Veritas installer	18
Downloading the Symantec VirtualStore software	19
Setting environment variables	20
Optimizing LLT media speed settings on private NICs	20
Guidelines for setting the media speed of the LLT interconnects	20
Creating the /opt directory	21
About configuring ssh or rsh using the Veritas installer	21
Setting up shared storage	22
Setting up shared storage: SCSI disks	22
Setting up shared storage: Fibre Channel	25
Cluster environment requirements for Sun Clusters	26
Prerequisites for Symantec VirtualStore	26
Hardware overview and requirements for Symantec VirtualStore	27
Shared storage	28
Fibre Channel switch	28
Cluster platforms	29

Chapter 3	System requirements	31
	Release notes	31
	Hardware compatibility list (HCL)	32
	I/O fencing requirements	32
	Coordinator disk requirements for I/O fencing	32
	CP server requirements	33
	Veritas File System requirements	36
	Supported Solaris operating systems	36
	Supported VMware software version	37
	Supported Guest operating system for Guest operating system customization while cloning	37
	Disk space requirements	37
	Number of nodes supported	38
Chapter 4	Licensing Veritas products	39
	About Veritas product licensing	39
	Setting or changing the product level for keyless licensing	40
	Installing Veritas product license keys	42
Section 2	Installation of Symantec VirtualStore	43
Chapter 5	Installing Symantec VirtualStore	45
	Installing Symantec VirtualStore using the installer	45
	Installing SVS with the Web-based installer	48
Section 3	Configuration of Symantec VirtualStore	51
Chapter 6	Preparing to configure SVS	53
	Preparing to configure the clusters in secure mode	53
	Installing the root broker for the security infrastructure	57
	Creating authentication broker accounts on root broker system	58
	Creating encrypted files for the security infrastructure	59
	Preparing the installation system for the security infrastructure	61
	About configuring SVS clusters for data integrity	62
	About I/O fencing components	63
	About data disks	63

About coordination points	63
About preferred fencing	65
About I/O fencing configuration files	65
About planning to configure I/O fencing	67
Typical SFCFS cluster configuration with server-based I/O fencing	70
Recommended CP server configurations	71
Setting up the CP server	74
Planning your CP server setup	74
Installing the CP server using the installer	75
Configuring the CP server cluster in secure mode	76
Setting up shared storage for the CP server database	77
Configuring the CP server using the configuration utility	78
Configuring the CP server manually	86
Verifying the CP server configuration	87
 Chapter 7	
Configuring Symantec VirtualStore	89
Configuring SVS using the script-based installer	89
Overview of tasks to configure Symantec VirtualStore using the script-based installer	89
Starting the software configuration	90
Specifying systems for configuration	91
Configuring the cluster name and ID	92
Configuring private heartbeat links	92
Configuring the virtual IP of the cluster	95
Configuring the cluster in secure mode	97
Adding VCS users	100
Configuring SMTP email notification	100
Configuring SNMP trap notification	102
Configuring global clusters	104
Completing the VCS configuration	105
Verifying and updating licenses on the system	106
Configuring Symantec VirtualStore using the Web-based installer	108
Database configuration requirements	114
Configuring the SFDB repository database after installation	114
Veritas Volume Replicator and Volume Manager setup after installation	114
 Chapter 8	
Configuring SVS for data integrity	115
Setting up disk-based I/O fencing using installsvs	115
Initializing disks as VxVM disks	115

Configuring disk-based I/O fencing using installsvs	116
Checking shared disks for I/O fencing	118
Setting up disk-based I/O fencing manually	122
Identifying disks to use as coordinator disks	123
Setting up coordinator disk groups	124
Creating I/O fencing configuration files	124
Modifying VCS configuration to use I/O fencing	125
Verifying I/O fencing configuration	127
Setting up server-based I/O fencing using installsvs	128
Verifying the security configuration on the SFCFS cluster to use CP server coordination point	128
Configuring server-based I/O fencing using the installsvs	130
Setting up server-based I/O fencing manually	139
Preparing the CP servers manually for use by the SFCFS cluster	139
Configuring server-based fencing on the SFCFS cluster manually	143
Configuring Coordination Point agent to monitor coordination points	147
Verifying server-based I/O fencing configuration	149
Enabling or disabling the preferred fencing policy	150

Section 4 Setting up Symantec VirtualStore 153

Chapter 9 Setting up Symantec VirtualStore	155
Disabling SMF for NFS daemons on Solaris 10	155
Setting up Clustered NFS	157
Setting up Symantec VirtualStore	158
Useful links from VMware on NFS support and customization while cloning virtual machines	163

Section 5 Creating virtual machine clones using Symantec FileSnap workflow 165

Chapter 10 Creating virtual machine clones using Symantec FileSnap	167
Creating virtual machine clones using Symantec FileSnap	167

Index	175
-------------	-----

Installation overview and planning

- [Chapter 1. Symantec VirtualStore](#)
- [Chapter 2. Before you install](#)
- [Chapter 3. System requirements](#)
- [Chapter 4. Licensing Veritas products](#)

Symantec VirtualStore

This chapter includes the following topics:

- [About Symantec VirtualStore](#)
- [About Symantec VirtualStore solution for VMware environment](#)

About Symantec VirtualStore

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

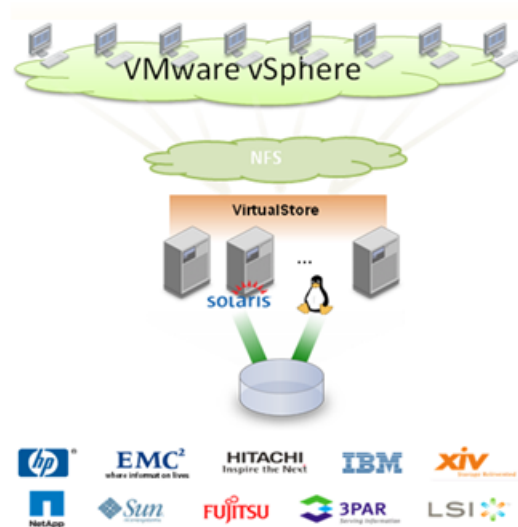
About Symantec VirtualStore solution for VMware environment

Symantec VirtualStore powered by Veritas Storage Foundation Cluster File System 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 SFCFS.

- 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 SFCFS (export same file system through multiple NAS heads, DST, and high availability plus others...).
- Leverage SFCFS 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



Before you install

This chapter includes the following topics:

- [About planning for SVS installation](#)
- [About installation and configuration methods](#)
- [Assessing system preparedness](#)
- [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 configuring ssh or rsh using the Veritas installer](#)
- [Setting up shared storage](#)
- [Cluster environment requirements for Sun Clusters](#)
- [Prerequisites for 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 website.

<http://www.symantec.com/business/support/overview.jsp?pid=15107>

Document version: 5.1SP1.1.

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 one of the Symantec VirtualStore products by Symantec.

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 2-1 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: ■ Common product installer script: <code>installer</code> The common product installer script provides a menu that simplifies the selection of installation and configuration options. Use this method to install other products, such as the Symantec Product Authentication Service (AT), along with SVS. ■ 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 2-1 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.
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>
JumpStart	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.
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 by manually or using interactive method with <code>installsvs</code> or <code>installer</code> script configure the SVS stack

Assessing system preparedness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Symantec VirtualStore 5.1 SP1.

Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a Web-based application that is designed to support Symantec enterprise products.

See “[Symantec Operations Readiness Tools](#)” on page 18.

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 Symantec VirtualStore 5.1 SP1.

See “[Prechecking your systems using the Veritas installer](#)” on page 18.

Symantec Operations Readiness Tools

Symantec™ Operations Readiness Tools (SORT) is a set of Web-based tools that supports Symantec enterprise products. SORT increases operational efficiency and helps improve application availability.

Among its broad set of features, SORT provides patches, patch notifications, and documentation for Symantec enterprise products.

To access SORT, go to:

<http://sort.symantec.com>

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.
- 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, you can use the following link. For other downloads, contact your Veritas representative for more information.

<http://www.symantec.com/business/products/downloads/index.jsp>

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.

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 37.

- 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.

```
# df -b 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 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 configuring ssh or rsh using the Veritas installer

The installer can configure 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.

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 the root broker is outside of the cluster that you plan to configure.
- When you add new nodes to an existing cluster.
- When the nodes are in a sub-cluster during a phased upgrade.
- When you perform installer sessions using a response file.

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 67.

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 `nvrarc` script. The path information varies from system to system.

5 Edit the `nvrarc` 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 `nvrarc` 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.

Cluster environment requirements for Sun Clusters

Use these steps if the configuration is with Sun cluster, which is a set of hosts that share a set of disks.

To configure a cluster

- 1 Obtain a license for the optional VxVM cluster feature for a Sun Cluster from your Oracle Customer Support channel.
- 2 If you plan to encapsulate the root disk group, decide where you want to place it for each node in the cluster. The root disk group, usually aliased as `bootdg`, contains the volumes that are used to boot the system. VxVM sets `bootdg` to the appropriate disk group if it takes control of the root disk. Otherwise `bootdg` is set to `nodg`. To check the name of the disk group, enter the command:

`vxkg bootdg`
- 3 Decide the layout of shared disk groups. There may be one or more shared disk groups. Determine how many you wish to use.
- 4 If you plan to use Dirty Region Logging (DRL) with VxVM in a cluster, leave a small amount of space on the disk for these logs. The log size is proportional to the volume size and the number of nodes. Refer to the *Veritas Volume Manager Administrator's Guide* for more information on DRL.
- 5 Install the license on every node in the cluster.

Prerequisites for 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 the SVS:

- The cluster name, beginning with a letter (a-z, A-Z).

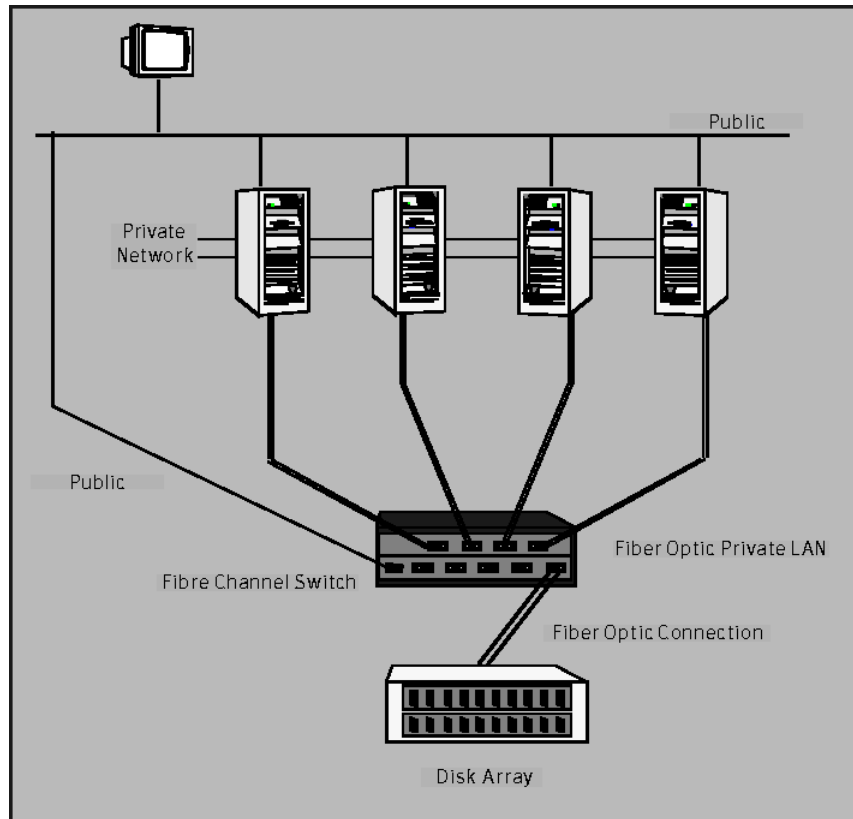
- A unique ID from 0-65535 for the cluster. Within the public subnet, a new cluster using a duplicate cluster ID can cause existing clusters to fail.
- The host names of the cluster nodes.
- The device names of the network interface cards (NICs) used for the private networks among nodes.
- Establishing 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 2-1](#) shows the configuration of a cluster file system on a Fibre Channel fabric with a disk array.

Figure 2-1 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 Storage Foundation Cluster File System (SFCFS) cluster.

See the *Veritas Storage Foundation Cluster File System 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.

System requirements

This chapter includes the following topics:

- [Release notes](#)
- [Hardware compatibility list \(HCL\)](#)
- [I/O fencing requirements](#)
- [Veritas File System requirements](#)
- [Supported Solaris operating systems](#)
- [Supported VMware software version](#)
- [Supported Guest operating system for Guest operating system customization while cloning](#)
- [Disk space requirements](#)
- [Number of nodes supported](#)

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:

<http://www.symantec.com/business/support/overview.jsp?pid=15107>

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://entsupport.symantec.com/docs/330441>

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

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 32.
- CP servers
See “[CP server requirements](#)” on page 33.

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 three 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 5.1SP1 clusters (application clusters) support CP servers which are hosted on the following VCS and SFHA versions:

- VCS 5.1 or 5.1SP1 single-node cluster
CP server requires LLT and GAB to be configured on the single-node VCS cluster that hosts CP server. This requirement also applies to any single-node application cluster that uses server-based fencing.
- SFHA 5.1 or 5.1SP1 cluster

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

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 3-1](#) lists additional requirements for hosting the CP server.

Table 3-1 CP server hardware requirements

Hardware required	Description
Disk space	To host the CP server on a VCS cluster or SFHA cluster, each host requires the following file system space: ■ 550 MB in the /opt directory (additionally, the language pack requires another 15 MB) ■ 300 MB in /usr ■ 20 MB in /var
Storage	When CP server is hosted on an SFHA cluster, there must be shared storage between the CP servers.
RAM	Each CP server requires at least 512 MB.
CP server to client node physical link	A secure TCP/IP connection is required to connect the CP servers to the Symantec VirtualStore clusters (application clusters).

[Table 3-2](#) 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 3-2 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	CP server supports any of the following operating systems: ■ AIX 5.3 and 6.1 ■ HP-UX 11i v3 ■ Linux: ■ RHEL 5 ■ SLES 10 ■ SLES 11 ■ Solaris 9 and 10 Review other details such as supported operating system levels and architecture for the supported operating systems. See the <i>Veritas Cluster Server Installation Guide</i> or the <i>Veritas Storage Foundation High Availability Installation Guide</i>.

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.
- 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 being 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 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 the number of hops between the nodes.

For secure communications between the SFCFS cluster 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.
- The CP server and application clusters should also use the same root broker. If the same root broker is not being used, then trust can be established between the cluster nodes and CP server for the secure communication. Trust can be established by the installer when configuring fencing.
- 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*.

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. 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:

```
# 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
```

If the values shown are less than 6000, 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:

```
set lwp_default_stksize=0x6000
set rpcmod:svc_default_stksize=0x6000
```

Supported Solaris operating systems

This release of the Veritas products is supported on the following Solaris operating systems:

- Solaris 9 (32-bit and 64-bit, SPARC) with Update 7, 8, and 9

Symantec VirtualStore is only supported on Solaris 9 (SPARC Platform 64-bit).

Note: In the next major release Veritas products no longer support Solaris 9.

- Solaris 10 (64-bit, SPARC or x86_64) with Update 6, 7, and 8
Symantec VirtualStore is only supported on Solaris 10 (SPARC or X86 Platform 64-bit).
- Solaris 10 (SPARC and x86_64) with Update 9 requires VRTSvxvm patch 142629-08 and 142630-08

For the most up-to-date list of operating system patches, refer to the Release Notes for your product.

For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:

<http://entsupport.symantec.com/docs/334829>

Supported VMware software version

VMware vSphere 4 (ESX 4.0 Update 1 and later with vCenter Server 4.0 Update 1 and later)

Supported Guest operating system for Guest operating system customization while cloning

- Windows 7
- Windows 2003 (32 and 64 bit)
- Windows XP (64 bit)
- RHEL 5
- SLES 10 and 11

Disk space requirements

Before installing any of the Veritas Storage Foundation products, confirm that your system has enough free disk space.

Use the "Perform a Preinstallation Check" (P) menu or the `-precheck` option of the product installer to determine whether there is sufficient space.

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

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

```
# ./installsvs -precheck
```

Number of nodes supported

SVS supports cluster configurations with up to 64 nodes.

For more updates on this support, see the Late-Breaking News TechNote on the Symantec Technical Support website:

<http://entsupport.symantec.com/docs/334829>

Licensing Veritas products

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 or continue with keyless licensing by managing the server or cluster with a management server. If you do not comply with the above terms, continuing to use the Veritas 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 product installer does not change the license keys that are already installed. 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 40.
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 42.
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. In order to use keyless licensing, you must set up a Management Server to manage your systems.

For more information 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 View the current setting for the product level.

