Veritas Storage Foundation™ Cluster File System Installation Guide

AIX

5.1 Service Pack 1

Symantec

Veritas Storage Foundation™ Cluster File System Installation 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: 5.1SP1.2

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

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

https://sort.symantec.com/documents

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

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

Section 1

Installation overview and planning

Chapter 1

About Storage Foundation Cluster File System

This chapter includes the following topics:

Veritas Storage Foundation Cluster File System suites

The following table lists the Symantec products and optionally licensed features available with each Veritas Storage Foundation Cluster File System (SFCFS) product suite.

Table 1-1 Contents of Veritas Storage Foundation Cluster File System products

Storage Foundation Cluster File System	Products and features
Storage Foundation Cluster File System	Veritas File System Veritas Volume Manager Veritas Quick I/O option Veritas Extension for Oracle Disk Manager option Veritas Storage Checkpoint option Veritas Storage Mapping option Optionally licensed features: Veritas Volume Replicator

Table 1-1 Contents of Veritas Storage Foundation Cluster File System products *(continued)*

Storage Foundation Cluster File System	Products and features
Storage Foundation Cluster File System HA	Veritas File System Veritas Volume Manager Veritas Cluster Server Veritas Quick I/O option Global Cluster Option Veritas Extension for Oracle Disk Manager option Veritas Storage Checkpoint option Veritas Storage Mapping option Optionally licensed features: Veritas Volume Replicator

About I/O fencing

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

The fencing operation determines the following:

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

This decision prevents possible data corruption. The installer installs the I/O fencing driver, VRTSvxfen, when you install Storage Foundation Cluster File System. To protect data on shared disks, you must configure I/O fencing after you install and configure Storage Foundation Cluster File System.

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

You can configure I/O fencing to use one or both of the following components as coordination points:

Coordinator disk

I/O fencing that uses coordinator disks is referred to as disk-based I/O fencing.

Disk-based I/O fencing ensures data integrity in a single cluster.

Coordination point server (CP server)	I/O fencing that uses at least one CP server system is referred to as server-based I/O fencing. Server-based I/O fencing ensures data integrity in multiple clusters. In virtualized environments that do not support SCSI-3 PR, Storage Foundation Cluster File System supports non-SCSI3 server-based I/O fencing. See "About I/O fencing for Storage Foundation Cluster File System in virtual machines that do not support SCSI-3 PR" on page 85.

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

See the *Veritas Storage Foundation Cluster File System Administrator's Guide*.

About Veritas graphical user interfaces

The following are descriptions of Veritas GUIs.

About Veritas Operations Manager

Veritas Operations Manager by Symantec gives you a single, centralized management console for the Veritas Storage Foundation and High Availability products. You can use it to monitor, visualize, and manage storage and cluster resources, and generate reports about them. Veritas Operations Manager lets administrators centrally manage diverse datacenter environments.

Veritas Operations Manager

Symantec recommends use of Veritas Operations Manager to manage Storage Foundation and Cluster Server environments.

The Veritas Enterprise Administrator (VEA) console is no longer packaged with Storage Foundation products. If you wish to continue using VEA, a version is available for download from http://go.symantec.com/vcsm_download. Veritas Storage Foundation Management Server is no longer supported.

If you wish to manage a single cluster using Cluster Manager (Java Console), a version is available for download from http://go.symantec.com/vcsm_download. Veritas Cluster Server Management Console is no longer supported.

Veritas Operations Manager provides a centralized management console for Veritas Storage Foundation and High Availability products. You can use Veritas Operations Manager to monitor, visualize, and manage storage resources and generate reports. Veritas Operations Manager is not available on the Storage Foundation and High Availability Solutions release. You can download Veritas Operations Manager at no charge at http://go.symantec.com/vom.

Refer to the Veritas Operations Manager documentation for installation, upgrade, and configuration instructions.

Chapter 2

Before you install

This chapter includes the following topics:

About planning for SFCFS 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: 5.1SP1.2.

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 SFCFS will be installed.

Follow the preinstallation instructions if you are installing one of the Veritas Storage Foundation Cluster File System products by Symantec.

The following Veritas Storage Foundation Cluster File System products by Symantec are installed with these instructions:

- Veritas Storage Foundation Cluster File System
- Veritas Storage Foundation Cluster File System High Availability (HA)

Several component products are bundled with each of these SFCFS products.

See "Veritas Storage Foundation Cluster File System suites" on page 23.

About installation and configuration methods

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

Table 2-1 Installation and configuration methods

Method	Description
Interactive installation and configuration using the script-based installer **Note:** If you obtained SFCFS from an electronic download site, you must use the `installsfcfs` script instead of the `installer` script.	You can use one of the following script-based installers: ■ Common product installer script: `installer` 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 SFCFS. ■ Product-specific installation script: `installsfcfs` ■ The product-specific installation script provides command-line interface options. Installing and configuring with the `installsfcfs` script is identical to specifying SFCFS from the `installer` script. Use this method to install or configure only SFCFS.
Silent installation using the response file	The response file automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. You can use the script-based installers with the response file to install silently on one or more systems. See "About response files" on page 383.
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. `./webinstaller` See "About the Web-based installer" on page 63.

Table 2-1 Installation and configuration methods *(continued)*

Method	Description
Network Installation Manager (NIM)	You can perform many advanced NIM installation tasks using the NIM interface and the System Management Interface Tool (SMIT). Use the Veritas product installer or the product-specific installation script to generate a NIM configuration file. Use the generated script to install Veritas packages from your NIM server. See "Installing SFCFS using NIM and the installer" on page 69.
Manual installation and configuration	Manual installation uses the AIX commands to install SFCFS. To retrieve a list of all filesets and patches required for all products in the correct installation order, enter: `# installer -allpkgs` Use the AIX commands to install SFCFS. Then use a manual or an interactive method with installsfcfs or `installer` script to configure the SFCFS stack.

Assessing system preparedness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Veritas Storage Foundation Cluster File System 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 31.

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 Veritas Storage Foundation Cluster File System 5.1 SP1. See "Prechecking your systems using the Veritas installer" on page 31.

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 Veritas Storage Foundation Cluster File System software

One method of obtaining the Veritas Storage Foundation Cluster File System 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.

See "About installation scripts" on page 375.

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 4 GB.

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 47.

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 -k 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, SFCFS commands are in /opt/VRTS/bin. SFCFS manual pages are stored in /opt/VRTS/man.

Some VCS custom scripts reside in /opt/VRTSvcs/bin. If you are installing a high availability product, add /opt/VRTSvcs/bin to the PATH also.

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
```

The nroff versions of the online manual pages are not readable using the man command if the bos.txt.tfs fileset is not installed; however, the VRTSvxvm and VRTSvxfs filesets install ASCII versions in the /opt/VRTS/man/cat* and /opt/VRTS/man/man* directories that are readable without the bos.txt.tfs fileset.

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.

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.

See "Installation script options" on page 376.

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.

See "About configuring secure shell or remote shell communication modes before installing products" on page 411.

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.

Note: Storage Foundation Cluster File System also supports non-SCSI3 server-based fencing configuration in virtual environments that do not support SCSI-3 PR-compliant storage.

See "About planning to configure I/O fencing" on page 90.

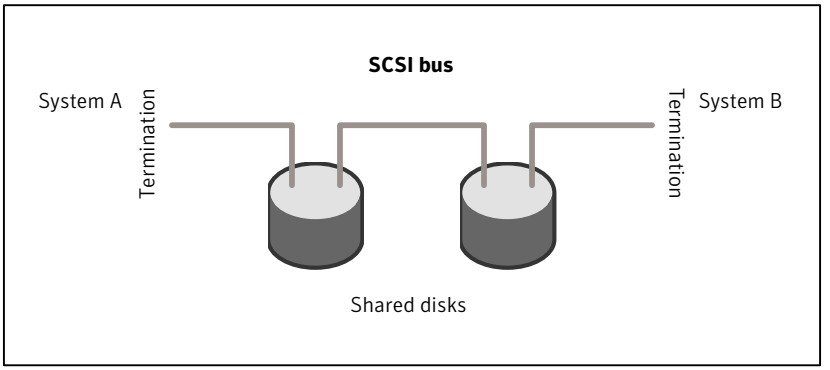
See also the *Veritas Storage Foundation Cluster File System Administrator's Guide* for a description of I/O fencing.

Setting the SCSI identifier value

SCSI adapters are typically set with a default identifier value of 7. Each device on a SCSI bus must have a unique SCSI identifier value. When more than one system is connected to a SCSI bus, you must change the SCSI identifier to a unique number. You must make this change to one or more systems, usually the unique number is 5 or 6.

Perform the procedure if you want to connect to shared storage with shared SCSI devices.

Figure 2-1 Cabling the shared storage



To set the SCSI identifier value

1 Determine the SCSI adapters on each system:

```
north # lsdev -C -c adapter | grep scsi
scsi0   Available 11-08    Wide/Ultra-2 SCSI I/O Controller
scsi1   Available 11-09    Wide/Ultra-2 SCSI I/O Controller
south # lsdev -C -c adapter | grep scsi
scsi0   Available 11-08    Wide/Ultra-2 SCSI I/O Controller
scsi1   Available 11-09    Wide/Ultra-2 SCSI I/O Controller
```

2 Verify the SCSI ID of each adapter:

```
north # lsattr -E -l scsi0 -a id
id 7 Adapter card SCSI ID True
north # lsattr -E -l scsi1 -a id
id 7 Adapter card SCSI ID True
south # lsattr -E -l scsi0 -a id
id 7 Adapter card SCSI ID True
south # lsattr -E -l scsi1 -a id
id 7 Adapter card SCSI ID True
```

3 If necessary, change the SCSI identifier on each system so that it is unique:

```
south # chdev -P -l scsi0 -a id=5
scsi0 changed
south # chdev -P -l scsi1 -a id=5
scsi1 changed
```

4 Shut down all systems in the cluster.

5 Cable the shared storage as illustrated in Figure 2-1.

6 Restart each system. After all systems have booted, use the `lspv` command to verify that each system can see all shared devices needed by the application.

Setting up Fibre Channel

Perform the following steps to set up Fibre Channel.

To set up Fibre Channel

1 Connect the Fibre Channel adapters 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.

2 Reboot each system:

```
shutdown -Fr
```

3 After all systems have booted, use the `lspv` command to verify that each system can see all shared devices needed by the application.

Prerequisites for Veritas Storage Foundation Cluster File System

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 SFCFS:

- 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.

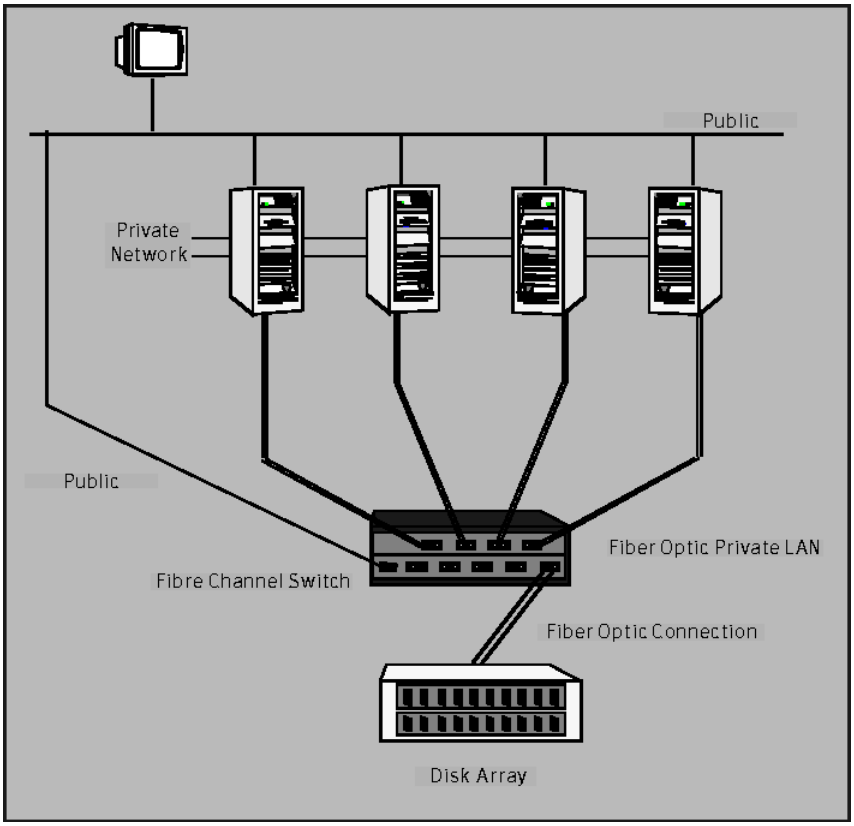
- Symantec recommends configuring the cluster with I/O fencing enabled. I/O fencing requires shared devices to support SCSI-3 Persistent Reservations (PR). Enabling I/O fencing prevents data corruption caused by a split brain scenario.
  The Veritas Storage Foundation Cluster File System is supported without I/O fencing enabled. However, without I/O fencing enabled, split brain scenarios can result in data corruption.

Hardware overview and requirements for Veritas Storage Foundation Cluster File System

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, SFCFS can be used in conjunction with the latest Veritas Storage Area Network (SAN) applications to provide a complete data storage and retrieval solution.

Figure 2-2 shows the configuration of a cluster file system on a Fibre Channel fabric with a disk array.

Figure 2-2 Four Node SFCFS 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.

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.

Chapter 3

System requirements

This chapter includes the following topics:

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://www.symantec.com/docs/TECH74012

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 42.
- CP servers
  See "CP server requirements" on page 43.

If you have installed Storage Foundation Cluster File System in a virtual environment that is not SCSI-3 PR compliant, review the requirements to configure non-SCSI3 server-based fencing.

See "Non-SCSI3 I/O fencing requirements" on page 46.

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

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

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 *Veritas Storage Foundation Cluster File System Administrator's Guide*.

Non-SCSI3 I/O fencing requirements

Supported virtual environment for non-SCSI3 fencing:

- VMware Server ESX 3.5 and 4.0 on AMD Opteron or Intel Xeon EM64T (x86_64)

  Guest operating system:

  - Red Hat Enterprise Linux 5 (RHEL5) with Update 3 (2.6.18-194.el5 kernel) or later
  - SUSE Linux Enterprise Server 10 (SLES10) with SP3 (2.6.16.60-0.54.5 kernel) or later
  - SUSE Linux Enterprise Server 11 (SLES11) with SP1 (2.6.32.12-0.7 kernel) or later

- IBM P Server LPARs with VIOS running
  Guest operating system: AIX 5.3 or 6.1

Make sure that you also meet the following requirements to configure non-SCSI3 fencing in the virtual environments that do not support SCSI-3 PR:

- Storage Foundation Cluster File System must be configured with Cluster attribute UseFence set to SCSI3
- All coordination points must be CP servers

Supported AIX operating systems

This section lists the supported operating systems for this release of Veritas products.

Product installation scripts verify the required update levels. The installation process terminates if the target systems do not meet the maintenance level requirements.

The minimum system requirements for this release are as follows:

For Power 6 or earlier processors at one of the following levels:

- AIX 6.1 TL2 or later
- AIX 5.3 at one of the following levels:
  - TL7 with SP6 or later
  - TL8 with SP4 or later

For Power 7 processors at one of the following levels:

- AIX 6.1 TL5 with Service Pack 1 or later

- AIX Version 5.3 executing in POWER6 or POWER6+ compatibility at the following levels:
  - TL11 with Service Pack 2 or later
  - TL10 with Service Pack 4 or later

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

http://entsupport.symantec.com/docs/334998

Memory requirements

2 GB of memory is required for Veritas Storage Foundation Cluster File System.

CPU requirements

A minimum of 2 CPUs is required for Veritas Storage Foundation Cluster File System.

Node requirements

All nodes in a Cluster File System must have the same operating system version and update level.

Database requirements

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

http://entsupport.symantec.com/docs/331625

Note: SFCFS does not support running SFDB tools with DB2 and Sybase.

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
```

Number of nodes supported

SFCFS is capable of supporting cluster configurations with up to 64 nodes. Symantec has tested and qualified configurations of up to 32 nodes at the time of the release.

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

http://entsupport.symantec.com/docs/334998

Chapter 4

Licensing Veritas products

This chapter includes the following topics:

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 50.
  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 52.
  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.

```
# vkeyless -v display
```

2 View the possible settings for the product level.

```
# vkeyless displayall
```

3 Set the desired product level.

```
# vkeyless -q set prod_levels
```

where *prod_levels* is a comma-separated list of keywords.

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.

```
# vkeyless [-v] display
```

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

```
# vkeyless [-q] set NONE
```

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

Installing Veritas product license keys

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

vxlicinst	Installs a license key for a Symantec product
vxlicrep	Displays currently installed licenses
vxlictest	Identifies whether a Symantec product feature is licensed on the system

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
```

Section 2

Installation of Storage Foundation Cluster File System

Chapter 5

Installing Storage Foundation Cluster File System using the common product installer

This chapter includes the following topics:

Installation preparation overview

Table 5-1 provides an overview of an installation using the product installer.

Table 5-1 Installation overview

Installation task	Section
Obtain product licenses.	See "About Veritas product licensing" on page 49.

Table 5-1 Installation overview *(continued)*

Installation task	Section
Download the software, or insert the product DVD.	See "Downloading the Veritas Storage Foundation Cluster File System software" on page 32. See "Mounting the product disc" on page 56.
Set environment variables.	See "Setting environment variables" on page 33.
Configure the secure shell (ssh) on all nodes.	See "About configuring secure shell or remote shell communication modes before installing products" on page 411.
Verify that hardware, software, and operating system requirements are met.	See "Supported AIX operating systems" on page 46. See "Release notes" on page 41.
Check that sufficient disk space is available.	See "Disk space requirements" on page 47.
Use the installer to install the products.	See "About the Veritas installer" on page 57.

Mounting the product disc

You must have superuser (root) privileges to load the SFCFS software.

To mount the product disc

1 Log in as superuser on a system where you want to install SFCFS.

The system from which you install SFCFS need not be part of the cluster. The systems must be in the same subnet.

2 Determine the device access name of the disc drive. For example, enter:

```
# lsdev -C -c cdrom
```

The output resembles:

```
cd0 Available 1G-19-00 IDE DVD-ROM Drive
```

In this example, cd0 is the disc's device access name.

3 Make sure the /cdrom file system is created:

```
# cat /etc/filesystems
```

If the /cdrom file system exists, the output contains a listing that resembles:

```
.
.
/cdrom:
dev = /dev/cd0
vfs = cdrfs
mount = false
options = ro
account = false
.
.
```

4 If the /cdrom file system does not exist, create it:

```
# crfs -v cdrfs -p ro -d cd0 -m /cdrom
```

5 Insert the product disc with the SFCFS software into a drive that is connected to the system.

6 Mount the disc:

```
# mount /cdrom
# cd /cdrom
```

About the Veritas installer

The installer also enables you to configure the product, verify preinstallation requirements, and view the product's description.

If you obtained a standalone Veritas product from an electronic download site, the single-product download files do not contain the general product installer. Use the product installation script to install the product.

See "About installation scripts" on page 375.

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

- Use `b` (back) to return to a previous section of the installation procedure. The back feature of the installation scripts is context-sensitive, so it returns to the beginning of a grouped section of questions.

- Use `Control-c` to stop and exit the program if an installation procedure hangs. After a short delay, the script exits.
- Use `q` to quit the installer.
- Use `?` to display help information.
- Use the Enter button to accept a default response.

Additional options are available for the installer.

See "Installation script options" on page 376.

Installing Storage Foundation Cluster File System using the product installer

The product installer is the recommended method to license and install Storage Foundation Cluster File System or Storage Foundation Cluster File System HA.

Note: Save a copy of `/var/adm/ras/errtmplt` and `/etc/trcfmt` files before you install the product. If the packages fail to install due to the `template file is corrupted` error message, replace `/var/adm/ras/errtmplt` and `/etc/trcfmt` files with the ones that you had saved. Uninstall all the packages you installed and reinstall.

See "Uninstalling Storage Foundation Cluster File System" on page 366.

The following sample procedure is based on the installation of a Veritas Storage Foundation Cluster File System HA cluster with two nodes: "host1" and "host2" If you are installing on standalone systems only, some steps are unnecessary, and these are indicated.

Default responses are enclosed by parentheses. Press Return to accept defaults.

Note: If you have obtained a Veritas product from an electronic download site, the single product download files do not contain the `installer` installation script, so you must use the product installation script to install the product. For example, if you download Veritas Cluster File System, use the `installsfcfs` script instead of the `installer` script.

To install Storage Foundation Cluster File System products

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

   See "About configuring secure shell or remote shell communication modes before installing products" on page 411.

2. Load and mount the software disc.

3. Move to the top-level directory on the disc.

   ```
   # cd /dvd_mount
   ```

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

   ```
   # ./installer
   ```

5. Enter `I` to install and press Return.

6. From the Installation menu, choose the `I` option for Install and enter the number for Storage Foundation Cluster File System or Storage Foundation Cluster File System HA. Press Return.

   Do not select the "Storage Foundation for Oracle RAC" option unless you have the correct license and setup.

   The example installation assumes you have selected SFCFS HA.

7. At the prompt, specify whether you accept the terms of the End User License Agreement (EULA).

   ```
   Do you agree with the terms of the End User License Agreement as
   specified in the
   storage_foundation_cluster_file_system/EULA/lang/EULA_CFS_Ux_5.1SP1.pdf
   file present

   on the media? [y,n,q,?] y
   ```

8. Select from one of the following install options:

   - Minimal filesets: installs only the basic functionality for the selected product.
   - Recommended filesets: installs the full feature set without optional filesets.
   - All filesets: installs all available filesets.

Each option displays the disk space that is required for installation. Select which option you want to install and press Return.

9 You are prompted to enter the system names (in the following example, "host1" and "host2") on which the software is to be installed. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces:[q?] (host1 host2)
```

10 During the initial system check, the installer verifies that communication between systems has been set up.

If the installer hangs or asks for a login password, stop the installer and set up ssh or rsh. Then run the installer again.

See "About configuring secure shell or remote shell communication modes before installing products" on page 411.

11 After the system checks complete, the installer displays a list of the filesets that will be installed. Press Enter to continue with the installation.

12 You are prompted to choose your licensing method.

```
To ensure compliance 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 (see http://go.symantec.com/vom for
details and free download)

     1)  Enter a valid license key
     2)  Enable keyless licensing

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

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

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

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

Keyless licensing requires that you manage the systems with a Management Server.Refer to the following URL for details:

http://go.symantec.com/vom

13 You are prompted to enter the Standard or Enterprise product mode.

```
Storage Foundation and High Availability Solutions 5.1 Install Program

     1)  SFCFS Standard HA
     2)  SFCFS Enterprise HA
     b)  Back to previous menu

Select product mode to install: [1-2,b,q,?] (1) 1
```

14 Select **yes** to enable the Veritas Volume Replicator.

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

15 Select **yes** to enable the Global Cluster Option.