```
# vxkeyless -v display
```

- 2 View the possible settings for the product level.

```
# vxkeyless displayall
```

- 3 Set the desired product level.

```
# vxkeyless -q set prod_levels
```

where *prod_levels* is a comma-separated list of keywords, as shown in step 2

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 xxxx-xxxx-xxxx-xxxx-xxxx-xxx
```

Installation of Symantec VirtualStore

- [Chapter 5. Installing Symantec VirtualStore](#)

Installing Symantec VirtualStore

This chapter includes the following topics:

- [Installing Symantec VirtualStore using the installer](#)
- [Installing SVS with the Web-based installer](#)

Installing Symantec VirtualStore using the installer

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

See [“Supported Solaris operating systems”](#) on page 36.

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.

- 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:

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 and install the SDK after the installer completes.

```
# ./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_VirtualStore_Ux_5.1SP1.pdf file present
on media? [y,n,q,?] y
```

- 8 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.
- 9 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.

- 10 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.

- 11 After the system checks complete, the installer displays a list of the patches and packages that will be installed. Press Enter to continue with the installation.
- 12 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 14.

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.

- 13 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**

- 14 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-****
```

- 15 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
```

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 ?.
- 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.

- 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 Indicate the systems where you want to install. Separate multiple system names with spaces. Click **Validate**.
- 7 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.
- 8 After the validation completes successfully, click **Next** to install SVS on the selected system.

- 9 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.

- 10 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 prompts you for another task.

Configuration of Symantec VirtualStore

- [Chapter 6. Preparing to configure SVS](#)
- [Chapter 7. Configuring Symantec VirtualStore](#)
- [Chapter 8. Configuring SVS for data integrity](#)

Preparing to configure SVS

This chapter includes the following topics:

- [Preparing to configure the clusters in secure mode](#)
- [About configuring SVS clusters for data integrity](#)
- [About I/O fencing components](#)
- [About I/O fencing configuration files](#)
- [About planning to configure I/O fencing](#)
- [Setting up the CP server](#)

Preparing to configure the clusters in secure mode

You can set up Symantec Product Authentication Service (AT) for the cluster during or after the Symantec VirtualStore configuration.

In a cluster that is online, if you want to enable or disable AT using the `installsvs -security` command, see the *Veritas Cluster Server Administrator's Guide* for instructions.

The prerequisites to configure a cluster in secure mode are as follows:

- A system in your enterprise that serves as root broker (RB).
You can either use an external system as root broker, or use one of the cluster nodes as root broker.
 - To use an external root broker, identify an existing root broker system in your enterprise or install and configure root broker on a stable system. See [“Installing the root broker for the security infrastructure”](#) on page 57.
 - To use one of the cluster nodes as root broker, the installer does not require you to do any preparatory tasks.

When you configure the cluster in secure mode using the script-based installer, choose the automatic mode and choose one of the nodes for the installer to configure as root broker.

Symantec recommends that you configure a single root broker system for your entire enterprise. If you use different root broker systems, then you must establish trust between the root brokers. For example, if the management server and the cluster use different root brokers, then you must establish trust.

- For external root broker, an authentication broker (AB) account for each node in the cluster is set up on the root broker system.
See [“Creating authentication broker accounts on root broker system”](#) on page 58.
- The system clocks of the external root broker and authentication brokers must be in sync.

The script-based installer provides the following configuration modes:

Automatic mode	The external root broker system must allow rsh or ssh passwordless login to use this mode.
Semi-automatic mode	This mode requires encrypted files (BLOB files) from the AT administrator to configure a cluster in secure mode. The nodes in the cluster must allow rsh or ssh passwordless login.
Manual mode	This mode requires root_hash file and the root broker information from the AT administrator to configure a cluster in secure mode. The nodes in the cluster must allow rsh or ssh passwordless login.

[Figure 6-1](#) depicts the flow of configuring Symantec VirtualStore cluster in secure mode.

Figure 6-1 Workflow to configure Symantec VirtualStore cluster in secure mode

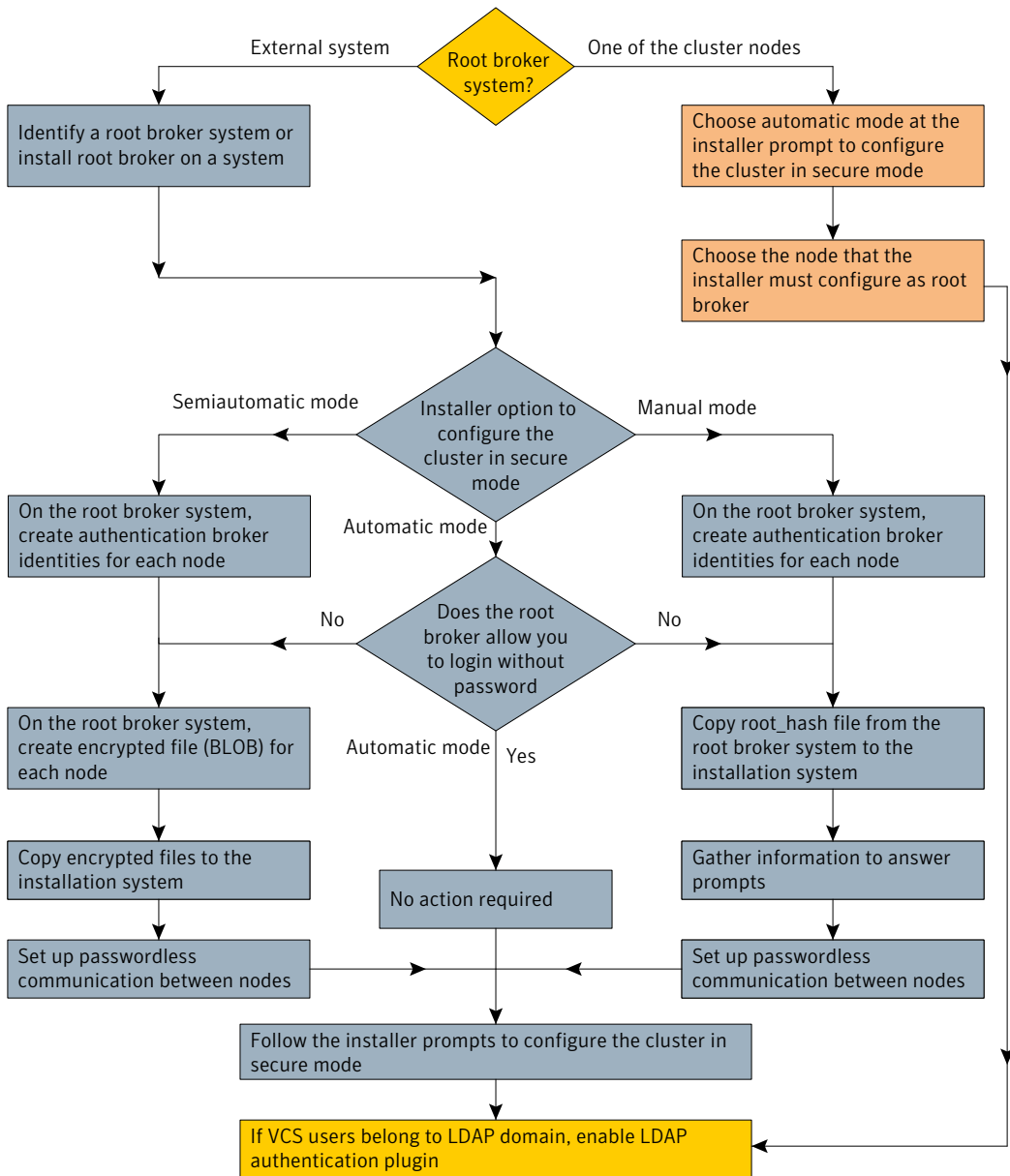


Table 6-1 lists the preparatory tasks in the order which the AT and VCS administrators must perform. These preparatory tasks apply only when you use an external root broker system for the cluster.

Table 6-1 Preparatory tasks to configure a cluster in secure mode (with an external root broker)

Tasks	Who performs this task
Decide one of the following configuration modes to set up a cluster in secure mode: ■ Automatic mode ■ Semi-automatic mode ■ Manual mode	VCS administrator
Install the root broker on a stable system in the enterprise. See “Installing the root broker for the security infrastructure” on page 57.	AT administrator
To use the semi-automatic mode or the manual mode, on the root broker system, create authentication broker accounts for each node in the cluster. See “Creating authentication broker accounts on root broker system” on page 58. AT administrator requires the following information from the VCS administrator: ■ Node names that are designated to serve as authentication brokers ■ Password for each authentication broker	AT administrator
To use the semi-automatic mode, create the encrypted files (BLOB files) for each node and provide the files to the VCS administrator. See “Creating encrypted files for the security infrastructure” on page 59. AT administrator requires the following additional information from the VCS administrator: ■ Administrator password for each authentication broker Typically, the password is the same for all nodes.	AT administrator
To use the manual mode, provide the root_hash file (/opt/VRTSat/bin/root_hash) from the root broker system to the VCS administrator.	AT administrator

Table 6-1 Preparatory tasks to configure a cluster in secure mode (with an external root broker) (*continued*)

Tasks	Who performs this task
Copy the files that are required to configure a cluster in secure mode to the system from where you plan to install and configure Symantec VirtualStore. See “Preparing the installation system for the security infrastructure” on page 61.	VCS administrator

Installing the root broker for the security infrastructure

Install the root broker only if you plan to use AT to configure the cluster in secure mode. You can use a system outside the cluster or one of the systems within the cluster as root broker. If you plan to use an external broker, the root broker administrator must install and configure the root broker before you configure the Authentication Service for Symantec VirtualStore. Symantec recommends that you install the root broker on a stable system that is outside the cluster.

You can also identify an existing root broker system in the data center to configure the cluster in secure mode. The root broker system can run AIX, HP-UX, Linux, or Solaris operating system.

See Symantec Product Authentication Service documentation for more information.

To install the root broker

- 1 Mount the product disc and start the installer.


```
# ./installer
```
- 2 From the Task Menu, choose I for "Install a Product."
- 3 From the displayed list of products to install, choose: Symantec Product Authentication Service (AT).
- 4 Enter **y** to agree to the End User License Agreement (EULA).
- 5 Enter **2** to install the recommended packages.
- 6 Enter the name of the system where you want to install the Root Broker.


```
Enter the operating_system system names separated by space [q,?]: venus
```
- 7 Review the output as the installer does the following:

- Checks to make sure that AT supports the operating system
- Verifies that you install from the global zone
- Checks if the packages are already on the system.

The installer lists the packages that the program is about to install on the system. Press Enter to continue.

- 8 Review the output as the installer installs the root broker on the system.
- 9 After the installation, configure the root broker.
- 10 Select to configure the root broker from the three choices that the installer presents:

```
1)Root+AB Mode
2)Root Mode
3)AB Mode
```

```
Enter the mode in which you would like AT to be configured? [1-3,q] 2
```

```
All AT processes that are currently running must be stopped
```

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

- 11 Press Enter to continue and review the output as the installer starts the Authentication Service.

Creating authentication broker accounts on root broker system

On the root broker system, the administrator must create an authentication broker (AB) account for each node in the cluster.

To create authentication broker accounts on root broker system

- 1 Determine the root broker domain name. Enter the following command on the root broker system:

```
venus> # vssat showalltrustedcreds
```

For example, the domain name resembles "Domain Name: root@venus.symantecexample.com" in the output.

- 2 For each node in the cluster, verify whether an account exists on the root broker system.

For example, to verify that an account exists for node galaxy:

```
venus> # vssat showprpl --pdrtype root \  
--domain root@venus.symantecexample.com --prplname galaxy
```

- If the output displays the principal account on root broker for the authentication broker on the node, then delete the existing principal accounts. For example:

```
venus> # vssat deleteprpl --pdrtype root \  
--domain root@venus.symantecexample.com \  
--prplname galaxy --silent
```

- If the output displays the following error, then the account for the given authentication broker is not created on this root broker:

```
"Failed To Get Attributes For Principal"
```

Proceed to step 3.

- 3 Create a principal account for each authentication broker in the cluster. For example:

```
venus> # vssat addprpl --pdrtype root --domain \  
root@venus.symantecexample.com --prplname galaxy \  
--password password --prpltype service
```

You must use this password that you create in the input file for the encrypted file.

Creating encrypted files for the security infrastructure

Create encrypted files (BLOB files) only if you plan to choose the semiautomatic mode that uses an encrypted file to configure the Authentication Service. The administrator must create the encrypted files on the root broker node. The administrator must create encrypted files for each node that is going to be a part of the cluster before you configure the Authentication Service for SVS.

To create encrypted files

- 1 Make a note of the following root broker information. This information is required for the input file for the encrypted file:

hash	The value of the root hash string, which consists of 40 characters. Execute the following command to find this value:
------	---

```
venus> # vssat showbrokerhash
```

root_domain The value for the domain name of the root broker system. Execute the following command to find this value:

```
venus> # vssat showalltrustedcreds
```

- 2 Make a note of the following authentication broker information for each node. This information is required for the input file for the encrypted file:

identity The value for the authentication broker identity, which you provided to create authentication broker principal on the root broker system.

This is the value for the **--prplname** option of the **addprpl** command.

See [“Creating authentication broker accounts on root broker system”](#) on page 58.

password The value for the authentication broker password, which you provided to create authentication broker principal on the root broker system.

This is the value for the **--password** option of the **addprpl** command.

See [“Creating authentication broker accounts on root broker system”](#) on page 58.

- 3 For each node in the cluster, create the input file for the encrypted file.

The installer presents the format of the input file for the encrypted file when you proceed to configure the Authentication Service using encrypted file. For example, the input file for authentication broker on galaxy resembles:

```
[setuptrust]
broker=venus.symantecexample.com
hash=758a33dbd6fae751630058ace3dedb54e562fe98
securitylevel=high
```

```
[configab]
identity=galaxy
password=password
root_domain=root@venus.symantecexample.com
root_broker=venus.symantecexample.com:2821
```

```
start_broker=false
enable_pbx=false
```

- 4 Back up these input files that you created for the authentication broker on each node in the cluster.

Note that for security purposes, the command to create the output file for the encrypted file deletes the input file.

- 5 For each node in the cluster, create the output file for the encrypted file from the root broker system using the following command.

```
RootBroker> # vssat createpkg \
--in /path/to/blob/input/file.txt \
--out /path/to/encrypted/blob/file.txt \
--host_ctx AB-hostname
```

For example:

```
venus> # vssat createpkg --in /tmp/galaxy.blob.in \
--out /tmp/galaxy.blob.out --host_ctx galaxy
```

Note that this command creates an encrypted file even if you provide wrong password for "password=" entry. But such an encrypted file with wrong password fails to install on authentication broker node.

- 6 After you complete creating the output files for the encrypted file, you must copy these encrypted BLOB files for each node in the cluster.

Preparing the installation system for the security infrastructure

The VCS administrator must gather the required information and prepare the installation system to configure a cluster in secure mode.

To prepare the installation system for the security infrastructure

- ◆ Depending on the configuration mode you decided to use, do one of the following:

Automatic mode Do the following:

- Gather the root broker system name from the AT administrator.
- During SVS configuration, choose the configuration option 1 when the installsvs prompts.

Semi-automatic mode	Do the following: ■ Copy the encrypted files (BLOB files) to the system from where you plan to install VCS. Note the path of these files that you copied to the installation system. ■ During SVS configuration, choose the configuration option 2 when the installsvs prompts.
Manual mode	Do the following: ■ Copy the root_hash file that you fetched to the system from where you plan to install VCS. Note the path of the root hash file that you copied to the installation system. ■ Gather the root broker information such as name, fully qualified domain name, domain, and port from the AT administrator. ■ Note the principal name and password information for each authentication broker that you provided to the AT administrator to create the authentication broker accounts. ■ During SVS configuration, choose the configuration option 3 when the installsvs prompts.

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 67.

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 63.
- Coordination points—Act as a global lock during membership changes
See [“About coordination points”](#) on page 63.

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. Racing for control of the coordination points to fence data disks is the key to understand how fencing prevents split-brain.

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 Volume Manager 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 SFCFS cluster nodes to perform the following tasks:

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

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

- 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 150.

About I/O fencing configuration files

[Table 6-2](#) lists the I/O fencing configuration files.

Table 6-2 I/O fencing configuration files

File	Description
/etc/default/vxfen	This file stores the start and stop environment variables for I/O fencing: ■ VXFEN_START—Defines the startup behavior for the I/O fencing module after a system reboot. Valid values include: 1—Indicates that I/O fencing is enabled to start up. 0—Indicates that I/O fencing is disabled to start up. ■ VXFEN_STOP—Defines the shutdown behavior for the I/O fencing module during a system shutdown. Valid values include: 1—Indicates that I/O fencing is enabled to shut down. 0—Indicates that I/O fencing is disabled to shut down. The installer sets the value of these variables to 1 at the end of Symantec VirtualStore configuration.
/etc/vxfendg	This file includes the coordinator disk group information. This file is not applicable for server-based fencing.

Table 6-2 I/O fencing configuration files (continued)

File	Description
/etc/vxfenmode	This file contains the following parameters: ■ vxfen_mode ■ scsi3—For disk-based fencing ■ customized—For server-based fencing ■ disabled—To run the I/O fencing driver but not do any fencing operations. ■ vxfen_mechanism This parameter is applicable only for server-based fencing. Set the value as cps. ■ scsi3_disk_policy ■ dmp—Configure the vxfen module to use DMP devices The disk policy is dmp by default. If you use iSCSI devices, you must set the disk policy as dmp. ■ raw—Configure the vxfen module to use the underlying raw character devices Note: You must use the same SCSI-3 disk policy on all the nodes. ■ security This parameter is applicable only for server-based fencing. 1—Indicates that Symantec Product Authentication Service is used for CP server communications. This setting is the default. 0—Indicates that communication with the CP server is in non-secure mode. Note: The CP server and the Symantec VirtualStore clusters must have the same security setting. ■ List of coordination points This list is required only for server-based fencing configuration. Coordination points in a server-based fencing can include coordinator disks, CP servers, or a mix of both. If you use coordinator disks, you must create a coordinator disk group with the coordinator disk names. Refer to the sample file /etc/vxfen.d/vxfenmode_cps for more information on how to specify the coordination points. ■ single_cp This parameter is applicable only for server-based fencing which uses a single highly available CP server as its coordination point.

Table 6-2 I/O fencing configuration files (continued)

File	Description
/etc/vxfentab	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. Note: The /etc/vxfentab file is a generated file; do not modify this file. For disk-based I/O fencing, the /etc/vxfentab file on each node contains a list of all paths to each coordinator disk. An example of the /etc/vxfentab file in a disk-based fencing configuration on one node resembles as follows: ■ Raw disk: <pre>/dev/rdisk/c1t1d0s2 /dev/rdisk/c2t1d0s2 /dev/rdisk/c3t1d2s2</pre> ■ DMP disk: <pre>/dev/vx/rdmp/c1t1d0s2 /dev/vx/rdmp/c2t1d0s2 /dev/vx/rdmp/c3t1d0s2</pre> For server-based fencing, the /etc/vxfentab file also includes the security settings information. For server-based fencing with single CP server, the /etc/vxfentab file also includes the single_cp settings information.

About planning to configure I/O fencing

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

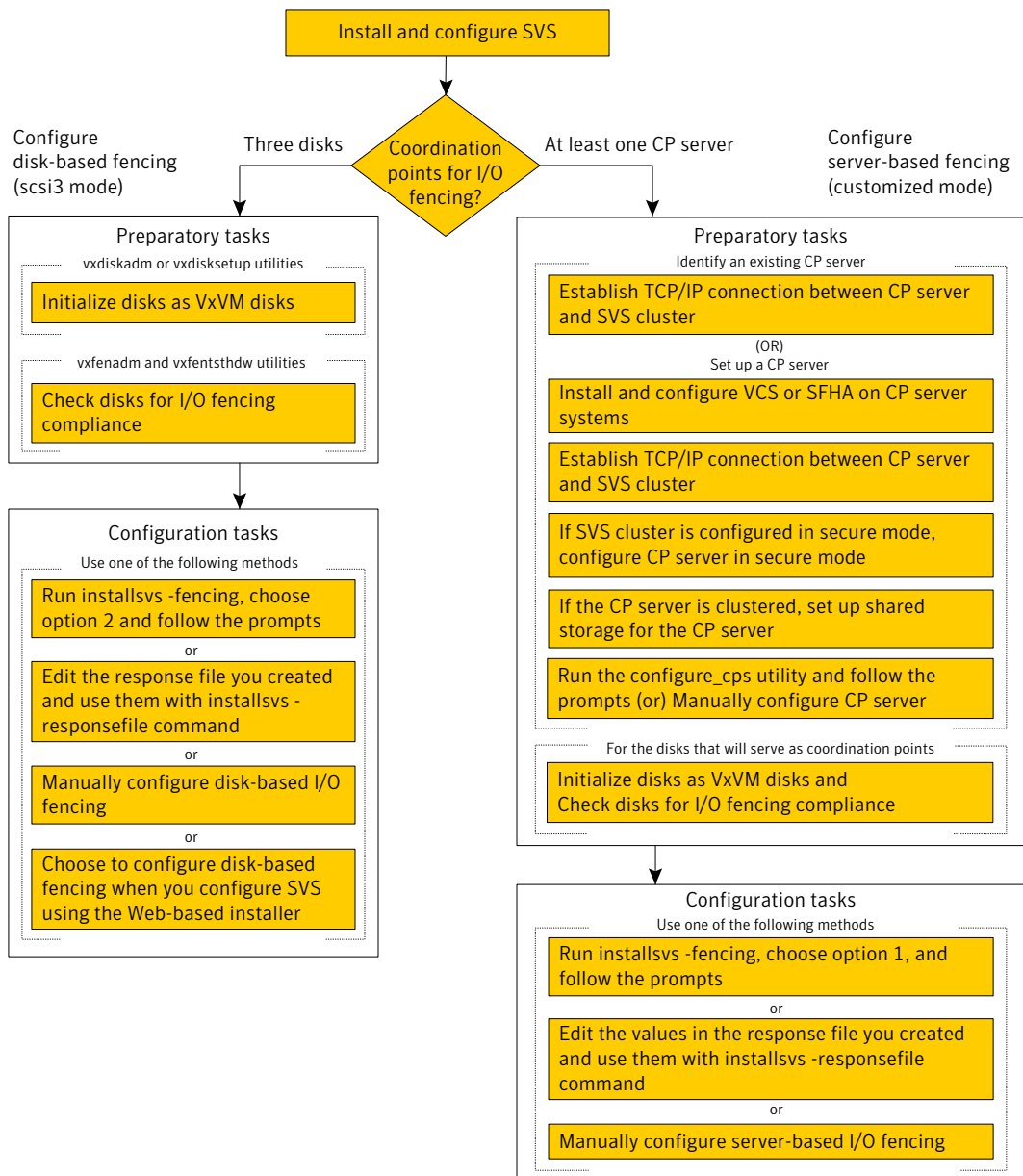
You can configure either disk-based I/O fencing or server-based I/O fencing. If your enterprise setup has multiple clusters that use VCS for clustering, Symantec recommends you to configure server-based I/O fencing.

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 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.

[Figure 6-2](#) illustrates a high-level flowchart to configure I/O fencing for the Symantec VirtualStore cluster.

Figure 6-2 Workflow to configure I/O fencing



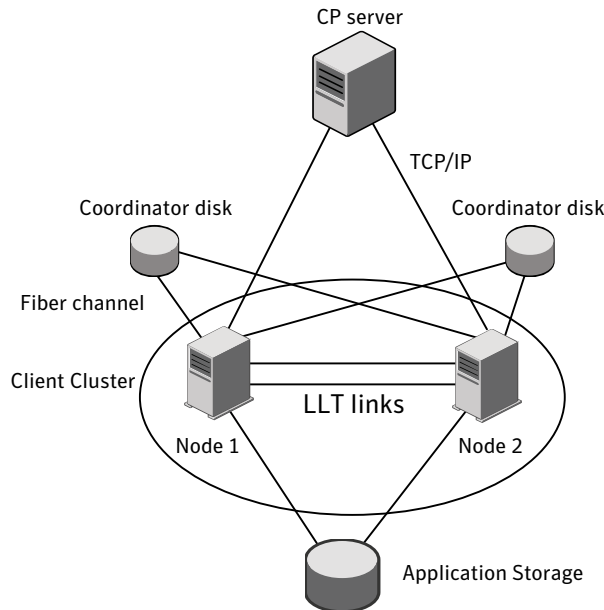
After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:

Using the installsvs	See “Setting up disk-based I/O fencing using installsvs” on page 115. See “Setting up server-based I/O fencing using installsvs” on page 128.
Using the Web-based installer	See “Configuring Symantec VirtualStore using the Web-based installer” on page 108. Note: The Web-based installer supports only the disk-based fencing configuration.
Using response files	
Manually editing configuration files	See “Setting up disk-based I/O fencing manually” on page 122. See “Setting up server-based I/O fencing manually” on page 139.

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

[Figure 6-3](#) displays a configuration using a SFCFS cluster (with two nodes), a single CP server, and two coordinator disks. The nodes within the SFCFS cluster are connected to and communicate with each other using LLT links.

Figure 6-3 CP server, SFCFS 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 6-4](#) on page 72.
- Multiple application clusters use a single CP server and multiple pairs of coordinator disks (two) as their coordination points
See [Figure 6-5](#) on page 73.
- 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 6-6](#) on page 73.

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 (must be an odd number) coordination points for I/O fencing. 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 6-4 displays a configuration using three CP servers that are connected to multiple application clusters.

Figure 6-4 Three CP servers connecting to multiple application clusters

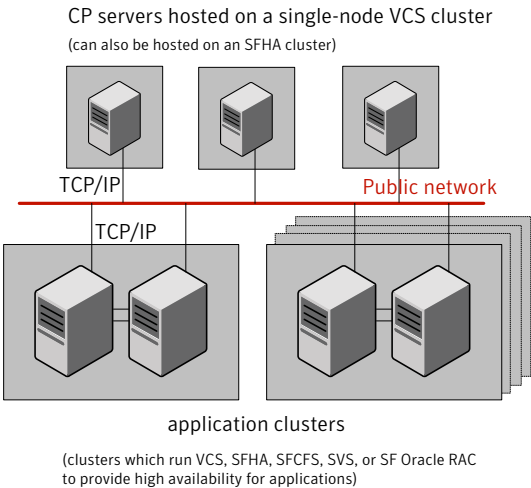


Figure 6-5 displays a configuration using a single CP server that is connected to multiple application clusters with each application cluster also using two coordinator disks.