```
Would you like to enable Global Cluster option?  [y,n,q] (n) y
```

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

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

17 The product installation completes.

Configure Storage Foundation Cluster File System when prompted.

```
Do you want to configure Storage Foundation Cluster File System on
these systems at this time? [y,n,q] (y) y
```

If you select **y** to configure now, respond to the prompts to configure the cluster.

18 If you select **n** to configure, the installation completes.

Note: You must configure Storage Foundation Cluster File System before you can use the product.

---

19 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-****
```

Chapter 6

Installing Storage Foundation Cluster File System using the web-based installer

This chapter includes the following topics:

About the Web-based installer

Use the Web-based installer's interface to install Veritas products. The Web-based installer can perform most of the tasks that the script-based installer performs.

You use the `webinstaller` script to start and stop the Veritas XPortal Server `xprtlwid` process. The `webinstaller` script can also be used to check the status of the XPortal Server.

When the `webinstaller` script starts the `xprtlwid` process, the script displays a URL. Use this URL to access the Web-based installer from Internet Explorer or FireFox.

The Web installer creates log files whenever the Web installer is operating. While the installation processes are operating, the log files are located in a session-based directory under the `/var/tmp` directory. After the install process completes, the log files are located in the `/opt/VRTS/install/logs` directory. It is recommended that you keep the files for auditing, debugging, and for future use.

The location of the Veritas XPortal Server configuration file is `/var/opt/webinstaller/xprtlwid.conf`.

See "Before using the Veritas Web-based installer" on page 64.

See "Starting the Veritas Web-based installer" on page 65.

Features not supported with Web-based installer

In this release, the following features that can be performed using the script installer are not available in the Web-based installer:

- Configuring server-based I/O fencing
- Configuring non-SCSI3 I/O fencing in virtual environments where SCSI3 is not supported

Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

Table 6-1 Web-based installer requirements

System	Function	Requirements
Target system	The systems where you plan to install the Veritas products.	Must be a supported platform for Veritas Storage Foundation Cluster File System 5.1 SP1.
Installation server	The server where you start the installation. The installation media is accessible from the installation server.	Must use the same operating system as the target systems and must be at one of the supported operating system update levels.

Table 6-1 Web-based installer requirements *(continued)*

System	Function	Requirements
Administrative system	The system where you run the Web browser to perform the installation.	Must have a Web browser. Supported browsers: ■ Internet Explorer 6, and later. ■ Firefox 3.x, and later.

Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

To start the Web-based installer

1 Start the Veritas XPortal Server process `xprtlwid`, on the installation server:

```
# ./webinstaller start
```

The webinstaller script displays a URL. Note this URL.

Note: If you do not see the URL, run the command again.

2 On the administrative server, start the Web browser.

3 Navigate to the URL that the script displayed.

4 The browser may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

5 When prompted, enter `root` and root's password of the installation server.

Obtaining a security exception on Mozilla Firefox

You may need to get a security exception on Mozilla Firefox.

To obtain a security exception

1 Click **Or you can add an exception** link.

2 Click **Add Exception** button.

3 Click **Get Certificate** button.

4 Uncheck **Permanently Store this exception checkbox (recommended)**.

5 Click **Confirm Security Exception** button.

6 Enter root in User Name field and root password of the web server in the Password field.

Performing a pre-installation check with the Veritas Web-based installer

This section describes performing a pre-installation check with the Veritas Web-based installer.

To perform a pre-installation check

1 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 65.

2 On the Select a task and a product page, select **Perform a Pre-installation Check** from the **Task** drop-down list.

3 Select the product from the **Product** drop-down list, and click **Next**.

4 Indicate the systems on which to perform the precheck. Enter one or more system names, separated by spaces. Click **Validate**.

5 The installer performs the precheck and displays the results.

6 If the validation completes successfully, the installer prompts you to begin the installation. Click **Yes** to install on the selected system. Click **No** to install later.

7 Click **Finish**. The installer prompts you for another task.

Installing SFCFS with the Web-based installer

This section describes installing SFCFS with the Veritas Web-based installer.

To install SFCFS using the Web-based installer

1 Perform preliminary steps. See "Performing a pre-installation check with the Veritas Web-based installer" on page 66.

2 Select **Install a Product** from the **Task** drop-down list.

3 Select **Veritas Storage Foundation Cluster File System** from the Product drop-down list, and click **Next**.

4 On the License agreement page, read the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.

5 Choose minimal, recommended, or all filesets. 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 SFCFS or SFCFSHA on the selected system.

9 After the installation completes, you must choose your licensing method.

On the license page, select one of the following tabs:

- Keyless licensing

  Note: The keyless license option enables you to install without entering a key. However, in order to ensure compliance you must manage the systems with a management server.

  For more information, go to the following website:

  http://go.symantec.com/sfhakeyless

  Complete the following information:

  - Choose whether you want to enable Veritas Volume Replicator.

  Click **Register**.

- Enter license key
  If you have a valid license key, select this tab. Enter the license key for each system. Click **Register**.

10 The installer prompts you to configure the cluster. Select **Yes** to continue with configuring the product.

If you select **NO**, you can exit the installer. You must configure the product before you can use SFCFS.

After the installation completes, the installer displays the location of the log and summary files. If required, view the files to confirm the installation status.

11 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**.

Chapter 7

Installing Storage Foundation Cluster File System, other methods

This chapter includes the following topics:

Installing SFCFS using NIM and the installer

You can use the product installer in concert with NIM to install the Veritas product, or to install the operating system and the Veritas product.

The instructions in this section assume a working knowledge of the Network Installation Management process. See the operating system documentation for detailed information on Network Installation Management.

In the following samples, the LPP resource uses LPP-6100-up2date and its relevant SPOT resource is spot-6100-up2date.

Preparing the bundle and script resources on NIM server

You need to prepare the bundle and script resources on the NIM server before using NIM to install SFCFS filesets. The following actions are executed on the NIM server.

Note: Make sure that a NIM LPP_SOURCE is present on the NIM server.

To prepare the bundle and script resources

1. Insert and mount the installation media.
2. Choose an LPP source:

```
# lsnim |grep -i lpp_source
LPP-6100-up2date resources lpp_source
LPP-5300-up2date resources lpp_source
```

3. Navigate to the product directory on the disc and run the `installsfcfs` command to prepare the bundle and script resources:

```
# ./installsfcfs -nim LPP-6100-up2date
```

   The installation program copies the necessary filesets and patches to the LPP resource directory.

4. Enter a name for the bundle, for example *SFCS51SP1*.
5. Enter **y** to generate the NIM script resource for copying the Veritas installer and libraries after the installation.

```
Do you want to generate the NIM script resource? [y,n,q] (n) y
NIM script resource copy_cpi for copying installer scripts
to disk created successfully
```

   The script configure file is created at `/opt/VRTS/nim/copy_cpi`.

6 Run the `lsnim -l` command to check that the install_bundle resource is created successfully.

```
# lsnim -l SFCFS51SP1_bundle
SFCFS51SP1_bundle:
class = resources
type = installp_bundle
Rstate = ready for use
prev_state = unavailable for use
location = /opt/VRTS/nim/SFCFS51SP1.bnd
alloc_count = 0
server = master
```

7 Verify that the script resource is created successfully:

```
# lsnim -l copy_cpi
copy_cpi:
class = resources
type = script
Rstate = ready for use
prev_state = unavailable for use
location = /opt/VRTS/nim/copy_cpi
alloc_count = 0
server = master
```

Installing SFCFS on the NIM client using SMIT

You can install SFCFS on the NIM client using the SMIT tool.

Perform these steps on each node to have SFCFS installed in a cluster.

To install SFCFS

1 On the NIM client, start smitty.

```
# smitty install
```

2 In the menu, select **Network Installation Management**.

3 In the menu, select **Perform NIM Software Installation and Maintenance Tasks**.

4 In the menu, select **Install Software Bundle**.

5 In the menu, select the LPP_SOURCE. In this example, specify **LPP-6100-up2date**.

6 In the menu, select the bundle, for example, **SFCFS51SP1_bundle**.

7 For the customization script that you want to run after installation, specify **copy_cpi**.

8 For the installp flags, specify that the ACCEPT new license agreements flag has a **yes** value.

9 Press the Enter key to start the installation. Note that it may take some time to finish.

Installing SFCFS and the operating system on the NIM client using SMIT

You can install VCS and the operating system on the NIM client using the SMIT tool.

Perform these steps on each node to have SFCFS and AIX installed in a cluster.

To install SFCFS and the operating system

1 On the NIM server, start smitty for a NIM and operating system installation.

```
# smitty nim_bosinst
```

2 In the menu, select the stand-alone target.

3 In the menu, select **spot - Install a copy of a SPOT resource**.

4 In the menu, select the spot resource **spot-6100-up2date**.

5 In the menu, select the LPP_SOURCE. In this example, select **LPP-6100-up2date**.

6 In the menu, select the following options:

- For the Customization SCRIPT to run after installation option, specify **copy_cpi**.
- For the ACCEPT new license agreements option, specify **yes**.

7 For the installp flags, specify that the ACCEPT new license agreements flag has a **yes** value.

Section 3

Configuration of Veritas Storage Foundation Cluster File System

Chapter 8

Preparing to configure SFCFS

This chapter includes the following topics:

Preparing to configure the clusters in secure mode

You can set up Symantec Product Authentication Service (AT) for the cluster during or after the Storage Foundation Cluster File System configuration.

In a cluster that is online, if you want to enable or disable AT using the `installsfcfs -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 79.
- 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 80.
- 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 8-1 depicts the flow of configuring Storage Foundation Cluster File System cluster in secure mode.

Figure 8-1 Workflow to configure Storage Foundation Cluster File System cluster in secure mode

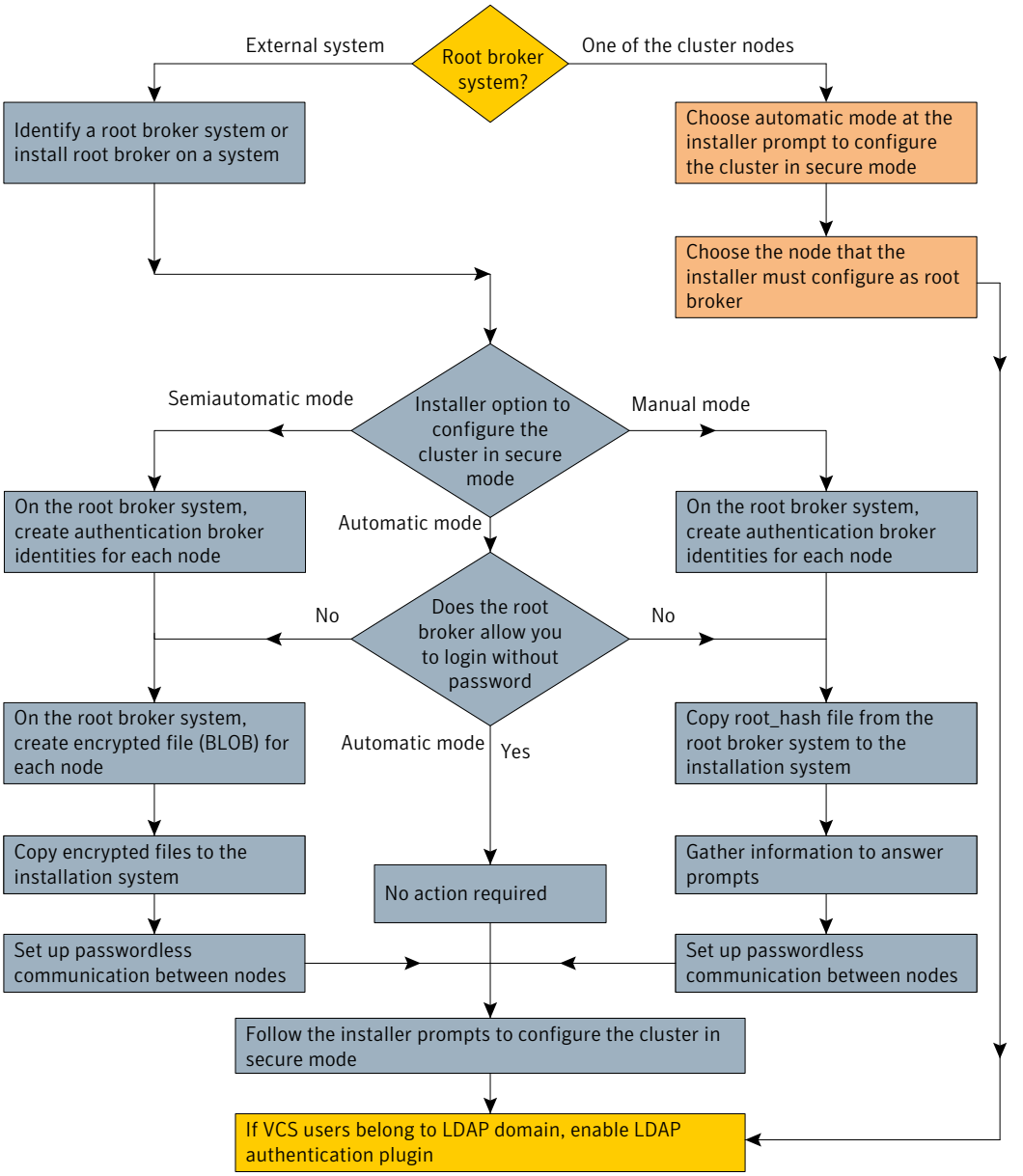


Table 8-1 lists the preparatory tasks in the order which the AT and VCS administrators must perform. These preparatory tasks apply only when you use an external root broker system for the cluster.

Table 8-1 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 79.	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 80. The 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 81. The 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 8-1 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 Storage Foundation Cluster File System. See "Preparing the installation system for the security infrastructure" on page 83.	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 Storage Foundation Cluster File System. 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
- Checks if the filesets are already on the system.

The installer lists the filesets 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 a mode 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 SFCFS.

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 80.

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 80.

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 SFCFS configuration, choose the configuration option 1 when the installsfcfs 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 SFCFS configuration, choose the configuration option 2 when the installsfcfs 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 SFCFS configuration, choose the configuration option 3 when the installsfcfs prompts.

About configuring SFCFS clusters for data integrity

When a node fails, SFCFS 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 a corrective action would cause a split-brain situation.

Some 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. SFCFS 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 SFCFS, you must configure I/O fencing in SFCFS to ensure data integrity.

See "About planning to configure I/O fencing" on page 90.

About I/O fencing for Storage Foundation Cluster File System in virtual machines that do not support SCSI-3 PR

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

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

In virtualized environments that do not support SCSI-3 PR, Storage Foundation Cluster File System attempts to provide reasonable safety for the data disks. Storage Foundation Cluster File System requires you to configure non-SCSI3 server-based I/O fencing in such environments. Non-SCSI3 fencing uses CP servers as coordination points with some additional configuration changes to support I/O fencing in such environments.

See "Setting up non-SCSI3 server-based I/O fencing using installsfcfs" on page 166.

See "Setting up non-SCSI3 fencing in virtual environments manually" on page 178.

About I/O fencing components

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

- Data disks—Store shared data
  See "About data disks" on page 86.
- Coordination points—Act as a global lock during membership changes
  See "About coordination points" on page 86.

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 be disks, 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 SFCFS 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 activeSFCFS 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 *Veritas Storage Foundation Cluster File System Administrator's Guide* for more details.

See "Enabling or disabling the preferred fencing policy" on page 182.

About I/O fencing configuration files

Table 8-2 lists the I/O fencing configuration files.

Table 8-2 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 Storage Foundation Cluster File System configuration.
/etc/vxfendg	This file includes the coordinator disk group information. This file is not applicable for server-based fencing.

Table 8-2 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 Storage Foundation Cluster File System 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 8-2 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:
	`/dev/rhdisk75`
	`/dev/rhdisk76`
	`/dev/rhdisk77`
	■ DMP disk:
	`/dev/vx/rdmp/rhdisk75`
	`/dev/vx/rdmp/rhdisk76`
	`/dev/vx/rdmp/rhdisk77`
	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 Storage Foundation Cluster File System 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.

If you have installed Storage Foundation Cluster File System in a virtual environment that is not SCSI-3 PR compliant, you can configure non-SCSI3 server-based fencing.

See Figure 8-3 on page 93.

Figure 8-2 illustrates a high-level flowchart to configure I/O fencing for the Storage Foundation Cluster File System cluster.

Figure 8-2 Workflow to configure I/O fencing

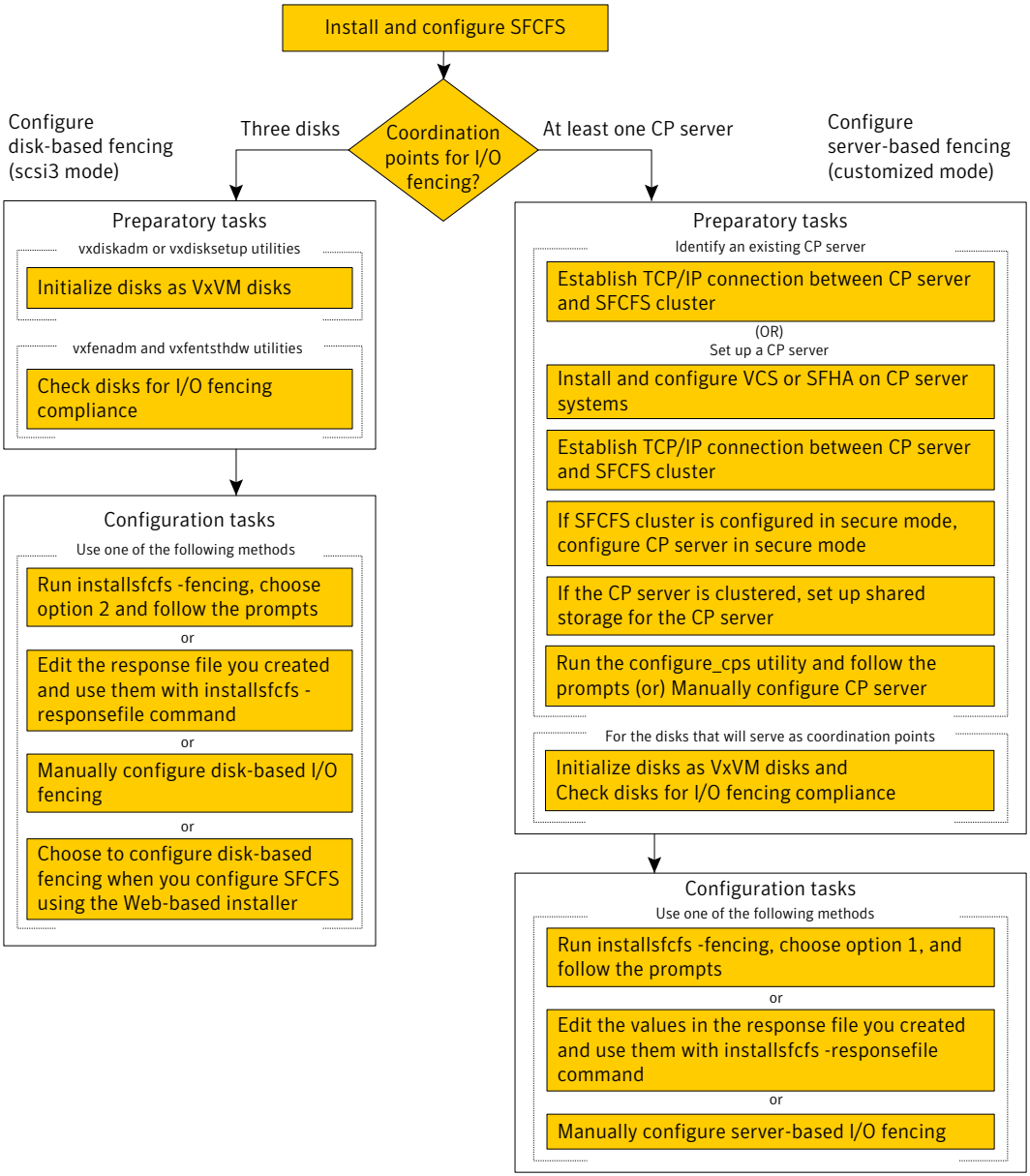
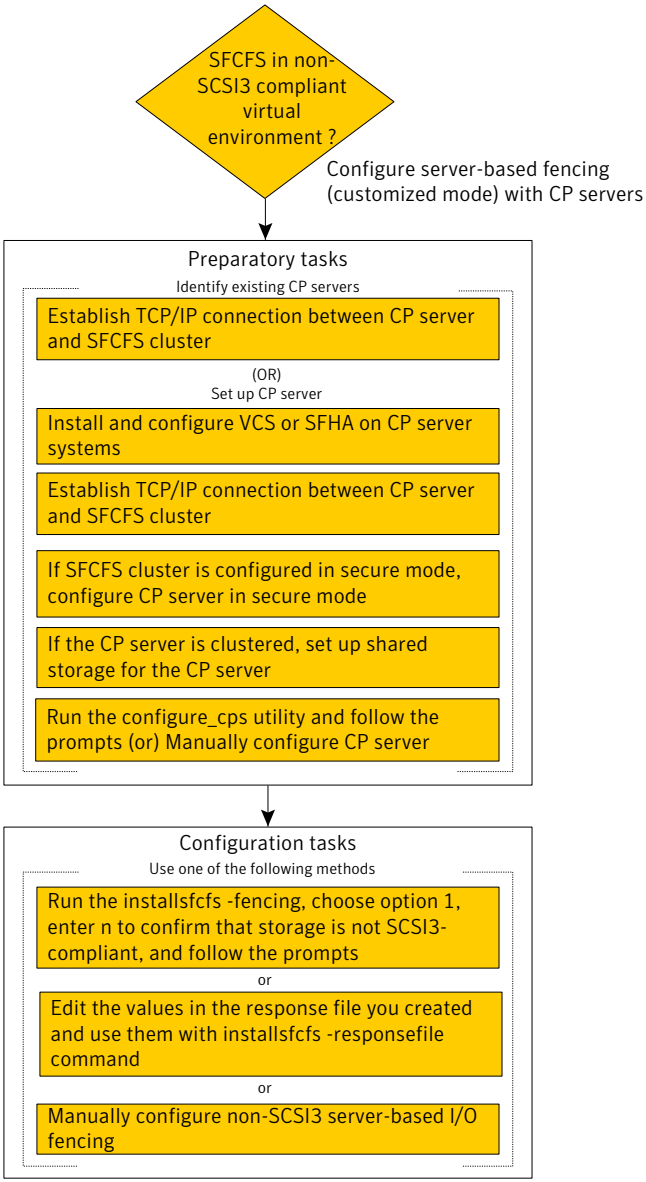


Figure 8-3 illustrates a high-level flowchart to configure non-SCSI3 server-based I/O fencing for the Storage Foundation Cluster File System cluster in virtual environments that do not support SCSI-3 PR.