Figure 6-5 Single CP server with two coordinator disks for each application cluster

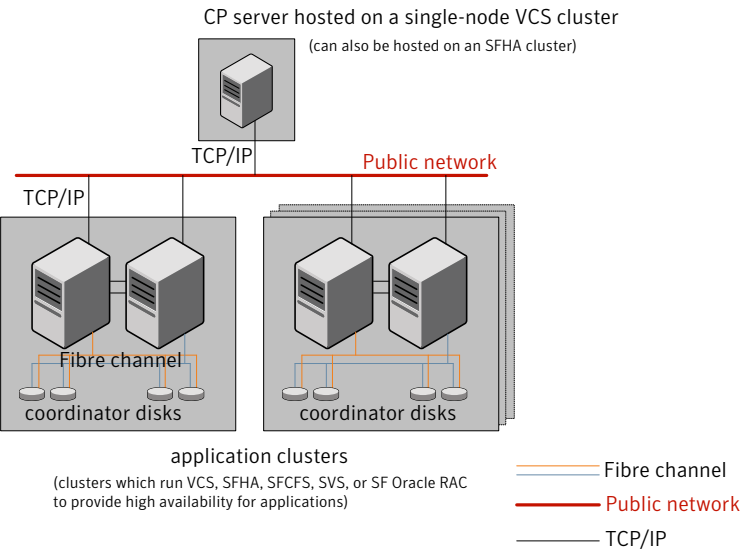
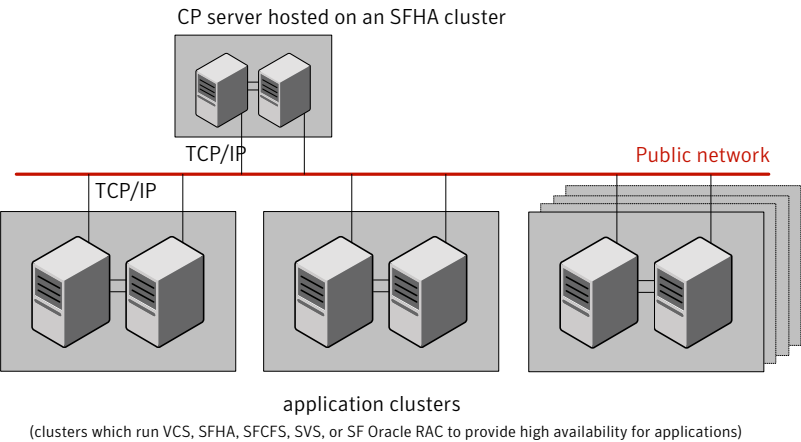


Figure 6-6 displays a configuration using a single CP server that is connected to multiple application clusters.

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



Setting up the CP server

Table 6-3 lists the tasks to set up the CP server for server-based I/O fencing.

Table 6-3 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 74.
Install the CP server	See “Installing the CP server using the installer” on page 75.
Configure the CP server cluster in secure mode	See “Configuring the CP server cluster in secure mode” on page 76.
Set up shared storage for the CP server database	See “Setting up shared storage for the CP server database” on page 77.
Configure the CP server	See “Configuring the CP server using the configuration utility” on page 78. See “Configuring the CP server manually” on page 86.
Verify the CP server configuration	See “Verifying the CP server configuration” on page 87.

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

- 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.
- 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 configure fencing in enabled mode during the SFHA configuration.
 - 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 SFCFS 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 using the Symantec Product Authentication Service (AT).

Symantec recommends configuring the CP server cluster in secure mode. Setting up AT secures the communication between the CP server and its clients (SFCFS clusters). It also secures the HAD communication on the CP server cluster, and makes the authentication broker highly available.
- 4 Set up the hardware and network for your CP server.

See [“CP server requirements”](#) on page 33.
- 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.
 - 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

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

Install and configure VCS to create a single-node VCS cluster.

Meet the following requirements for CP server:

- 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, make sure to configure LLT and GAB.
- During configuration, set up the cluster in secure mode if you want secure communication between the CP server and the SFCFS cluster (application cluster).

See the *Veritas Cluster Server Installation Guide* for instructions on installing and configuring VCS.

Proceed to configure the CP server.

See “[Configuring the CP server using the configuration utility](#)” on page 78.

See “[Configuring the CP server manually](#)” on page 86.

CP server setup uses multiple systems

Install and configure SFHA to create an SFHA cluster. This makes the CP server highly available.

Meet the following requirements for CP server:

- 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, set up the cluster in secure mode if you want secure communication between the CP server and the SFCFS cluster (application cluster).
See “[Preparing to configure the clusters in secure mode](#)” on page 53.
- During configuration, configure disk-based fencing (scsi3 mode).

See the *Veritas Storage Foundation and High Availability Installation Guide* for instructions on installing and configuring SFHA.

Proceed to set up shared storage for the CP server database.

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 SFCFS cluster (CP client).

This step secures the HAD communication on the CP server cluster, and makes the authentication broker highly available.

Note: If you already configured Symantec Product Authentication Service (AT) during 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:

```
# installsvs -security
```

See [“Preparing to configure the clusters in secure mode”](#) on page 53.

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 Import the disk group if it's not already imported.

For example:

```
# vxdg import cps_dg
```

- 3 Create a mirrored volume over the disk group.

For example:

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

- 4 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 configuration utility

The CP server configuration utility (`configure_cps.pl`) is part of the VRTScps package.

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 78.

For CP servers on an SFHA cluster: See [“To configure the CP server on an SFHA cluster”](#) on page 82.

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 CP server configuration script on the node where you want to configure the CP server:

```
# /opt/VRTScps/bin/configure_cps.pl
```

- 3 Enter **1** at the prompt to configure CP server on a single-node VCS cluster.
The configuration utility 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 configuration utility informs the user and requests that the user unconfigure the CP server before trying to configure it.

- 4 Enter the name of the CP server.

```
Enter the name of the CP Server: mycps1.symantecexample.com
```

- 5 Enter a valid virtual IP address on which the CP server process should depend on.

```
Enter a valid Virtual IP address on which  
the CP Server process should depend on:  
10.209.83.85
```

You can also use IPv6 address.

- 6 Enter the CP server port number or press Enter to accept the default value (14250).

```
Enter a port number in range [49152, 65535], or  
press <enter> for default port (14250):
```

- 7 Choose whether the communication between the CP server and the SFCFS 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.

Veritas 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)
(Default:y) :

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

CP Server uses an internal database to store the client information.

Note: As the CP Server is being configured on a single node VCS, the database can reside on local file system.

Enter absolute path of the database (Default:/etc/VRTScps/db):

- 9 Verify and confirm the CP server configuration information.

Following is the CP Server configuration information:

```
-----
(a)CP Server Name: mycps1.symantecexample.com
(b)CP Server Virtual IP: 10.209.83.85
(c)CP Server Port: 14250
(d)CP Server Security : 1
(e)CP Server Database Dir: /etc/VRTScps/db
-----
```

Press b if you want to change the configuration, <enter> to continue :

- 10** The configuration utility 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.
```

```
Configuring CP Server Service Group (CPSSG) for this cluster  
-----
```

```
NOTE: Please ensure that the supplied network interface is a  
public NIC
```

- 11** Enter a valid network interface for the virtual IP address for the CP server process.

```
Enter a valid network interface for virtual IP 10.209.83.85  
on mycps1.symantecexample.com: bge0
```

- 12** Enter networkhosts information for the NIC resource.

```
Symantec recommends configuring NetworkHosts attribute to ensure  
NIC resource to be online always.  
Do you want to add NetworkHosts attribute for the NIC resource bge0 on  
system mycps1? [y/n] : y  
Enter a valid IP address to configure NetworkHosts for NIC bge0 on  
system mycps1 : 10.209.83.86  
Do you want to add another Network Host ?[y/n] : n
```

- 13** Enter the netmask for the virtual IP address. For example:

```
Enter the netmask for virtual IP 10.209.83.85 :  
255.255.252.0
```

- 14** After the configuration process has completed, a success message appears. For example:

```
Successfully added the CPSSG service group to  
VCS configuration. Bringing the CPSSG service  
group online. Please wait...
```

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

- 15** 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      mycps1.symantecexample.com         |ONLINE|
```

It also generates the configuration file for CP server (`/etc/vxcps.conf`).

The configuration utility adds the `vxcpssrv` process and other resources to the VCS configuration in the CP server service group (CPSSG).

For information about the CPSSG, refer to the *Symantec VirtualStore Administrator's Guide*.

In addition, the `main.cf` samples contain details about the `vxcpssrv` resource and its dependencies.

To configure the CP server on an SFHA cluster

- 1** Verify that the VRTScps package is installed on each node.
- 2** Make sure that you have configured passwordless ssh or rsh on the CP server cluster nodes.
- 3** Run the CP server configuration script on the node where you want to configure the CP server:

```
# /opt/VRTScps/bin/configure_cps.pl [-n]
```

The CP server configuration utility uses ssh by default to communicate between systems. Use the `-n` option for rsh communication.

- 4** Enter **2** at the prompt to configure CP server on an SFHA cluster.

The configuration utility 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 configuration utility informs the user and requests that the user unconfigure the CP server before trying to configure it.

5 Enter the name of the CP server.

```
Enter the name of the CP Server: mycps1.symantecexample.com
```

6 Enter a valid virtual IP address on which the CP server process should depend on.

```
Enter a valid Virtual IP address on which  
the CP Server process should depend on:  
10.209.83.85
```

You can also use IPv6 address.

7 Enter the CP server port number or press Enter to accept the default value (14250).

```
Enter a port number in range [49152, 65535], or  
press <enter> for default port (14250):
```

8 Choose whether the communication between the CP server and the SFCFS 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.

Veritas 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)  
(Default:y) :
```

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

CP Server uses an internal database to store the client information.

Note: 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 (Default:/etc/VRTScps/db):

- 10 Verify and confirm the CP server configuration information.

Following is the CP Server configuration information:

```
-----
(a) CP Server Name: mycps1.symantecexample.com
(b) CP Server Virtual IP: 10.209.83.85
(c) CP Server Port: 14250
(d) CP Server Security : 1
(e) CP Server Database Dir: /etc/VRTScps/db
-----
```

Press b if you want to change the configuration, <enter> to continue :

- 11 The configuration utility proceeds with the configuration process, and creates a vxcps.conf configuration file on each node.

The following output is for one node:

```
Successfully generated the /etc/vxcps.conf
configuration file.
Successfully created directory /etc/VRTScps/db.
Creating mount point /etc/VRTScps/db on
mycps1.symantecexample.com.
Copying configuration file /etc/vxcps.conf to
mycps1.symantecexample.com
```

Configuring CP Server Service Group (CPSSG) for this cluster

```
-----
```

12 Confirm whether you use the same NIC name for the virtual IP on all the systems in the cluster.

```
Is the name of NIC for virtual IP 10.209.83.85 same on all the systems?  
[y/n] : y
```

NOTE: Please ensure that the supplied network interface is a public NIC

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

```
Enter a valid interface for virtual IP 10.209.83.85  
on all the systems : bge0
```

14 Enter networkhosts information for the NIC resource.

```
Symantec recommends configuring NetworkHosts attribute to ensure  
NIC resource to be online always.  
Do you want to add NetworkHosts attribute for the NIC resource bge0 on  
system mycps1? [y/n] : y  
Enter a valid IP address to configure NetworkHosts for NIC bge0 on  
system mycps1 : 10.209.83.86  
Do you want to add another Network Host ?[y/n] : n
```

15 Enter the netmask for the virtual IP address.

```
Enter the netmask for virtual IP 10.209.83.85 :  
255.255.252.0
```

16 Enter the name of the disk group for the CP server database.

```
Enter the name of diskgroup for cps database :  
cps_dg
```

17 Enter the name of the volume that is created on the above disk group.

```
Enter the name of volume created on diskgroup cps_dg :  
cps_volume
```

- 18** After the configuration process has completed, a success message appears. For example:

```
Successfully added the CPSSG service group to  
VCS configuration. Bringing the CPSSG service  
group online. Please wait...
```

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

- 19** 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	mycps1.symantecexample.com	ONLINE
CPSSG	State	mycps2.symantecexample.com	OFFLINE

It also generates the configuration file for CP server (`/etc/vxcps.conf`).

The configuration utility adds the `vxcperv` process and other resources to the VCS configuration in the CP server service group (CPSSG).

For information about the CPSSG, refer to the *Symantec VirtualStore Administrator's Guide*.

In addition, the `main.cf` samples contain details about the `vxcperv` resource and its dependencies.

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:

```
# hastop -local
```

- 2** Edit the `main.cf` file to add the CPSSG service group on any node. Use the CPSSG service group in the `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.

```
# hagrps -state CPSSG
```

Output similar to the following appears:

#	Group	Attribute	System	Value
	CPSSG	State	mycps1.symantecexample.com	ONLINE

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/VRTScps/db (default location for CP server database)

- 2 Run the `cpsadm` command to check if the `vxcperv` 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:

- [Configuring SVS using the script-based installer](#)
- [Configuring Symantec VirtualStore using the Web-based installer](#)
- [Database configuration requirements](#)
- [Configuring the SFDB repository database after installation](#)
- [Veritas Volume Replicator and Volume Manager setup after installation](#)

Configuring SVS using the script-based installer

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

[Table 7-1](#) lists the tasks that are involved in configuring Symantec VirtualStore using the script-based installer.

Table 7-1 Tasks to configure Symantec VirtualStore using the script-based installer

Task	Reference
Start the software configuration	See “Starting the software configuration” on page 90.
Specify the systems where you want to configure Symantec VirtualStore	See “Specifying systems for configuration” on page 91.

Table 7-1 Tasks to configure Symantec VirtualStore using the script-based installer *(continued)*

Task	Reference
Configure the basic cluster	See “Configuring the cluster name and ID” on page 92. See “Configuring private heartbeat links” on page 92.
Configure virtual IP address of the cluster (optional)	See “Configuring the virtual IP of the cluster” on page 95.
Configure the cluster in secure mode (optional)	See “Configuring the cluster in secure mode” on page 97.
Add VCS users (required if you did not configure the cluster in secure mode)	See “Adding VCS users” on page 100.
Configure SMTP email notification (optional)	See “Configuring SMTP email notification” on page 100.
Configure SNMP email notification (optional)	See “Configuring SNMP trap notification” on page 102.
Complete the software configuration	See “Completing the VCS configuration” on page 105.

Starting the software configuration

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

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 `hasstop` 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:

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 -configure
```

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,?] (galaxy) galaxy nebula
```

- 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.

- Makes sure that the systems are running with the supported operating system
 - Makes sure the systems install from the global zone
 - Checks whether Symantec VirtualStore is installed
 - Exits if Symantec VirtualStore 5.1 SP1 is not installed
- 3 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 67.

Configuring the cluster name and ID

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 and cluster ID.

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

```
Enter a unique Cluster ID number between 0-65535: [b,q,?] 7
```

Configuring private heartbeat links

You now configure the private heartbeats 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, unless hardware requirements force you to use LLT over UDP. If you want to configure LLT over UDP, make sure you meet the prerequisites.

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: LLT over Ethernet (allow installer to detect)

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.

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. You can use either the standard interfaces or the aggregated interfaces (bonded NICs).

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 NIC on galaxy:
```

```
[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 NIC on galaxy:
```

```
[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 bge0.)

```
Enter the NIC for the first private heartbeat NIC on galaxy:
```

```
[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 NIC on galaxy:
```

```
[b,q,?] e1000g2
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)
```

- 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
NIC on galaxy: [b,q,?] private_NIC1
Do you want to use address 192.168.0.1 for the
first private heartbeat link on galaxy: [y,n,q,b,?] (y)
Enter the UDP port for the first private heartbeat
link on galaxy: [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
NIC on galaxy: [b,q,?] private_NIC2
Do you want to use address 192.168.1.1 for the
second private heartbeat link on galaxy: [y,n,q,b,?] (y)
Enter the UDP port for the second private heartbeat
link on galaxy: [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 galaxy: [b,q,?] (private_NIC0)
Do you want to use address 192.168.3.1 for
the low priority heartbeat link on galaxy: [y,n,q,b,?] (y)
Enter the UDP port for the low priority heartbeat
link on galaxy: [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 galaxy, 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 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 to the Cluster Manager (Java Console) 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 To configure virtual IP, enter **y** at the prompt.
- 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 galaxy: bge0
Enter the NIC for Virtual IP of the Cluster to use on galaxy:
[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)
```

Configuring the cluster in secure mode

If you want to configure the cluster in secure mode, make sure that you meet the prerequisites for secure cluster configuration.

The installer provides different configuration modes to configure a secure cluster. Make sure that you completed the pre-configuration tasks for the configuration mode that you want to choose.

See [“Preparing to configure the clusters in secure mode”](#) on page 53.

To configure the cluster in secure mode

- 1 Choose whether to configure Symantec VirtualStore to use Symantec Product Authentication Service.

```
Would you like to configure VCS to use Symantec Security
Services? [y,n,q] (n) y
```

- If you want to configure the cluster in secure mode, make sure you meet the prerequisites and enter **y**.
- If you do not want to configure the cluster in secure mode, enter **n**. You must add VCS users when the configuration program prompts. See [“Adding VCS users”](#) on page 100.

- 2 Select one of the options to enable security.

Before you choose any of the options, make sure that all the nodes in the cluster can successfully ping the root broker system.

Select the Security option you would like to perform [1-3,b,q,?] (1)

Security Menu

- 1) Configure security completely automatically
- 2) Provide AB credentials using BLOBs
- 3) Provide AB credentials without using BLOBs
- b) Back to previous menu

Review the following configuration modes. Based on the configuration that you want to use, enter one of the following values:

Option 1.
Automatic
configuration

Based on the root broker you want to use, do one of the following:

- To use an external root broker:
Enter the name of the root broker system when prompted.
Requires remote access to the root broker. Make sure that all the nodes in the cluster can successfully ping the root broker system.
Review the output as the installer verifies communication with the root broker system, checks vxatd process and version, and checks security domain.
- To configure one of the nodes as root broker:
■ Press Enter at the following installer prompt:

If you already have an external
RB (Root Broker) installed and configured, enter
the RB name, or press Enter to skip: [b]

- Choose the node that the installer must configure as root and authentication broker. The installer configures the other nodes as authentication brokers.
At the installer prompt, you can choose the first node in the cluster to configure as RAB, or you can enter n to configure another node as RAB. For example:

Do you want to configure <galaxy> as RAB,
and other nodes as AB? [y,n,q,b] (y) **n**
Enter the node name which you want to
configure as RAB: nebula

Option 2.
Semiautomatic
configuration

Enter the path of the encrypted file (BLOB file) for each node when prompted.

Option 3.
 Manual
 configuration

Enter the following Root Broker information as the installer prompts you:

```
Enter root broker name: [b]
east.symantecexample.com
Enter root broker FQDN: [b]
(symantecexample.com)
symantecexample.com
Enter the root broker domain name for the
Authentication Broker's identity: [b]
root@east.symantecexample.com
Enter root broker port: [b] 2821
Enter path to the locally accessible root hash [b]
(/var/tmp/installvcs-200910221810ROA/root_hash)
/var/tmp/installvcs-200910221810ROA/root_hash
```

Enter the following Authentication Broker information as the installer prompts you for each node:

```
Enter Authentication broker's identity on
galaxy [b]
(galaxy.symantecexample.com)
galaxy.symantecexample.com
Enter the password for the Authentication broker's
identity on galaxy:
Enter Authentication broker's identity on
nebula [b]
(nebula.symantecexample.com)
nebula.symantecexample.com
Enter the password for the Authentication broker's
identity on nebula:
```

- 3 After you provide the required information to configure the cluster in secure mode, the program prompts you to configure SMTP email notification.

Note that the installer does not prompt you to add VCS users if you configured the cluster in secure mode. However, you must add VCS users later.

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

Adding VCS users

If you have enabled Symantec Product Authentication Service, 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 want to set the username and/or password for the Admin user
(default username = 'admin', password='password')? [y,n,q] (n) y
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 102.

- 3 Provide information to configure SMTP notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on galaxy: bge0
Enter the NIC for the VCS Notifier to use on galaxy:
[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 104.

- 3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on galaxy: bge0
Enter the NIC for the VCS Notifier to use on galaxy:
[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,?] saturn
```

- **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 saturn [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,?] jupiter
Enter the minimum severity of events for which SNMP traps
should be sent to jupiter [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: saturn receives SNMP traps for Error or  
higher events
```

```
Console: jupiter 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: 192.168.1.16
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 VCS configuration

After you enter the Symantec VirtualStore configuration information, the installer prompts to stop the VCS 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 VCS, it restarts Symantec VirtualStore and its related processes.

If you chose to configure the cluster in secure mode, the installer then does the following before it starts Symantec VirtualStore in secure mode:

- Depending on the security mode you chose to set up Authentication Service, the installer does one of the following:
 - Creates the security principal

- Executes the encrypted file to create security principal on each node in the cluster
- Creates the VxSS service group
- Creates the Authentication Server credentials on each node in the cluster
- Creates the Web credentials for Symantec VirtualStore users
- Sets up trust with the root broker

To complete the VCS configuration

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

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

- 2 Review the output as the installer stops various processes and performs the configuration. The installer then restarts Symantec VirtualStore 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.

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 107.

See [“Updating product licenses using vxlicinst”](#) on page 107.

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 using `vxlicinst`

You can use the `vxlicinst` command 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 107.

To update product licenses

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

```
# vxlicinst -k XXXX-XXXX-XXXX-XXXX-XXXX-XXX
```

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:

```
# hstop -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 XXXX-XXXX-XXXX-XXXX-XXXX-XXX
```

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

```
# vxlicrep
```

- 5 Start Symantec VirtualStore on each node:

```
# hstart
```

Configuring Symantec VirtualStore using the Web-based installer

Before you begin to configure Symantec VirtualStore using the Web-based installer, review the configuration requirements.

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.

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.

Note: If you want to configure server-based I/O fencing, you must either use the script-based installer or manually configure.

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.

- 2 On the Select a task and a product page, select the task and the product as follows:

Task	Configure a Product
Product	

Click **Next**.

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

Example: **galaxy nebula**

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 In the Confirmation dialog box that appears, choose whether or not to configure I/O fencing.

To configure disk-based I/O fencing, click **Yes**.

If you want to configure server-based I/O fencing, or if you decide to configure I/O fencing later, click **No**. You can either use the `installsvs -fencing` command or manually configure.

- 5 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.
LLT Type	Select an LLT type from the list. You can choose to configure LLT over UDP or over Ethernet. If you choose Auto detect over Ethernet, the installer auto-detects the LLT links over Ethernet. Verify the links and click Yes in the Confirmation dialog box. Skip to step 7. If you click No, you must manually enter the details to configure LLT over Ethernet.
Number of Heartbeats	Choose the number of heartbeat links you want to configure.
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**.

- 6 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**.

- 7 In the Confirmation dialog box that appears, choose whether or not to configure the cluster in secure mode using Symantec Product Authentication Service (AT).

To configure the cluster in secure mode, click **Yes**.

If you want to perform this task later, click **No**. You can use the `installsvs -security` command. Go to step 9.

- 8 On the Security Options page, choose an option to enable security and specify the required information.

Do not configure security services	Choose this option if you do not want to enable security. The installer takes you to the next page to configure optional features of Symantec VirtualStore.
Configure security automatically	Choose this option to use an external root broker. Enter the name of the root broker that is already configured for your enterprise environment, and click Validate. The installer configures the cluster in secure mode.
Configure one node as RAB and the others as AB	Select the system that you want to configure as RAB node. The installer configures the cluster in secure mode.

Click **Next**.

- 9 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:

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. ■ 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**.

- 10** On the Stop Processes page, click **Next** after the installer stops all the processes successfully.

- 11 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 4, then skip to step 14. Go to step 12 to configure fencing.

- 12 On the Select Fencing Type page, specify the following information:

Configure disk based fencing	Choose the Configure disk based fencing option.
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 mechanism for the disk group. Go to step 14. ■ 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. Go to step 13.

- 13 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 Mechanism	Choose the fencing mechanism for the disk group.

- 14 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.
- 15 Select the checkbox to specify whether you want to send your installation information to Symantec. Click **Finish**. The installer prompts you for another task.

Database configuration requirements

Most relational database management system (RDBMS) software requires operating system parameters to be set prior to operation. The DB2, Oracle, and Sybase databases require modifications to kernel settings in the `/etc/system` file in Solaris 9 before the databases will run correctly. In Solaris 10, system parameters are managed through the Resource Controls facility. The most critical settings are normally located in the Shared Memory and Semaphore settings on Solaris. For precise settings, consult your current database installation and configuration documentation.

Configuring the SFDB repository database after installation

If you want to use the Storage Foundation Database (SFDB) tools, you must set up the SFDB repository after installing and configuring SVS and Oracle. For SFDB repository set up procedures:

See *Veritas Storage Foundation: Storage and Availability Management for Oracle Databases*

Veritas Volume Replicator and Volume Manager setup after installation

VVR is fully integrated with Veritas Volume Manager (VxVM). Before using VVR, you must have the VxVM volumes set up and initialized.

Refer to the Volume Manager documentation for more information.

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 server-based I/O fencing 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:


```
# devfsadm
```
- 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 Volume Manager 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 -fencing
```

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 5.1 SP1 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 [1-3,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.
 - 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 118.
- 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 fencing mechanism name (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.
 - 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 to monitor the coordinator disks.
See [“Configuring Coordination Point agent to monitor coordination points”](#) on page 147.

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 `vxfststhdw` 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 `vxfststhdw` 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 119.

- Verifying that nodes have access to the same disk
See “[Verifying that the nodes have access to the same disk](#)” on page 120.
- Testing the shared disks for SCSI-3
See “[Testing the disks using vxfcntl utility](#)” on page 120.

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
libvxCLARiON.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 `vxfcntlsthdw` 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 vxfcntlsthdw 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 `vxfcntlshdw` utility indicates a disk can be used for I/O fencing with a message resembling:

```
The disk /dev/rdisk/clt1d0s2 is ready to be configured for I/O Fencing on
node galaxy
```

For more information on how to replace coordinator disks, refer to the *Symantec VirtualStore Administrator's Guide*.

To test the disks using `vxfcntlshdw` 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.

```
# vxfcntlshdw [-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: galaxy
```

```
Enter the second node of the cluster: nebula
```

- 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_galaxy 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_ofgalaxy and IP_adrs_of_nebula
/dev/rdisk/c2t13d0s2
```

```
Enter the disk name to be checked for SCSI-3 PGR on node
IP_adrs_of_nebula 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_ofgalaxy and IP_adrs_of_nebula
/dev/rdisk/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 report 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 galaxy.

```
The disk is now ready to be configured for I/O Fencing on node
galaxy
```

```
ALL tests on the disk /dev/rdisk/c1t1d0s2 have PASSED
The disk is now ready to be configured for I/O Fencing on node
galaxy
```

- 7 Run the vxfcntlshdw utility for each disk you intend to verify.

Setting up disk-based I/O fencing manually

[Table 8-1](#) lists the tasks that are involved in setting up I/O fencing.

Table 8-1 Tasks to set up I/O fencing manually

Task	Reference
Initializing disks as VxVM disks	See “Initializing disks as VxVM disks” on page 115.
Identifying disks to use as coordinator disks	See “Identifying disks to use as coordinator disks” on page 123.
Checking shared disks for I/O fencing	See “Checking shared disks for I/O fencing” on page 118.
Setting up coordinator disk groups	See “Setting up coordinator disk groups” on page 124.
Creating I/O fencing configuration files	See “Creating I/O fencing configuration files” on page 124.
Modifying Symantec VirtualStore configuration to use I/O fencing	See “Modifying VCS configuration to use I/O fencing” on page 125.
Configuring Coordination Point agent to monitor coordination points	See “Configuring Coordination Point agent to monitor coordination points” on page 147.
Verifying I/O fencing configuration	See “Verifying I/O fencing configuration” on page 127.

Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See [“Initializing disks as VxVM disks”](#) on page 115.

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 118.

Setting up coordinator disk groups

From one node, create a disk group named `vxfencoorddg`. 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 Volume Manager 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 `vxfencoorddg` disk group

- 1 On any node, create the disk group by specifying the device names:

```
# vxdg init vxfencoorddg c1t1d0s2 c2t1d0s2 c3t1d0s2
```

- 2 Set the coordinator attribute value as "on" for the coordinator disk group.

```
# vxdg -g vxfencoorddg set coordinator=on
```

- 3 Deport the coordinator disk group:

```
# vxdg deport vxfencoorddg
```

- 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 "vxencoorddg" > /etc/vxfendg
```

Do not use spaces between the quotes in the "vxencoorddg" 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 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 If the I/O fencing driver vxfen is already running, stop the I/O fencing driver. Depending on the Solaris version on the cluster nodes, run the following command:

■ Solaris 9:

```
# /etc/init.d/vxfen stop
```

■ Solaris 10:

```
# svcadm disable -t vxfen
```

- 4 Make a backup copy of the main.cf file:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.orig
```

- 5 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.

- 6 Save and close the file.
- 7 Verify the syntax of the file /etc/VRTSvcs/conf/config/main.cf:

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

- 8 Using rcp or another utility, copy the VCS configuration file from a node (for example, galaxy) to the remaining cluster nodes.

For example, on each remaining node, enter:

```
# rcp galaxy:/etc/VRTSvcs/conf/config/main.cf \  
/etc/VRTSvcs/conf/config
```

- 9 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`.