Figure 8-3 Workflow to configure non-SCSI3 server-based I/O fencing



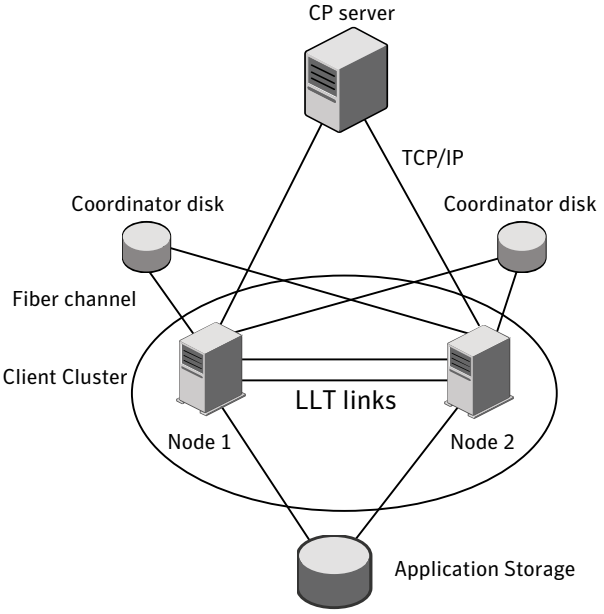
After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:

Using the installsfcfs	See "Setting up disk-based I/O fencing using installsfcfs" on page 141. See "Setting up server-based I/O fencing using installsfcfs" on page 154. See "Setting up non-SCSI3 server-based I/O fencing using installsfcfs" on page 166.
Using the Web-based installer **Note:** The Web-based installer supports only the disk-based fencing configuration.	See "Configuring Storage Foundation Cluster File System using the Web-based installer" on page 133.
Using response files	See "Response file variables to configure disk-based I/O fencing" on page 402. See "Response file variables to configure server-based I/O fencing" on page 404. See "Response file variables to configure server-based I/O fencing" on page 404. See "Configuring I/O fencing using response files" on page 401.
Manually editing configuration files	See "Setting up disk-based I/O fencing manually" on page 149. See "Setting up server-based I/O fencing manually" on page 166. See "Setting up non-SCSI3 fencing in virtual environments manually" on page 178.

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

Figure 8-4 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 8-4 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 8-5 on page 96.
- Multiple application clusters use a single CP server and multiple pairs of coordinator disks (two) as their coordination points.
  See Figure 8-6 on page 97.
- 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 8-7 on page 97.

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 8-5 displays a configuration using three CP servers that are connected to multiple application clusters.

Figure 8-5 Three CP servers connecting to multiple application clusters

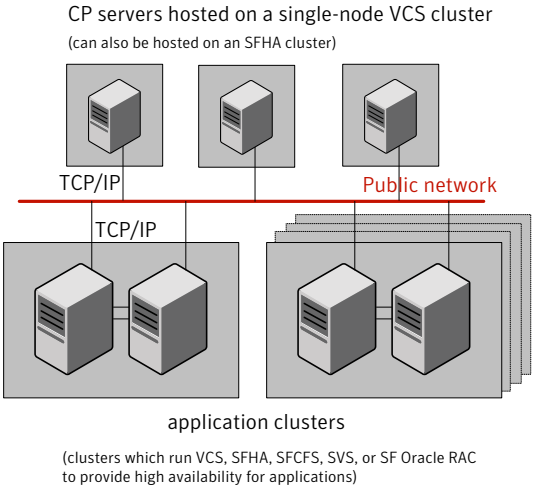


Figure 8-6 displays a configuration using a single CP server that is connected to multiple application clusters with each application cluster also using two coordinator disks.

Figure 8-6 Single CP server with two coordinator disks for each application cluster

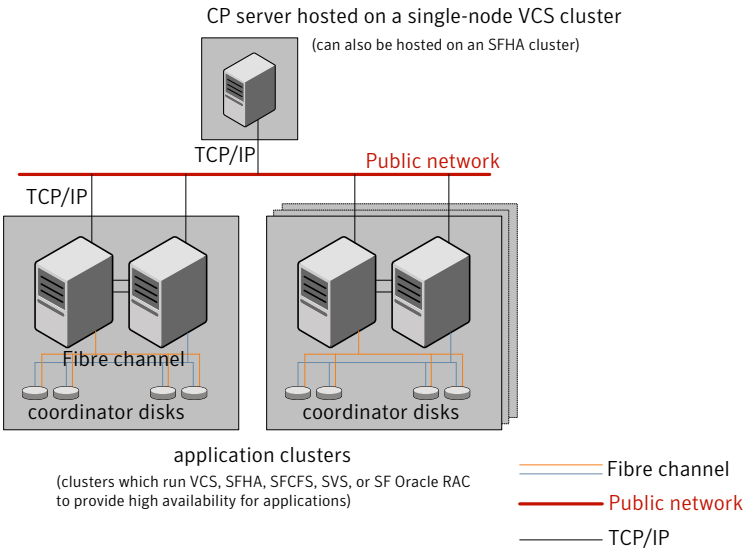
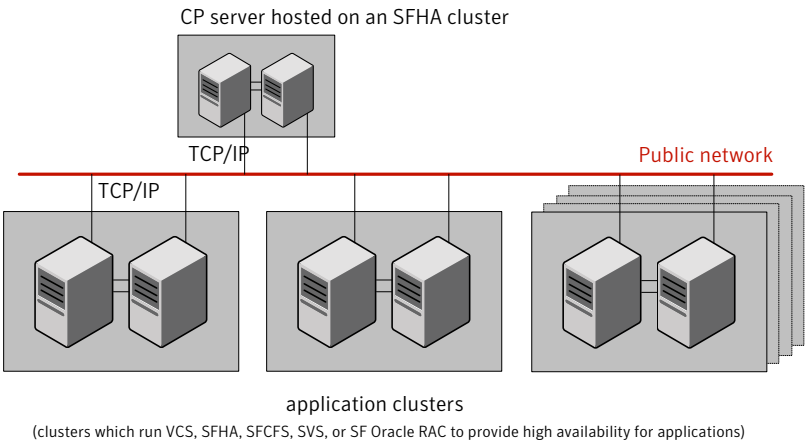


Figure 8-7 displays a configuration using a single CP server that is connected to multiple application clusters.

Figure 8-7 Single CP server connecting to multiple application clusters



See "Configuration diagrams for setting up server-based I/O fencing" on page 473.

Setting up the CP server

Table 8-3 lists the tasks to set up the CP server for server-based I/O fencing.

Table 8-3 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 98.
Install the CP server	See "Installing the CP server using the installer" on page 99.
Configure the CP server cluster in secure mode	See "Configuring the CP server cluster in secure mode" on page 100.
Set up shared storage for the CP server database	See "Setting up shared storage for the CP server database" on page 101.
Configure the CP server	See " Configuring the CP server using the configuration utility" on page 102. See "Configuring the CP server manually" on page 110.
Verify the CP server configuration	See "Verifying the CP server configuration" on page 111.

Planning your CP server setup

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

To plan your CP server setup

1. Decide whether you want to host the CP server on a single-node VCS cluster, or on an SFHA cluster.

   Symantec recommends hosting the CP server on an SFHA cluster.

2. If you host the CP server on an SFHA cluster, review the following information. Make sure you make the decisions and meet these prerequisites when you set up the CP server:

   - You must 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 43.

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 filesets for installation. The VRTScps fileset is installed only if you select to install all filesets.
- 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 102.

See "Configuring the CP server manually" on page 110.

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 filesets for installation. The VRTScps fileset is installed only if you select to install all filesets.
- 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 75.
- 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, you can 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:

  ```
  # installsfcfs -security
  ```

  See "Preparing to configure the clusters in secure mode" on page 75.

Setting 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.

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

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 fileset.

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 102.
For CP servers on an SFHA cluster:	See "To configure the CP server on an SFHA cluster" on page 106.

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

1 Verify that the VRTScps fileset 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: en0
```

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 en0 on
system mycps1? [y/n] : y
Enter a valid IP address to configure NetworkHosts for NIC en0 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 vxcpserv process and other resources to the VCS configuration in the CP server service group (CPSSG).

For information about the CPSSG, refer to the *Veritas Storage Foundation Cluster File System Administrator's Guide*.

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

To configure the CP server on an SFHA cluster

1 Verify that the VRTScps fileset 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 : en0
```

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 en0 on
system mycps1? [y/n] : y
Enter a valid IP address to configure NetworkHosts for NIC en0 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 vxcpserv process and other resources to the VCS configuration in the CP server service group (CPSSG).

For information about the CPSSG, refer to the *Veritas Storage Foundation Cluster File System Administrator's Guide*.

In addition, the main.cf samples contain details about the vxcpserv 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.

```
# hastart
```

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

```
# hagrp -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 vxcpserv 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.

Chapter 9

Configuring Veritas Storage Foundation Cluster File System

This chapter includes the following topics:

Configuring Veritas Storage Foundation Cluster File System using the script-based installer

Overview of tasks to configure Storage Foundation Cluster File System using the script-based installer

Overview of tasks to configure Storage Foundation Cluster File System using the script-based installer lists the tasks that are involved in configuring Storage Foundation Cluster File System using the script-based installer.

Table 9-1 Tasks to configure Storage Foundation Cluster File System using the script-based installer

Task	Reference
Start the software configuration	See "Starting the software configuration" on page 114.
Specify the systems where you want to configure Storage Foundation Cluster File System	See "Specifying systems for configuration" on page 115.
Configure the basic cluster	See "Configuring the cluster name and ID" on page 116. See "Configuring private heartbeat links" on page 116.
Configure virtual IP address of the cluster (optional)	See "Configuring the virtual IP of the cluster" on page 119.
Configure the cluster in secure mode (optional)	See "Configuring the cluster in secure mode" on page 121.
Add VCS users (required if you did not configure the cluster in secure mode)	See "Adding VCS users" on page 125.
Configure SMTP email notification (optional)	See "Configuring SMTP email notification" on page 125.
Configure SNMP email notification (optional)	See "Configuring SNMP trap notification" on page 127.
Complete the software configuration	See "Completing the VCS configuration" on page 130.

Starting the software configuration

You can configure Storage Foundation Cluster File System using the Veritas product installer or the installsfcfs.

To configure Storage Foundation Cluster File System 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 Storage Foundation Cluster File System using the installsfcfs program

1. Confirm that you are logged in as the superuser.
2. Start the installsfcfs program.

   ```
   # /opt/VRTS/install/installsfcfs -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 Storage Foundation Cluster File System. 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 Storage Foundation Cluster File System.

   ```
   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
- Checks whether Storage Foundation Cluster File System is installed
- Exits if Veritas Storage Foundation Cluster File System 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 90.

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.

See "Using the UDP layer for LLT" on page 489.

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).

  You must not enter the network interface card that is used for the public network (typically en0.)