Depending on the Solaris version on the cluster nodes, run the following command:

- Solaris 9:

```
# /etc/init.d/vxfen start
```

- Solaris 10:

```
# 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 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 (galaxy)  
1 (nebula)
```

```
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

If Symantec VirtualStore cluster is configured to run in secure mode, then verify that the configuration is correct before you configure CP server-based I/O fencing.

See [“Verifying the security configuration on the SFCFS cluster to use CP server coordination point”](#) on page 128.

See [“Configuring server-based I/O fencing using the installsvs”](#) on page 130.

Verifying the security configuration on the SFCFS cluster to use CP server coordination point

After configuring security using the `installsvs -security` command, follow the procedure below on each SFCFS cluster node to confirm that security is correctly configured.

To verify the security configuration on SFCFS cluster to use CP server coordination point

- 1 Run the following command:

```
# /opt/VRTScps/bin/cpsat listpd -t local
```

The following is an example of the command output:

```
Domain(s) Found 1
```

```
*****
```

```
Domain Name HA_SERVICES@galaxy.symantec.com
```

```
Expiry Interval 0
```

```
*****
```

- 2 There should be a domain name entry with the following format in the command output:

```
HA_SERVICES@hostname.domainname
```

or

```
HA_SERVICES@hostname
```

3 There should not be duplicate entries for HA_SERVICES domain.

The following is an example of an incorrect configuration:

```
showdomains

Domain(s) Found :          3

*****

Domain Name:      HA_SERVICES@galaxy.symantec.com

Domain Type:      vx

*****

Domain Name:      broker@galaxy.symantec.com

Domain Type:      vx

*****

Domain Name:      HA_SERVICES@galaxy

Domain Type:      vx

*****
```

Proceed to reconfigure security in case duplicate entries appear as shown in the above example.

Configuring server-based I/O fencing using the 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 67.

See [“Recommended CP server configurations”](#) on page 71.

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 131.
Single CP server	See “To configure server-based fencing for the Symantec VirtualStore cluster (single CP server)” on page 136.

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 74.
 - The coordination disks are verified for SCSI3-PR compliance.
See [“Checking shared disks for I/O fencing”](#) on page 118.

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

```
# /opt/VRTS/install/installsvs -fencing
```

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.

- 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 5.1 SP1 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 [1-3,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  
CP 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 virtual IP addresses or host names of the virtual IP address 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/fully qualified host name  
for the Co-ordination Point Server #1:  
[b] 10.209.80.197
```

- Enter the port that the CP server would be listening on.

```
Enter the port in the range [49152, 65535] which the  
Co-ordination 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 fencing mechanism 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] (vxfencoorddg)
```

9 Verify and confirm the coordination points information for the fencing configuration.

For example:

```
Total number of coordination points being used: 3
CP Server (Port):
  1. 10.209.80.197 (14250)
SCSI-3 disks:
  1. c1t1d0s2
  2. c2t1d0s2
Disk Group name for the disks in customized fencing: vxfencoorddg
Disk mechanism 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):

- Make sure that the security configuration in the application cluster and the CP server is the same. If CP server is configured for security, ensure that the application cluster also runs in secure mode.
- If the CP server is configured for security, perform the following steps:
 - Review the output as the installer verifies if the Symantec VirtualStore (application cluster) nodes have already established trust with an AT root broker.
 - If the Symantec VirtualStore (application cluster) nodes and the CP server use different AT root brokers, enter y at the installer prompt and provide the following information:
 - Hostname for the authentication broker for any one of the CP servers
 - Port number where the authentication broker for the CP server is listening for establishing trust
 - Hostname for the authentication broker for any one of the Symantec VirtualStore (application cluster) nodes
 - Port number where the authentication broker for the Symantec VirtualStore (application cluster) is listening for establishing trust

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 CP Server 10.210.80.199

Adding the client cluster to the CP Server 10.210.80.199 ..... Done

Registering client node galaxy with CP Server 10.210.80.199..... Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ..... Done
Adding cluster clus1 to the CPClient user on CP Server 10.210.80.199 ... Done

Registering client node nebula with CP Server 10.210.80.199 ..... Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ..... Done
Adding cluster clus1 to the CPClient user on CP Server 10.210.80.199 ... Done

Updating /etc/vxfenmode file on galaxy ..... Done
Updating /etc/vxfenmode file on nebula ..... Done
```

See [“About I/O fencing configuration files”](#) on page 65.

- 13** Configure the CP agent on the Symantec VirtualStore (application cluster).

```
Do you want to configure CP Agent on the client cluster? [y,n,q]
(y)

Enter a non-existing name for the service group for CP Agent:
[b] (vxfen)

Adding CP Agent via galaxy ..... Done
```

- 14** 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.
- 15** 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.

See “[Setting up the CP server](#)” on page 74.

- 2** Start the installsvs with `-fencing` option.

```
# /opt/VRTS/install/installsvs -fencing
```

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.

- 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 5.1 SP1 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 [1-3,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** Enter the total number of coordination points as **1**.

```
Enter the total number of co-ordination points including both
CP servers and disks: [b] (3) 1
```

Read the installer warning carefully before you proceed with the configuration.

- 7** Provide the following CP server details at the installer prompt:

- Enter the virtual IP address or the host name of the virtual IP address 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/fully qualified host name
for the Co-ordination Point Server #1:
[b] 10.209.80.197
```

- Enter the port that the CP server would be listening on.

```
Enter the port in the range [49152, 65535] which the
Co-ordination Point Server 10.209.80.197
would be listening on or simply accept the default port suggested:
[b] (14250)
```

8 Verify and confirm the coordination points information for the fencing configuration.

For example:

```
Total number of coordination points being used: 1
CP Server (Port):
    1. 10.209.80.197 (14250)
```

9 If the CP server is configured for security, the installer sets up secure communication between the CP server and the Symantec VirtualStore (application cluster):

- Make sure that the security configuration in the application cluster and the CP server is the same. If CP server is configured for security, ensure that the application cluster also runs in secure mode.
- If the CP server is configured for security, perform the following steps:
 - Review the output as the installer verifies if the Symantec VirtualStore (application cluster) nodes have already established trust with an AT root broker.
 - If the Symantec VirtualStore (application cluster) nodes and the CP server use different AT root brokers, enter y at the installer prompt and provide the following information:
 - Hostname for the authentication broker for any one of the CP servers
 - Port number where the authentication broker for the CP server is listening for establishing trust
 - Hostname for the authentication broker for any one of the Symantec VirtualStore (application cluster) nodes
 - Port number where the authentication broker for the Symantec VirtualStore (application cluster) is listening for establishing trust

After the installer establishes trust between the authentication brokers of the CP servers and the application cluster nodes, press Enter to continue.

10 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}
```

11 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 CP Server 10.210.80.199

Adding the client cluster to the CP Server 10.210.80.199 ..... Done

Registering client node galaxy with CP Server 10.210.80.199..... Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ..... Done
Adding cluster clus1 to the CPClient user on CP Server 10.210.80.199 ... Done

Registering client node nebula with CP Server 10.210.80.199 ..... Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ..... Done
Adding cluster clus1 to the CPClient user on CP Server 10.210.80.199 ... Done

Updating /etc/vxfenmode file on galaxy ..... Done
Updating /etc/vxfenmode file on nebula ..... Done
```

See [“About I/O fencing configuration files”](#) on page 65.

12 Configure the CP agent on the Symantec VirtualStore (application cluster).

```
Do you want to configure CP Agent on the client cluster? [y,n,q]
(y)

Enter a non-existing name for the service group for CP Agent:
[b] (vxfen)

Adding CP Agent via galaxy ..... Done
```

- 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 Note the location of the configuration log files, summary files, and response files that the installer displays for later use.

Setting up server-based I/O fencing manually

Tasks that are involved in setting up server-based I/O fencing manually include:

Table 8-2 Tasks to set up server-based I/O fencing manually

Action	Description
Preparing the CP servers for use by the Symantec VirtualStore cluster	See “Preparing the CP servers manually for use by the SFCFS cluster” on page 139.
Modifying I/O fencing configuration files to configure server-based I/O fencing	See “Configuring server-based fencing on the SFCFS cluster manually” on page 143.
Modifying Symantec VirtualStore configuration to use I/O fencing	See “Modifying VCS configuration to use I/O fencing” on page 125.
Configuring Coordination Point agent to monitor coordination points	See “Configuring Coordination Point agent to monitor coordination points” on page 147.
Verifying the server-based I/O fencing configuration	See “Verifying server-based I/O fencing configuration” on page 149.

Preparing the CP servers manually for use by the SFCFS cluster

Use this procedure to manually prepare the CP server for use by the SFCFS cluster or clusters.

[Table 8-3](#) displays the sample values used in this procedure.

Table 8-3 Sample values in procedure

CP server configuration component	Sample name
CP server	mycps1.symantecexample.com
Node #1 - SFCFS cluster	galaxy

Table 8-3 Sample values in procedure *(continued)*

CP server configuration component	Sample name
Node #2 - SFCFS cluster	nebula
Cluster name	clus1
Cluster UUID	{f0735332-1dd1-11b2}

To manually configure CP servers for use by the SFCFS cluster

- 1
- Determine the cluster name and uuid on the SFCFS cluster.

For example, issue the following commands on one of the SFCFS cluster nodes (galaxy):

```
# grep cluster /etc/VRTSvcS/conf/config/main.cf

cluster clus1

# cat /etc/vx/.uuids/clusuuid

{f0735332-1dd1-11b2}
```

- 2
- Use the `cpsadm` command to check whether the SFCFS cluster and nodes are present in the CP server.

For example:

```
# cpsadm -s mycps1.symantecexample.com -a list_nodes

ClusName  UUID                               Hostname(Node ID)  Registered
clus1     {f0735332-1dd1-11b2} galaxy(0)           0
clus1     {f0735332-1dd1-11b2} nebula(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 SFCFS cluster and nodes to each CP server.

For example, issue the following command on the CP server (mycps1.symantecexample.com) to add the cluster:

```
# cpsadm -s mycps1.symantecexample.com -a add_clus\  
-c clus1 -u {f0735332-1dd1-11b2}
```

Cluster clus1 added successfully

Issue the following command on the CP server (mycps1.symantecexample.com) to add the first node:

```
# cpsadm -s mycps1.symantecexample.com -a add_node\  
-c clus1 -u {f0735332-1dd1-11b2} -h galaxy -n0
```

Node 0 (galaxy) successfully added

Issue the following command on the CP server (mycps1.symantecexample.com) to add the second node:

```
# cpsadm -s mycps1.symantecexample.com -a add_node\  
-c clus1 -u {f0735332-1dd1-11b2} -h nebula -n1
```

Node 1 (nebula) successfully added

4 If security is to be enabled, check whether the _HA_VCS_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 mycps1.symantecexample.com -a list_users
```

Username/Domain	Type	Cluster Name / UUID	Role
_HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com	vx	clus1/{f0735332-1dd1-11b2}	Operator
_HA_VCS_nebula@HA_SERVICES@nebula.symantec.com	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 _HA_VCS_users (for example, cpsclient@galaxy).

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.

First, determine the user@domain to be added on the SFCFS cluster (application cluster).

The user for fencing should be of the form `_HA_VCS_short-hostname` and domain name is that of HA_SERVICES user in the output of command:

```
# /opt/VRTScps/bin/cpsat listpd -t local
```

Next, issue the following commands on the CP server (mycps1.symantecexample.com):

```
# cpsadm -s mycps1.symantecexample.com -a add_user -e\  
_HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com\  
-f cps_operator -g vx
```

```
User _HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com  
successfully added
```

```
# cpsadm -s mycps1.symantecexample.com -a add_user -e\  
_HA_VCS_nebula@HA_SERVICES@nebula.symantec.com\  
-f cps_operator -g vx
```

```
User _HA_VCS_nebula@HA_SERVICES@nebula.symantec.com  
successfully added
```

- 6 Authorize the CP server user to administer the SFCFS cluster. You must perform this task for the CP server users corresponding to each node in the SFCFS cluster.

For example, issue the following command on the CP server (mycps1.symantecexample.com) for SFCFS cluster clus1 with two nodes galaxy and nebula:

```
# cpsadm -s mycps1.symantecexample.com -a\  
add_clus_to_user -c clus1\  
-u {f0735332-1dd1-11b2}\  
-e _HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com\  
-f cps_operator -g vx
```

```
Cluster successfully added to user  
_HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com privileges.
```

```
# cpsadm -s mycps1.symantecexample.com -a\  
add_clus_to_user -c clus1\  
-u {f0735332-1dd1-11b2}\  
-e _HA_VCS_nebula@HA_SERVICES@nebula.symantec.com\  
-f cps_operator -g vx
```

```
Cluster successfully added to user  
_HA_VCS_nebula@HA_SERVICES@nebula.symantec.com privileges.
```

Configuring server-based fencing on the SFCFS cluster manually

The configuration process for the client or SFCFS 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 (vxfgndg). You must specify this disk group in the `/etc/vxfenmode` file.

See [“Setting up coordinator disk groups”](#) on page 124.

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 SFCFS 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”](#) on page 144.

- 3 After editing the `/etc/vxfenmode` file, run the `vxfen init` script to start fencing.

For example:

On Solaris 9 systems:

```
# /etc/init.d/vxfen start
```

On Solaris 10 systems:

```
# svcadm enable vxfen
```

Sample vxfenmode file output

The following sample file output displays

```
#  
# 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

# 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 each row. 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>=<Virtual IP/ Virtual hostname of cp server> in
# square brackets ([]), followed by ":" and CPS port number.
#
# Examples:
# cps1=[192.168.0.23]:14250
# cps2=[mycps.company.com]:14250
#
# 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
#
```

Table 8-4 defines the vxfenmode parameters that must be edited.

Table 8-4 vxfenmode file parameters

vxfenmode File Parameter	Description
vxfen_mode	Fencing mode of operation. This parameter must be set to “customized”.

Table 8-4 vxfenmode file parameters (*continued*)

vxfenmode File Parameter	Description
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 Symantec Product Authentication Service 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. Note: Symantec only supports a configuration where both the CP server and client sides have the same security setting. The security setting on both sides must be either enabled or disabled.
cps1, cps2, cps3, or vxfendg	Coordination point parameters. Enter either the Virtual IP address or FQHN (whichever is accessible) of the CP server. Note: Whenever coordinator disks are used in an I/O fencing configuration, a disk group has to be created (vxfendg) 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).
single_cp	Value 1 for single_cp parameter indicates that the server-based fencing uses a single highly available CP server as its only coordination point. Value 0 for single_cp parameter indicates that the server-based fencing uses at least three coordination points.

Configuring Coordination Point agent to monitor coordination points

The following procedure describes how to manually configure the Coordination Point agent to monitor coordination points (CP server or SCSI-3 disks).

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

To configure Configuration Point agent to monitor coordination points

- 1** Ensure that your SFCFS 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 galaxy 0 nebula 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 1
# hares -modify coordpoint Enabled 1
# haconf -dump -makero
```

- 3 Verify the status of the agent on the SFCFS 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        galaxy      ONLINE
coordpoint      State        nebula      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 Coordination Point agent monitoring information; including information about whether the Coordination Point agent is able to access all the coordination points, information to check on which coordination points the Coordination Point agent is reporting missing keys, etc.

To view all such information 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.

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 65.

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 galaxy five times more weight compared to nebula, run the following commands:

```
# hasys -modify galaxy FencingWeight 50
# hasys -modify nebula 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
```

Setting up Symantec VirtualStore

- [Chapter 9. Setting up Symantec VirtualStore](#)

Setting up Symantec VirtualStore

This chapter includes the following topics:

- [Disabling SMF for NFS daemons on Solaris 10](#)
- [Setting up Clustered NFS](#)
- [Setting up Symantec VirtualStore](#)
- [Useful links from VMware on NFS support and customization while cloning virtual machines](#)

Disabling SMF for NFS daemons on Solaris 10

On Solaris 10, 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

This section describes how to set up Clustered NFS (CNFS).

Note: Disk layout Version 8 is required for taking FileSnaps of virtual machines. See the `vxupgrade` (1M) and the `mkfs` (1M) manual pages.

To set up CNFS

- 1 Create a shared volume (around 100M) on the shared disk group to store the CNFS metadata, create a disk layout Version 8 file system on top, and add it to the configuration. For example:

```
# vxassist -g shared_disk_group make svsmeta_vol 100m
# mkfs -F vxfs -o version=8 /dev/vx/rdisk/shared_disk_group/svsmeta_vol
# cfsshare config -p nfs shared_disk_group svsmeta_vol /svsmeta_mntpt
```

- 2 Create another shared volume that will be used to store the VMware images, create a disk layout Version 8 file system on it, and add it to the configuration. For example:

```
# vxassist -g shared_disk_group make svldata size
# mkfs -F vxfs -o version=8 /dev/vx/rdisk/shared_disk_group/svldata_vol
# cfsshare add -p nfs -N nfs_share_options shared_disk_group \
svldata_vol /svldata_mntpt all=[mount_options]
```

- 3 Add a Virtual IP address to access the cluster:

```
# cfsshare addvip bge0 10.182.111.222 255.255.255.0
```

- 4 Add the CNFS share created and the VIP added in the above steps to configure a NFS datastore on all your ESX machines.

Setting up Symantec VirtualStore

This section describes how to set up Symantec VirtualStore.

To set up Symantec VirtualStore

- 1 On all the nodes in the cluster, install the `openssl`, if it is not already installed.

```
# gunzip -c openssl-1.0.0a_build.tar.gz | tar -xvf -
# cd openssl-1.0.0a
# ./config
# make
# make install
```

- 2 On all nodes in the cluster, install the following Perl modules, if not already installed.

Note: You can download the perl modules from the CPAN site.

<http://www.cpan.org>

Ensure that all prerequisites Perl modules of the Perl modules that are listed below are installed.

- Perl modules:
- Crypt-SSLeay
- Data-Dumper
- Class-MethodMaker
- ExtUtils-MakeMaker
- XML-NamespaceSupport
- XML-SAX
- XML-LibXML
- libwww-perl
- Class-Inspector
- Task-Weaken
- XML-Parser
- SOAP-Lite
- UUID

For each perl module above perform the following commands on each node in the cluster:

```
# gunzip -c <perl_module>.tar.gz | tar -xvf -
# cd <perl_module>
# perl Makefile.PL
# make
# make install
```

where `<perl_module>` is the name of the perl module.

- 3 On all the nodes in the cluster, install the latest VMWare vSphere SDK for PERL.

Note: As there is no Solaris version of the VMWare vSphere SDK for PERL you need to download the Linux version of the SDK, even for the Solaris platform.

```
# gunzip -c VMware-vSphere-SDK-for-Perl-4.0.0-161974.x86_64.tar.gz \
| tar -xvf -
# cd vmware-vsphere-cli-distrib
# perl Makefile.PL
# make
# make install
```

- 4 (Optional) In case the vmware-sdk or any of its dependent libraries are installed in non-default locations (anything outside of system perl folders), edit the `/etc/opt/VRTSsfmh/xprtld.conf` file to update the PERL5LIB path on all nodes in the cluster.

If you have modified the `/etc/opt/VRTSsfmh/xprtld.conf` file, you must restart `xprtld` using the following commands:

```
# /etc/init.d/xprtld stop
# /etc/init.d/xprtld start
```

- 5 If the directory does not exist, create a text file in `/opt/VRTSsfmh/web/admin/cgi-bin` and verify that you are able to access text file without any authorization by:

`https://<virtual_IP_for_svs>:5634/admin/cgi-bin/<text_file>`

where `<virtual_IP_for_svs>` is the Virtual IP for SVS.

where `<text_file>` is the text file you create in

`/opt/VRTSsfmh/web/admin/cgi-bin`.

- 6 Register the plugin.

```
# cd /opt/VRTSsfmh/web/admin/cgi-bin
# perl vstore_register.pl
--conf_dir= "<configuration_directory>"
--action="install"
--vstore_server="<virtual_IP_for_SVS>"
--server="<vCenter_server_IP_or_hostname>"
--username="<vcenter_login>"
--password="<vcenter_password>"
```

where *<vCenter_server_IP_or_hostname>* is the name of the vCenter server IP or host name.

where *<vcenter login>* is the username of the vCenter login.

where *<vcenter password>* is the vCenter password.

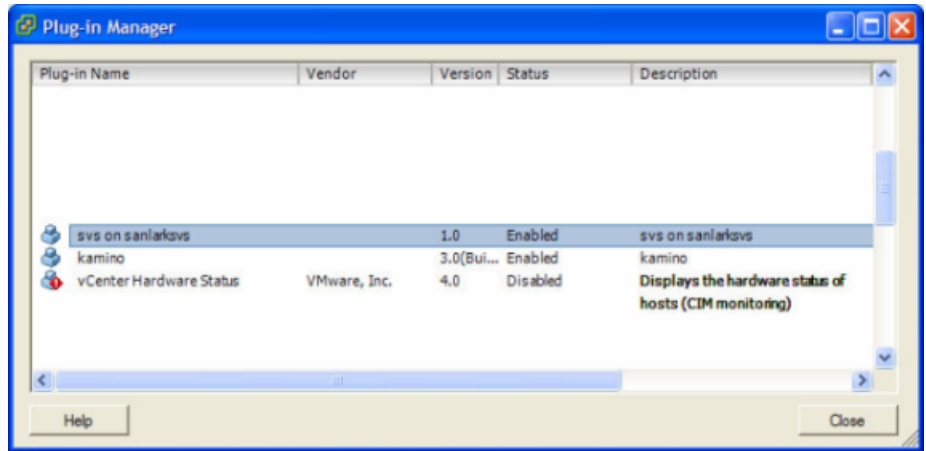
- In order to unregister the plugin, you can run the above command with the `--action="remove"` argument.

For example:

```
# perl vstore_register.pl
--action="remove"
--vstore_server="<virtual_IP_for_SVS>"
--server="<vCenter_server_IP_or_hostname>"
--username="<vcenter_login>"
--password="<vcenter_password>"
```

7 Verify that the plugin is installed and working:

- Go to vCenter VI client.
- Click on "Plug-ins" : A "Plug-in Manager" window displays.
- Ensure that you see "svs on *<cluster_name>*" in the list of installed plugins.
- Verify that the plug-in is in the enabled state.



- 8 In order for the customizatoin to work properly, VMware tools need to be installed in the Windows and Linux guest.

For Windows:

- Right click on virtual machine
- Guest -> Install/Upgrade VMware Tools
This kickstarts the tools installation in the guest.

For Linux:

- Right click on Virtual Machine
- Guest -> Install/Upgrade VMware Tools
This mounts the VMware tools CD.

Login to the guest console and execute following commands:

```
# mount /dev/cdrom /mnt
# cd /mnt
# cp VMwareTools-*.tar.gz /root/
# cd /root
# gunzip -c VMwareTools*.tar.gz | tar -xvf -
```

```
# cd vmware-tools-distrib
# ./vmware-install.pl
```

9 For Windows the following is also needed for customization to work:

The `sysprep.exe` and all the related files must be copied at appropriate location on the vCenter server:

```
C:\ProgramData\VMware\VMware VirtualCenter\sysprep>dir
Volume in drive C has no label.
Volume Serial Number is 4C07-3EE8
```

Directory of C:\ProgramData\VMware\VMware VirtualCenter\sysprep

```
04/05/2010  01:46 AM    <DIR>          .
04/05/2010  01:46 AM    <DIR>          ..
04/05/2010  01:46 AM    <DIR>          1.1
04/05/2010  01:46 AM    <DIR>          2k
05/18/2010  08:16 AM    <DIR>          svr2003
04/05/2010  01:46 AM    <DIR>          svr2003-64
04/05/2010  01:46 AM    <DIR>          xp
04/05/2010  01:46 AM    <DIR>          xp-64
               0 File(s)                0 bytes
               8 Dir(s)  263,370,924,032 bytes free
```

Copy all the files for the sysprep directory under corresponding folder shown above.

For Windows 2003 32-bit: svr2003

For Windows 2003 64-bit: svr2003-64

And so on.

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
- vSphere Basic System Administration Guide

See the guest operating systems customization chapter.

https://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_admin_guide.pdf

Creating virtual machine clones using Symantec FileSnap workflow

- [Chapter 10. Creating virtual machine clones using Symantec FileSnap](#)

Creating virtual machine clones using Symantec FileSnap

This chapter includes the following topics:

- [Creating virtual machine clones using Symantec FileSnap](#)

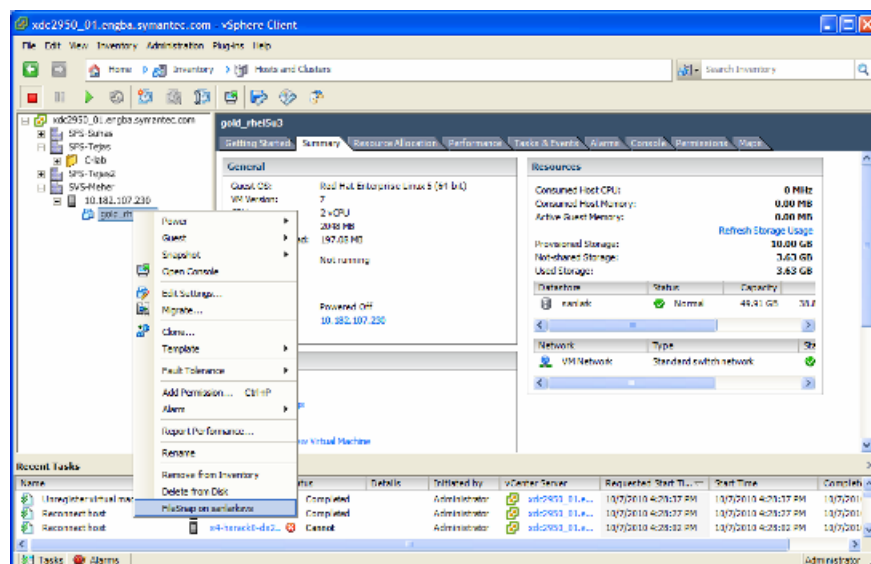
Creating virtual machine clones using Symantec FileSnap

This section describes how to Create virtual machine clones using Symantec FileSnap.

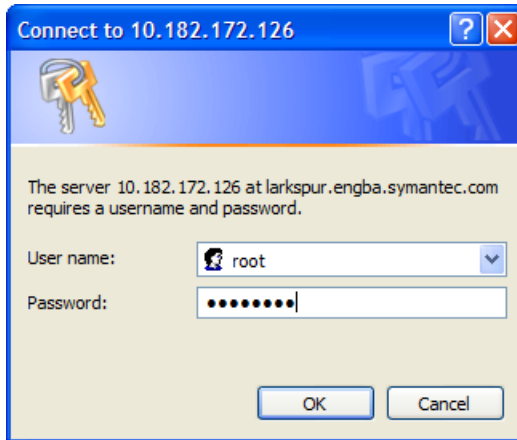
To Create virtual machine clones using Symantec FileSnap

- 1 Right click on the virtual machine you want to clone, and select "FileSnap on <clustername>" in the vSphere Client window.

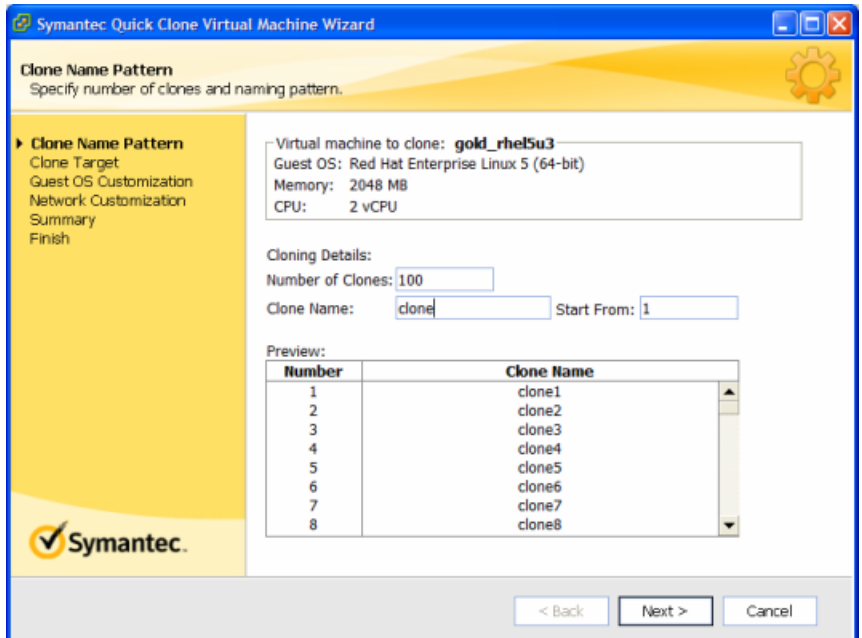
Note: Depending upon whether the virtual disks belong to Symantec datastore (CNFS/SVS), the GUI allows or disallows the cloning operation of the virtual machine. To allow cloning, at least one virtual disk must be from Symantec datastore. If the NEXT button is not displayed, then the GUI displays a message that the cloning operation is not allowed on this virtual machine.



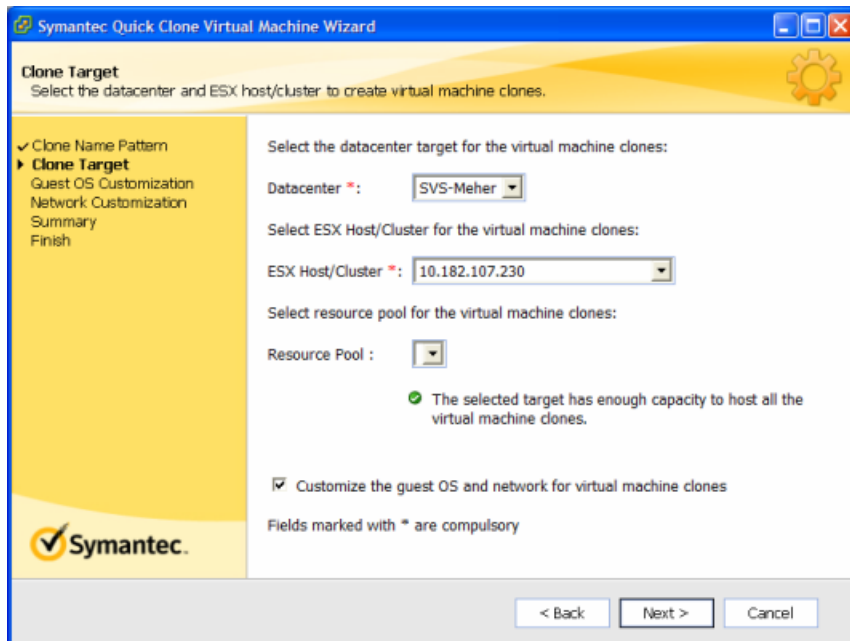
- 2 Provide root credentials to the virtualstore cluster.