```
Enter the NIC for the first private heartbeat NIC on galaxy:
[b,q,?] en2
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,?] en3
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: en0
Enter the NIC for Virtual IP of the Cluster to use on galaxy:
[b,q,?](en0)
```

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 en0 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)
  ```

- Enter the NetworkHosts IP addresses that are separated with spaces for checking the connections.

  ```
  Enter the NetworkHosts IP addresses, separated
  by spaces: [b,q,?] 192.168.1.17
  ```

- Verify and confirm the Cluster Virtual IP information.

  ```
  Cluster Virtual IP verification:

        NIC: en0
        IP: 192.168.1.16
        Netmask: 255.255.240.0

        NetworkHosts: 192.168.1.17

  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
  ```

- Enter the NetworkHosts IP addresses that are separated with spaces for checking the connections.

  ```
  Enter the NetworkHosts IP addresses, separated
  by spaces: [b,q,?] 2001:db8::1 2001:db8::2
  ```

- Verify and confirm the Cluster Virtual IP information.

  ```
  Cluster Virtual IP verification:

        NIC: en0
        IP: 2001:454e:205a:110:203:baff:feee:10
        Prefix: 64

        NetworkHosts: 2001:db8::1 2001:db8::2

  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 75.

To configure the cluster in secure mode

1 Choose whether to configure Storage Foundation Cluster File System 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 125.

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 127.
3. Provide information to configure SMTP notification.

   Provide the following information:

   - Enter the NIC information.

     ```
     Active NIC devices discovered on galaxy: en0
     Enter the NIC for the VCS Notifier to use on galaxy:
     [b,q,?] (en0)
     Is en0 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: en0

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 129.

3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on galaxy: en0
Enter the NIC for the VCS Notifier to use on galaxy:
[b,q,?] (en0)
Is en0 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: en0

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 *Veritas Storage Foundation Cluster File System Installation Guide* for instructions to set up Storage Foundation Cluster File System 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, value for the netmask, and value for the network hosts.

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: en0
      IP: 192.168.1.16
      Netmask: 255.255.240.0

      NetworkHosts: 192.168.1.17

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

For IPv6

```
Global Cluster Option configuration verification:

      NIC: en0
      IP: 2001:454e:205a:110:203:baff:feee:10
      Prefix: 64

      NetworkHosts: 2001:db8::1 2001:db8::2

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

Completing the VCS configuration

After you enter the Storage Foundation Cluster File System 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 Storage Foundation Cluster File System and its related processes.

If you chose to configure the cluster in secure mode, the installer then does the following before it starts Storage Foundation Cluster File System 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 Storage Foundation Cluster File System 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 Storage Foundation Cluster File System 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 Storage Foundation Cluster File System successfully, note the location of summary, log, and response files that installer creates.

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

summary file	Describes the cluster and its configured resources.
log file	Details the entire configuration.
response file	Contains the configuration information that can be used to perform secure or unattended installations on other systems. See "Configuring SFCFS using response files" on page 384.

Verifying and updating licenses on the system

After you install Storage Foundation Cluster File System, 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 132.

See "Updating product licenses using vxlicinst" on page 132.

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 Storage Foundation Cluster File System license key on each node. If you have Storage Foundation Cluster File System already installed and configured and you use a demo license, you can replace the demo license.

See "Replacing a Storage Foundation Cluster File System demo license with a permanent license" on page 133.

To update product licenses

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

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

Replacing a Storage Foundation Cluster File System demo license with a permanent license

When a Storage Foundation Cluster File System 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 Storage Foundation Cluster File System on all nodes in the cluster:

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

   This command does not shut down any running applications.
3. Enter the permanent license key using the following command on each node:

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

4. Make sure demo licenses are replaced on all cluster nodes before starting Storage Foundation Cluster File System.

   ```
   # vxlicrep
   ```

5. Start Storage Foundation Cluster File System on each node:

   ```
   # hastart
   ```

Configuring Storage Foundation Cluster File System using the Web-based installer

Before you begin to configure Storage Foundation Cluster File System using the Web-based installer, review the configuration requirements.

By default, the communication between the systems is selected as SSH. If SSH is used for communication between systems, the SSH commands execute without prompting for passwords or confirmations.

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 Storage Foundation Cluster File System on a cluster

1 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 65.

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

Task	Configure a Product
Product	Storage Foundation for Cluster File System or Storage Foundation for Cluster File System/HA

Click **Next**.

3 On the Select Systems page, enter the system names where you want to configure Storage Foundation Cluster File System, 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 `installsfcfs -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 To configure Storage Foundation Cluster File System on a cluster. 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 `installsfcfs -security` command. Go to step To configure Storage Foundation Cluster File System on a cluster.

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 Storage Foundation Cluster File System.
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.

See the *Veritas Storage Foundation Cluster File System Installation Guide* for instructions to set up SFCFS global clusters.

- 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 To configure Storage Foundation Cluster File System on a cluster, then skip to step To configure Storage Foundation Cluster File System on a cluster. Go to step To configure Storage Foundation Cluster File System on a cluster 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 To configure Storage Foundation Cluster File System on a cluster. ■ 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 To configure Storage Foundation Cluster File System on a cluster.

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 Storage Foundation Cluster File System.

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.

Configuring Veritas Storage Foundation Cluster File System manually

You can manually configure different products within Veritas Storage Foundation Cluster File System.

Configuring Veritas File System

After installing Veritas File System, you can create a file system on a disk slice or Veritas Volume Manager volume with the `mkfs` command. Before you can use this file system, you must mount it with the `mount` command. You can unmount the file system later with the `umount` command. A file system can be automatically mounted at system boot time if you add an entry for it in the following file:

```
/etc/filesystems
```

The Veritas-specific commands are described in the Veritas File System guides and online manual pages.

See the *Veritas File System Administrator's Guide*.

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 SFCFS and Oracle. For SFDB repository set up procedures:

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

Chapter 10

Configuring SFCFS for data integrity

This chapter includes the following topics:

Setting up disk-based I/O fencing using installsfcfs

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

Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

To initialize disks as VxVM disks

1 Scan for the new hdisk devices.

```
# /usr/sbin/cfgmgr
```

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

```
# lsdev -Cc disk
```

3 Determine the VxVM name by which a disk drive (or LUN) is known.

In the following example, VxVM identifies a disk with the AIX device name /dev/rhdisk75 as EMC0_17:

```
# vxdmpadm getdmpnode nodename=hdisk75
NAME     STATE    ENCLR-TYPE   PATHS    ENBL    DSBL    ENCLR-NAME
============================================================
EMC0_17  ENABLED  EMC          1        1       0       EMC0
Notice that in the example command, the AIX device name for
the block device was used.
```

As an option, you can run the command `vxdisk list` *vxvm_device_name* to see additional information about the disk like the AIX device name. For example:

```
# vxdisk list EMC0_17
```

4 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 EMC0_17
  ```

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

Configuring disk-based I/O fencing using installsfcfs

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

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

1 Start the installsfcfs with `-fencing` option.

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

The installsfcfs 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 Storage Foundation Cluster File System 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 vxfentsthdw utility and then return to this configuration program.

See "Checking shared disks for I/O fencing" on page 145.

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 Storage Foundation Cluster File System 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 175.

Checking shared disks for I/O fencing

Make sure that the shared storage you set up while preparing to configure SFCFS meets the I/O fencing requirements. You can test the shared disks using the vxfentsthdw 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.

You can use the vxfentsthdw utility to test disks either in DMP format or in raw format.

- If you test disks in DMP format, use the VxVM command `vxdisk list` to get the DMP path name.
- If you test disks in raw format for Active/Passive disk arrays, you must use an active enabled path with the vxfentsthdw command. Run the `vxdmpadm getsubpaths dmpnodename=`*`enclosure-based_name`* command to list the active enabled paths.
  DMP opens the secondary (passive) paths with an exclusive flag in Active/Passive arrays. So, if you test the secondary (passive) raw paths of the disk, the vxfentsthdw command may fail due to DMP's exclusive flag.

The vxfentsthdw 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 *Veritas Storage Foundation Cluster File System 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 146.

- Verifying that nodes have access to the same disk
  See "Verifying that the nodes have access to the same disk" on page 147.
- Testing the shared disks for SCSI-3
  See "Testing the disks using vxfentsthdw utility" on page 147.

Verifying Array Support Library (ASL)

Make sure that the Array Support Library (ASL) for the array that you add is installed.

To verify Array Support Library (ASL)

1 If the Array Support Library (ASL) for the array that you add is not installed, obtain and install it on each node before proceeding.

The ASL for the supported storage device that you add is available from the disk array vendor or Symantec technical support.

2 Verify that the ASL for the disk array is installed on each of the nodes. Run the following command on each node and examine the output to verify the installation of ASL.

The following output is a sample:

```
# vxddladm listsupport all


LIBNAME             VID                 PID
============================================================
libvx3par.so        3PARdata            VV
libvxCLARiiON.so    DGC                 All
libvxFJTSYe6k.so    FUJITSU             E6000
libvxFJTSYe8k.so    FUJITSU             All
libvxcompellent.so  COMPELNT            Compellent Vol
libvxcopan.so       COPANSYS            8814, 8818
libvxddns2a.so      DDN                 S2A 9550, S2A 9900,
                                        S2A 9700
```

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 vxfentsthdw 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 SFCFS.
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
   ```

   For A/P arrays, run the `vxfentsthdw` command only on secondary paths.

   Refer to the `vxfenadm` (1M) manual page.

   For example, an EMC disk is accessible by the /dev/rhdisk75 path on node A and the /dev/rhdisk76 path on node B.

   From node A, enter:

   ```
   vxfenadm -i /dev/rhdisk75

   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/rhdisk76 path.

   On a disk from another manufacturer, Hitachi Data Systems, the output is different and may resemble:

   ```
   # vxfenadm -i /dev/rhdisk77

   Vendor id       : HITACHI
   Product id      : OPEN-3
   Revision        : 0117
   Serial Number   : 0401EB6F0002
   ```

Testing the disks using vxfentsthdw utility

This procedure uses the /dev/rhdisk75 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 vxfentsthdw utility indicates a disk can be used for I/O fencing with a message resembling:

```
The disk /dev/rhdisk75 is ready to be configured for I/O Fencing on
node galaxy
```

For more information on how to replace coordinator disks, refer to the *Veritas Storage Foundation Cluster File System Administrator's Guide*.

To test the disks using vxfentsthdw utility

1. Make sure system-to-system communication functions properly.

2. From one node, start the utility.

   Run the utility with the -n option if you use `rsh` for communication.

   ```
   # vxfentsthdw [-n]
   ```

3. The script warns that the tests overwrite data on the disks. After you review the overview and the warning, confirm to continue the process and enter the node names.

   Warning: The tests overwrite and destroy data on the disks unless you use the `-r` option.

   ```
   ******** WARNING!!!!!!!! ********
   THIS UTILITY WILL DESTROY THE DATA ON THE DISK!!

   Do you still want to continue : [y/n] (default: n) y
   Enter the first node of the cluster: 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/DiskXX
for raw: /dev/rhdiskXX
Make sure it's the same disk as seen by nodes
IP_adrs_ofgalaxy and IP_adrs_of_nebula
/dev/rhdisk75

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/DiskXX
for raw: /dev/rhdiskXX
Make sure it's the same disk as seen by nodes
IP_adrs_ofgalaxy and IP_adrs_of_nebula
 /dev/rhdisk75
```

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/rhdisk75 have PASSED
The disk is now ready to be configured for I/O Fencing on node
galaxy
```

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

Setting up disk-based I/O fencing manually

Table 10-1 lists the tasks that are involved in setting up I/O fencing.

Table 10-1 Tasks to set up I/O fencing manually

Task	Reference
Initializing disks as VxVM disks	See "Initializing disks as VxVM disks" on page 141.