- 3 Verify the virtual machine being cloned and provide details for the clones being created.



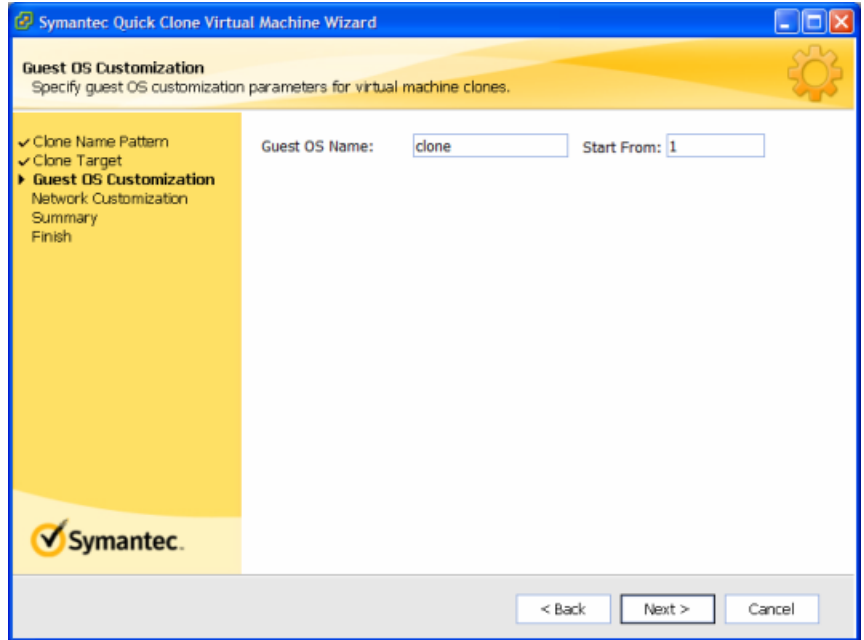
- 4 Select the target where you want the clones to reside. If you want to customize the clones, check the "Customize the guest OS and network for virtual machine clones" box.



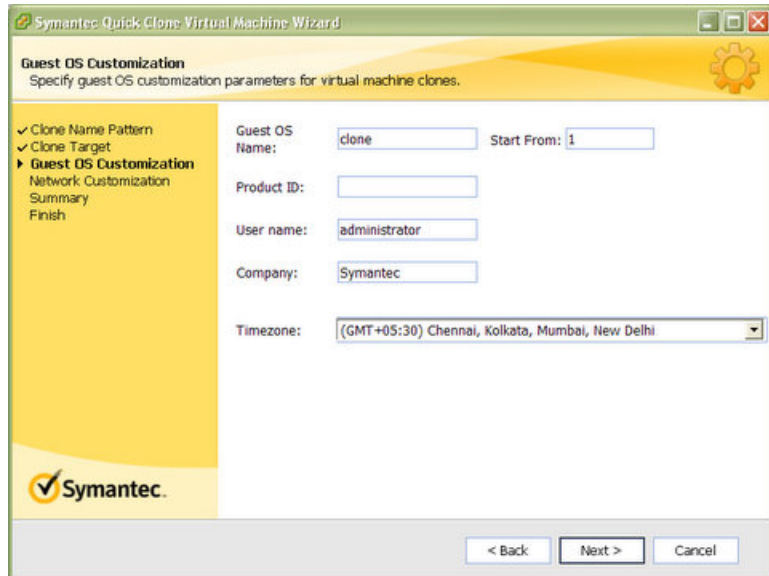
The image shows the 'Symantec Quick Clone Virtual Machine Wizard' window, specifically the 'Clone Target' step. The window has a yellow header bar with the title 'Symantec Quick Clone Virtual Machine Wizard' and standard window controls. Below the header, the 'Clone Target' section is highlighted in yellow. The main area is white and contains the following elements:

- Clone Target**: Select the datacenter and ESX host/cluster to create virtual machine clones.
- Clone Name Pattern**: A list of steps including 'Clone Name Pattern', 'Clone Target' (selected), 'Guest OS Customization', 'Network Customization', 'Summary', and 'Finish'.
- Select the datacenter target for the virtual machine clones:** A dropdown menu showing 'SVS-Meher'.
- Select ESX Host/Cluster for the virtual machine clones:** A dropdown menu showing '10.182.107.230'.
- Select resource pool for the virtual machine clones:** A dropdown menu showing an empty box.
- Resource Pool :** A dropdown menu showing an empty box.
- Checkmark:** A green checkmark indicating 'The selected target has enough capacity to host all the virtual machine clones.'
- Customize the guest OS and network for virtual machine clones:** A checkbox that is checked.
- Fields marked with * are compulsory:** A note at the bottom.
- Navigation buttons:** '< Back', 'Next >', and 'Cancel' buttons at the bottom right.

- 5 Provide Customization details for the guest OS.
 - a. For Linux, Provide customization details.



- b. For Windows, Provide customization details.



The image shows a screenshot of the 'Symantec Quick Clone Virtual Machine Wizard' window, specifically the 'Guest OS Customization' step. The window has a yellow header bar with the title 'Symantec Quick Clone Virtual Machine Wizard' and a gear icon. Below the header, the text 'Guest OS Customization' is displayed, followed by the instruction 'Specify guest OS customization parameters for virtual machine clones.' On the left side, there is a vertical navigation pane with a yellow background. It contains a list of steps: 'Clone Name Pattern' (checked), 'Clone Target' (checked), 'Guest OS Customization' (selected with a right-pointing triangle), 'Network Customization', 'Summary', and 'Finish'. The main area of the window is white and contains several input fields: 'Guest OS Name' (with the value 'clone'), 'Start From' (with the value '1'), 'Product ID' (empty), 'User name' (with the value 'administrator'), 'Company' (with the value 'Symantec'), and 'Timezone' (a dropdown menu showing '(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi'). At the bottom of the window, there is a grey bar containing three buttons: '< Back', 'Next >', and 'Cancel'. The Symantec logo is visible in the bottom left corner of the main area.

Symantec Quick Clone Virtual Machine Wizard

Guest OS Customization
Specify guest OS customization parameters for virtual machine clones.

✓ Clone Name Pattern
✓ Clone Target
▶ Guest OS Customization
Network Customization
Summary
Finish

Guest OS Name: clone Start From: 1

Product ID:

User name: administrator

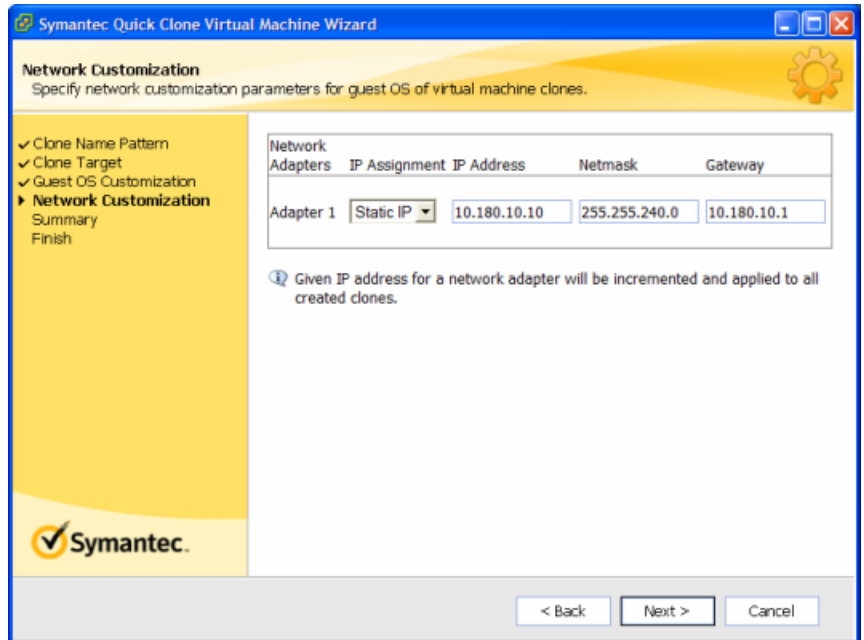
Company: Symantec

Timezone: (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi

Symantec

< Back Next > Cancel

6 Provide IP address details for the virtual machines.



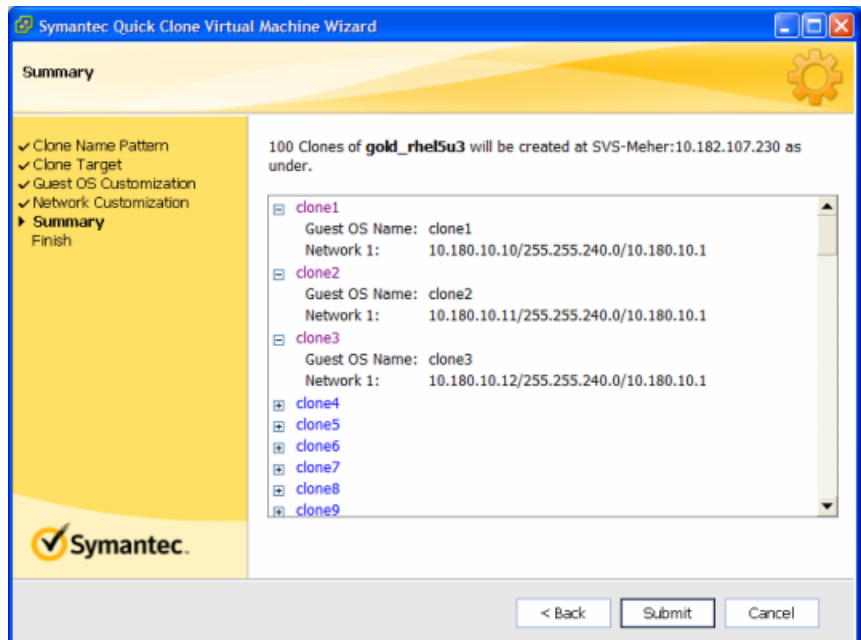
The screenshot shows the 'Symantec Quick Clone Virtual Machine Wizard' window, specifically the 'Network Customization' step. The window has a yellow header bar with the title and a gear icon. Below the header, a subtitle reads 'Specify network customization parameters for guest OS of virtual machine clones.' On the left, a sidebar lists the steps: 'Clone Name Pattern', 'Clone Target', 'Guest OS Customization', 'Network Customization' (which is expanded), 'Summary', and 'Finish'. The main area contains a table for network adapters. The table has columns: 'Adapters', 'IP Assignment', 'IP Address', 'Netmask', and 'Gateway'. There is one row for 'Adapter 1' with 'Static IP' selected in the dropdown, and the values '10.180.10.10', '255.255.240.0', and '10.180.10.1' respectively. Below the table, a note with an information icon states: 'Given IP address for a network adapter will be incremented and applied to all created clones.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The Symantec logo is in the bottom left corner.

Adapters	IP Assignment	IP Address	Netmask	Gateway
Adapter 1	Static IP	10.180.10.10	255.255.240.0	10.180.10.1

Given IP address for a network adapter will be incremented and applied to all created clones.

< Back Next > Cancel

7 Verify and click Submit.



Index

A

- About
 - Symantec VirtualStore 13
- adding
 - users 100
- attributes
 - UseFence 125

C

- cluster functionality
 - environment requirements 26
- Clustered NFS
 - setting up 157
- commands
 - format 25
 - vxdisksetup (initializing disks) 115
 - vxlicinst 107
 - vxlicrep 107
- configuring
 - rsh 21
 - ssh 21
- configuring Symantec VirtualStore
 - script-based installer 89
- configuring VCS
 - adding users 100
 - event notification 100, 102
 - global clusters 104
 - secure mode 97
 - starting 90
- controllers
 - SCSI 22
- coordinator disks
 - DMP devices 63
 - for I/O fencing 63
 - setting up 124
- Creating
 - virtual machine clones 167

D

- data disks
 - for I/O fencing 63
- disks
 - adding and initializing 115
 - coordinator 124
 - testing with vxfcntlthdw 118
 - verifying node access 120

F

- FC-AL controllers 25
- Fibre Channel fabric 27
- FileSnap 167

G

- global clusters
 - configuration 104

I

- I/O fencing
 - checking disks 118
 - setting up 122
 - shared storage 118
- installer
 - Symantec VirtualStore 45
- Installing
 - SVS with the Web-based installer 48
 - Symantec VirtualStore using the installer 45
- installing
 - post 105
 - Root Broker 57

L

- license keys
 - adding with vxlicinst 107
 - replacing demo key 107
- licenses
 - information about 107
- LLT
 - interconnects 20

M

- media speed 20
- optimizing 20

O

- optimizing
 - media speed 20

P

- persistent reservations
 - SCSI-3 22

R

- Root Broker
 - installing 57
- rsh 91
 - configuration 21

S

- SAN
 - see Storage Area Network 27
- script-based installer
 - Symantec VirtualStore configuration overview 89
- SCSI-3
 - persistent reservations 22
- SCSI-3 persistent reservations
 - verifying 122
- Setting up
 - Clustered NFS 157
 - Symantec VirtualStore 158
- shared storage
 - Fibre Channel
 - setting up 25
- SMTP email notification 100
- SNMP trap notification 102
- Solution
 - Symantec VirtualStore 13
- ssh 91
 - configuration 21
- starting configuration
 - installvcs program 91
 - Veritas product installer 91
- storage
 - setting up shared fibre 25
- Storage Area Network 27

SVS

- coordinator disks 124
- Symantec FileSnap 167
- Symantec Product Authentication Service 57, 97
- Symantec VirtualStore
 - about 13
 - configuring 89
 - installer 45
 - setting up 158
 - solution 13

U

- Useful links
 - VMware 163

V

- Virtual machine clones
 - creating 167
- VirtualStore
 - WMware Vsphere environment 13
- VMotion 13
- VMware 13
 - useful links 163
- Volume Manager
 - Fibre Channel 25
- vxdisksetup command 115
- vxlicinst command 107
- vxlicrep command 107

W

- Web-based installer 48