Table 10-1 Tasks to set up I/O fencing manually *(continued)*

Task	Reference
Identifying disks to use as coordinator disks	See "Identifying disks to use as coordinator disks" on page 150.
Checking shared disks for I/O fencing	See "Checking shared disks for I/O fencing" on page 145.
Setting up coordinator disk groups	See "Setting up coordinator disk groups" on page 151.
Creating I/O fencing configuration files	See "Creating I/O fencing configuration files" on page 151.
Modifying Storage Foundation Cluster File System configuration to use I/O fencing	See "Modifying VCS configuration to use I/O fencing" on page 152.
Configuring Coordination Point agent to monitor coordination points	See "Configuring Coordination Point agent to monitor coordination points" on page 175.
Verifying I/O fencing configuration	See "Verifying I/O fencing configuration" on page 154.

Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See "Initializing disks as VxVM disks" on page 141.

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 145.

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 EMC0_12, EMC0_16, and EMC0_17.

To create the vxfencoorddg disk group

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

```
# vxdg init vxfencoorddg EMC0_12 EMC0_16 EMC0_17
```

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 "vxfencoorddg" > /etc/vxfendg
```

Do not use spaces between the quotes in the "vxfencoorddg" text.

This command creates the /etc/vxfendg file, which includes the name of the coordinator disk group.

2 On all cluster nodes depending on the SCSI-3 mechanism, type one of the following selections:

- For DMP configuration:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
```

- For raw device configuration:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_raw /etc/vxfenmode
```

3 To check the updated /etc/vxfenmode configuration, enter the following command on one of the nodes. For example:

```
# more /etc/vxfenmode
```

4 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.

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

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.

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

- 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 installsfcfs

If Storage Foundation Cluster File System 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 155.

See “Configuring server-based I/O fencing using the installsfcfs” on page 157.

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

After configuring security using the `installsfcfs -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.symantecexample.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.symantecexample.com

Domain Type:    vx

************************************

Domain Name:    broker@galaxy.symantecexample.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 installsfcfs

You can configure server-based I/O fencing for the Storage Foundation Cluster File System cluster using the installsfcfs.

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 90.

See "Recommended CP server configurations" on page 95.

This section covers the following example procedures:

Mix of CP servers and coordinator disks	See "To configure server-based fencing for the Storage Foundation Cluster File System cluster (one CP server and two coordinator disks)" on page 158.
Single CP server	See "To configure server-based fencing for the Storage Foundation Cluster File System cluster (single CP server)" on page 163.

To configure server-based fencing for the Storage Foundation Cluster File System 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 Storage Foundation Cluster File System cluster. The Storage Foundation Cluster File System cluster is also referred to as the application cluster or the client cluster.
  See "Setting up the CP server" on page 98.
- The coordination disks are verified for SCSI3-PR compliance.
  See "Checking shared disks for I/O fencing" on page 145.

2 Start the installsfcfs with `-fencing` option.

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

The installsfcfs 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 Storage Foundation Cluster File System 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 Storage Foundation Cluster File System (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) rhdisk75
2) rhdisk76
3) rhdisk77

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. rhdisk75
    2. rhdisk76
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 deports the disk group on the Storage Foundation Cluster File System (application cluster) node.

10 If the CP server is configured for security, the installer sets up secure communication between the CP server and the Storage Foundation Cluster File System (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 Storage Foundation Cluster File System (application cluster) nodes have already established trust with an AT root broker.
  - If the Storage Foundation Cluster File System (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 Storage Foundation Cluster File System (application cluster) nodes
    - Port number where the authentication broker for the Storage Foundation Cluster File System (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 88.

13 Configure the CP agent on the Storage Foundation Cluster File System (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 Storage Foundation Cluster File System cluster (single CP server)

1. Make sure that the CP server is configured and is reachable from the Storage Foundation Cluster File System cluster. The Storage Foundation Cluster File System cluster is also referred to as the application cluster or the client cluster.

   See "Setting up the CP server" on page 98.

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

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

   The installsfcfs 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 Storage Foundation Cluster File System 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 Storage Foundation Cluster File System (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 Storage Foundation Cluster File System (application cluster) nodes have already established trust with an AT root broker.
  - If the Storage Foundation Cluster File System (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 Storage Foundation Cluster File System (application cluster) nodes

- Port number where the authentication broker for the Storage Foundation Cluster File System (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 88.

12 Configure the CP agent on the Storage Foundation Cluster File System (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 VCS with 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 non-SCSI3 server-based I/O fencing using installsfcfs

If Storage Foundation Cluster File System cluster is configured to run in secure mode, then verify that the configuration is correct before you configure non-SCSI3 server-based I/O fencing.

See "Verifying the security configuration on the SFCFS cluster to use CP server coordination point" on page 155.

Setting up server-based I/O fencing manually

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

Table 10-2 Tasks to set up server-based I/O fencing manually

Action	Description
Preparing the CP servers for use by the Storage Foundation Cluster File System cluster	See "Preparing the CP servers manually for use by the SFCFS cluster" on page 167.
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 171.

Table 10-2 Tasks to set up server-based I/O fencing manually *(continued)*

Action	Description
Modifying Storage Foundation Cluster File System configuration to use I/O fencing	See "Modifying VCS configuration to use I/O fencing" on page 152.
Configuring Coordination Point agent to monitor coordination points	See "Configuring Coordination Point agent to monitor coordination points" on page 175.
Verifying the server-based I/O fencing configuration	See "Verifying server-based I/O fencing configuration" on page 177.

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 10-3 displays the sample values used in this procedure.

Table 10-3 Sample values in procedure

CP server configuration component	Sample name
CP server	mycps1.symantecexample.com
Node #1 - SFCFS cluster	galaxy
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 *Veritas Storage Foundation Cluster File System 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.symantecexample.com/vx
                      clus1/{f0735332-1dd1-11b2} Operator

_HA_VCS_nebula@HA_SERVICES@nebula.symantecexample.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.symantecexample.com\
 -f cps_operator -g vx

User _HA_VCS_galaxy@HA_SERVICES@galaxy.symantecexample.com
successfully added

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

User _HA_VCS_nebula@HA_SERVICES@nebula.symantecexample.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.symantecexample.com\
 -f cps_operator -g vx

Cluster successfully added to user
 _HA_VCS_galaxy@HA_SERVICES@galaxy.symantecexample.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.symantecexample.com\
 -f cps_operator -g vx

Cluster successfully added to user
 _HA_VCS_nebula@HA_SERVICES@nebula.symantecexample.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 (vxfendg). You must specify this disk group in the `/etc/vxfenmode` file.

See "Setting up coordinator disk groups" on page 151.

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 172.

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

   For example:

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

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 10-4 defines the vxfenmode parameters that must be edited.

Table 10-4 vxfenmode file parameters

vxfenmode File Parameter	Description
vxfen_mode	Fencing mode of operation. This parameter must be set to “customized”.
vxfen_mechanism	Fencing mechanism. This parameter defines the mechanism that is used for fencing. If one of the three coordination points is a CP server, then this parameter must be set to “cps”.
scsi3_disk_policy	Configure the vxfen module to use either DMP devices, "dmp" or the underlying raw character devices, "raw". **Note:** The configured disk policy is applied on all the nodes.

Table 10-4 vxfenmode file parameters *(continued)*

vxfenmode File Parameter	Description
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).

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
# hagrp -add vxfen
# hagrp -modify vxfen SystemList galaxy 0 nebula 1
# hagrp -modify vxfen AutoFailOver 0
# hagrp -modify vxfen Parallel 1
# hagrp -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

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

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 *Veritas Storage Foundation Cluster File System Administrator's Guide*.

---

2 Verify that I/O fencing is using the specified coordination points by running the `vxfenconfig` command.

For example, run the following command:

```
# vxfenconfig -l
```

If the output displays `single_cp=1`, it indicates that the application cluster uses a CP server as the single coordination point for server-based fencing.

Setting up non-SCSI3 fencing in virtual environments manually

To manually set up I/O fencing in a non-SCSI-3 PR compliant setup

1 Configure I/O fencing in customized mode with only CP servers as coordination points.

See "Setting up server-based I/O fencing manually" on page 166.

2 Make sure that the Storage Foundation Cluster File System cluster is online and check that the fencing mode is customized.

```
# vxfenadm -d
```

3 Make sure that the cluster attribute UseFence is set to SCSI3.

```
# haclus -value UseFence
```

4 On each node, edit the /etc/vxenviron file as follows:

```
data_disk_fencing=off
```

5 Enter the following command to change the vxfen_min_delay parameter value:

```
# chdev -l vxfen -P -a vxfen_vxfnd_tmt=25
```

6 On each node, edit the /etc/vxfenmode file as follows:

```
loser_exit_delay=55
vxfen_script_timeout=25
```

Refer to the sample /etc/vxfenmode file.

7 On each node, set the value of the LLT sendhbcap timer parameter value as follows:

- Run the following command:

```
lltconfig -T sendhbcap:3000
```

- Add the following line to the /etc/llttab file so that the changes remain persistent after any reboot:

```
set-timer senhbcap:3000
```

8 On any one node, edit the VCS configuration file as follows:

- Make the VCS configuration file writable:

```
# haconf -makerw
```

- For each resource of the type DiskGroup, set the value of the MonitorReservation attribute to 0 and the value of the Reservation attribute to NONE.

```
# hares -modify <dg_resource> MonitorReservation 0

# hares -modify <dg_resource> Reservation "NONE"
```

- Run the following command to verify the value:

```
# hares -list Type=DiskGroup MonitorReservation!=0

# hares -list Type=DiskGroup Reservation!="NONE"
```

The command should not list any resources.

- Modify the default value of the Reservation attribute at type-level.

```
# haattr -default DiskGroup Reservation "NONE"
```

- Make the VCS configuration file read-only

```
# haconf -dump -makero
```

9 Make sure that the UseFence attribute in the VCS configuration file main.cf is set to SCSI3.

10 To make these VxFEN changes take effect, stop and restart VxFEN and the dependent modules

- On each node, run the following command to stop VCS:

```
# /etc/init.d/vcs.rc stop
```

- After VCS takes all services offline, run the following command to stop VxFEN:

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

- On each node, run the following commands to restart VxFEN and VCS:

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

Sample /etc/vxfenmode file for non-SCSI3 fencing

```
================================
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=customized

# vxfen_mechanism determines the mechanism for customized I/O
# fencing that should be used.
#
# available options:
# cps      - use a coordination point server with optional script
#            controlled scsi3 disks
#
vxfen_mechanism=cps
```

```
#
# scsi3_disk_policy determines the way in which I/O Fencing communicates wi
# the coordination disks. This field is required only if customized
# coordinator disks are being used.
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
# scsi3_disk_policy=dmp

#
# Seconds for which the winning sub cluster waits to allow for the losing
# subcluster to panic & drain I/Os. Useful in the absence of SCSI3 based
# data disk fencing
loser_exit_delay=55

#
# Seconds for which vxfend process wait for a customized fencing
# script to complete. Only used with vxfen_mode=customized
vxfen_script_timeout=25

#
# security when enabled uses secure communication to the cp server
# using VxAT (Veritas Authentication Service)
# available options:
# 0 - don't use Veritas Authentication Service for cp server
#   communication
# 1  - use Veritas Authentication Service for cp server
#   communication
security=1

#
# Specify 3 or more odd number of coordination points in this file,
# one in 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
#
cps1=[mycps1.company.com]:14250
cps2=[mycps2.company.com]:14250
cps3=[mycps3.company.com]:14250
================================
```

Enabling or disabling the preferred fencing policy

You can enable or disable the preferred fencing feature for your I/O fencing configuration.

You can enable preferred fencing to use system-based race policy or group-based race policy. If you disable preferred fencing, the I/O fencing configuration uses the default count-based race policy.

See “About preferred fencing” on page 87.

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:

```
# hagrp -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
```

Section 4

Upgrading Storage Foundation Cluster File System

Chapter 11

Preparing to upgrade Veritas Storage Foundation Cluster File System

This chapter includes the following topics:

About upgrading

You have many types of upgrades available. Before you start to upgrade, review the types of upgrades for the Veritas products.

See "About the different ways that you can upgrade" on page 188.

Review the supported upgrade paths that are available for the different methods of upgrading.

See "Supported upgrade paths" on page 189.

After you determine the type of upgrade that you want to perform and its upgrade paths, review the steps to prepare for the upgrade.

Caution: After you perform an upgrade from 5.1 or 5.1RPx to 5.1 SP1, Symantec recommends that you do not roll-back to 5.1 or 5.1RPx.

If you want to upgrade CP server systems that use VCS or SFHA to 5.1 SP1, make sure you upgraded all application clusters to 5.1 SP1. Then, upgrade VCS or SFHA on the CP server systems.

About the different ways that you can upgrade

Symantec offers you several different ways to upgrade. You need to decide which upgrade method best suits your environment, your expertise, and the downtime required.

Table 11-1 Available upgrade methods

Upgrade types and considerations	Methods available for upgrade
Typical upgrades—uses a Veritas provided tool or you can perform the upgrade manually. Requires some server downtime.	Script-based—you can use this to upgrade for the supported upgrade paths Web-based—you can use this to upgrade for the supported upgrade paths Manual—you can use this to upgrade from the previous release Response file—you can use this to upgrade from the previous release
Rolling upgrade—uses a Veritas provided tool or you can perform the upgrade manually. Requires least amount of server downtime.	Script-based—you can use this to upgrade from the previous release Web-based—you can use this to upgrade from the previous release
Phased upgrades—uses a Veritas provided tool and some manual steps. Requires less server downtime than a regular upgrade.	Script-based with some manual steps—you can use this to upgrade from the previous release
Native operating system upgrade—uses the upgrade software that comes with the operating system. Note that not all operating systems support native upgrades.	Operating system specific methods Operating system upgrades

Note: Script- and Web-based upgrades ask for very similar system information for upgrades.

Supported upgrade paths

The following tables describe upgrading to 5.1 SP1.

Table 11-2 AIX upgrades using the script- or Web-based installer

Veritas software versions	5.2	5.3	6.1
4.0 4.0 MP1 - 4.0 MP4	Upgrade to 4.0MP4, upgrade OS to 5.3 TL7/SP6 or later, then upgrade to 5.1SP1 using the installer script	Upgrade to 4.0MP4, upgrade OS to 5.3 TL7/SP6 or later, then upgrade to 5.1SP1 using the installer script	N/A
5.0	Upgrade OS to 5.3 TL7/SP6 or later, then upgrade to 5.1SP1 using the installer script	Upgrade OS to TL7/SP6 or later, then upgrade to 5.1SP1 using the installer script	N/A
5.0 MP1	Upgrade OS to 5.3 TL7/SP6 or later, or 6.1 TL0/SP6 or later, then upgrade to 5.1SP1 using the installer script	Upgrade OS to TL7/SP6 or later, then upgrade to 5.1SP1 using the installer script	Upgrade OS to TL0/SP6 or later, then upgrade to 5.1SP1 using the installer script
5.0 MP3 5.0 MP3 RP3	N/A	Upgrade OS to TL7/SP6 or later, then upgrade to 5.1SP1 using the installer script	Upgrade OS to TL0/SP6 or later, then upgrade to 5.1SP1 using the installer script
5.1 5.1 P1 5.1 RPx	N/A	Upgrade OS to TL7/SP6 or later, then upgrade to 5.1SP1 using the installer script	Upgrade OS to TL0/SP6 or later, then upgrade to 5.1SP1 using the installer script
No Veritas product	N/A	Upgrade OS to TL7/SP6 or later, then do full 5.1SP1 install using installer script	Upgrade OS to TL0/SP6 or later, then do full 5.1SP1 install using installer script

Preparing to upgrade

Before you upgrade, you need to prepare the systems and storage. Review the following procedures and perform the appropriate tasks.

Creating backups

Save relevant system information before the upgrade.

To create backups

1. Log in as superuser.
2. Make a record of the mount points for VxFS file systems and VxVM volumes that are defined in the /`etc/filesystems` file. You need to recreate these entries in the `/etc/filesystems` file on the freshly upgraded system.
3. Before the upgrade, ensure that you have made backups of all data that you want to preserve.
4. Copy the `filesystems` file to `filesystems.orig`:

   ```
   # cp /etc/filesystems /etc/filesystems.orig
   ```

5. Run the `vxlicrep`, `vxdisk list`, and `vxprint -ht` commands and record the output. Use this information to reconfigure your system after the upgrade.
6. If you are installing the high availability version of the Veritas Storage Foundation 5.1 SP1 software, follow the guidelines given in the *Veritas Cluster Server Installation Guide* and *Veritas Cluster Server Release Notes* for information on preserving your VCS configuration across the installation procedure.

Preupgrade planning for Veritas Volume Replicator

Before installing or upgrading Veritas Volume Replicator (VVR):

- Confirm that your system has enough free disk space to install VVR.
- Make sure you have root permissions. You must have root permissions to perform the install and upgrade procedures.

The following related documents are available:

Veritas Volume Replicator Planning and Tuning Guide	Provides detailed explanation of VVR tunables

Veritas Volume Replicator Administrator's Guide	Describes how to change tunable values

See the *Getting Started Guide* for more information on the documentation.

Planning an upgrade from the previous VVR version

If you plan to upgrade VVR from the previous VVR version, you can upgrade VVR with reduced application downtime by upgrading the hosts at separate times. While the Primary is being upgraded, the application can be migrated to the Secondary, thus reducing downtime. The replication between the (upgraded) Primary and the Secondary, which have different versions of VVR, will still continue. This feature facilitates high availability even when the VVR upgrade is not complete on both the sites. Symantec recommends that the Secondary hosts be upgraded before the Primary host in the Replicated Data Set (RDS).

See the *Veritas Storage Foundation Release Notes* for information regarding VVR support for replicating across Storage Foundation versions.

Replicating between versions is intended to remove the restriction of upgrading the Primary and Secondary at the same time. VVR can continue to replicate an existing RDS with Replicated Volume Groups (RVGs) on the systems that you want to upgrade. When the Primary and Secondary are at different versions, VVR does not support changing the configuration with the `vradmin` command or creating a new RDS.

When you upgrade the VVR Primary site from any version before 5.1 to 5.1 SP1 and VVR is not configured under VCS, cfs datavolumes may not get mounted after the upgrade.In such a situation you need to pause replication and mount the datavolumes and again resume the replication.

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in Table 11-3, if either the Primary or Secondary are running a version of VVR prior to 5.1 SP1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 5.1 SP1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

Table 11-3 VVR versions and checksum calculations

VVR prior to 5.1 SP1 (DG version <= 140)	VVR 5.1 SP1 (DG version >= 150)	VVR calculates checksum TCP connections?
Primary	Secondary	Yes

Table 11-3 VVR versions and checksum calculations *(continued)*

VVR prior to 5.1 SP1 (DG version <= 140)	VVR 5.1 SP1 (DG version >= 150)	VVR calculates checksum TCP connections?
Secondary	Primary	Yes
Primary and Secondary		Yes
	Primary and Secondary	No

Note: When replicating between versions of VVR, avoid using commands associated with new features. The earlier version may not support new features and problems could occur.

If you do not need to upgrade all the hosts in the RDS simultaneously, you can use replication between versions after you upgrade one host. You can then upgrade the other hosts in the RDS later at your convenience.

Note: If you have a cluster setup, you must upgrade all the nodes in the cluster at the same time.

Planning and upgrading VVR to use IPv6 as connection protocol

Storage Foundation High Availability supports using IPv6 as the connection protocol.

This release supports the following configurations for VVR:

- VVR continues to support replication between IPv4-only nodes with IPv4 as the internet protocol
- VVR supports replication between IPv4-only nodes and IPv4/IPv6 dual-stack nodes with IPv4 as the internet protocol
- VVR supports replication between IPv6-only nodes and IPv4/IPv6 dual-stack nodes with IPv6 as the internet protocol
- VVR supports replication between IPv6 only nodes
- VVR supports replication to one or more IPv6 only nodes and one or more IPv4 only nodes from a IPv4/IPv6 dual-stack node
- VVR supports replication of a shared disk group only when all the nodes in the cluster that share the disk group are at IPv4 or IPv6

Preparing to upgrade VVR when VCS agents are configured

To prepare to upgrade VVR when VCS agents for VVR are configured, perform the following tasks in the order presented:

- Freezing the service groups and stopping all the applications
- Preparing for the upgrade when VCS agents are configured

Freezing the service groups and stopping all the applications

This section describes how to freeze the service groups and stop all applications.

To freeze the service groups and stop applications for the Primary and Secondary clusters

1. Log in as the superuser.
2. Make sure that `/opt/VRTS/bin` is in your PATH so that you can execute all the product commands.
3. Before the upgrade, cleanly shut down all applications.

   In a shared disk group environment:

   - OFFLINE all application service groups that do not contain RVGShared resources. Do not OFFLINE the ClusterService, cvm and RVGLogowner groups.
   - If the application resources are part of the same service group as an RVGShared resource, then OFFLINE only the application resources.

   In a private disk group environment:

   - OFFLINE all application service groups that do not contain RVG resources. Do not OFFLINE the service groups containing RVG resources.
   - If the application resources are part of the same service group as an RVG resource, then OFFLINE only the application resources. In other words, ensure that the RVG resource remains ONLINE so that the private disk groups containing these RVG objects do not get deported.

   Note: You must also stop any remaining applications not managed by VCS.

4. On any node in the cluster, make the VCS configuration writable:

   ```
   # haconf -makerw
   ```

5 On any node in the cluster, list the groups in your configuration:

```
# hagrp -list
```

6 On any node in the cluster, freeze all service groups except the ClusterService group by typing the following command for each group name displayed in the output from step 5.

```
# hagrp -freeze group_name -persistent
```

Note: Write down the list of frozen service groups for future use.

7 On any node in the cluster, save the configuration file (`main.cf`) with the groups frozen:

```
# haconf -dump -makero
```

Note: Continue only after you have performed steps 3 to step 7 for each cluster.

8 Display the list of service groups that have RVG resources and the nodes on which each service group is online by typing the following command on any node in the cluster:

```
# hares -display -type RVG -attribute State
Resource        Attribute         System      Value
VVRGrp           State            system02    ONLINE
ORAGrp           State            system02    ONLINE
```

Note: For the resources that are ONLINE, write down the nodes displayed in the System column of the output.

9 Repeat step 8 for each cluster.

10 For private disk groups, determine and note down the hosts on which the disk groups are imported.

See "Determining the nodes on which disk groups are online" on page 195.

11 For shared disk groups, run the following command on any node in the CVM cluster:

```
# vxdctl -c mode
```

Note the master and record it for future use.

Determining the nodes on which disk groups are online

For private disk groups, determine and note down the hosts on which the disk groups containing RVG resources are imported. This information is required for restoring the configuration after the upgrade.

To determine the online disk groups

1 On any node in the cluster, list the disk groups in your configuration, and note down the disk group names listed in the output for future use:

```
# hares -display -type RVG -attribute DiskGroup
```

Note: Write down the list of the disk groups that are under VCS control.

2 For each disk group listed in the output in step 1, list its corresponding disk group resource name:

```
# hares -list DiskGroup=diskgroup Type=DiskGroup
```

3 For each disk group resource name listed in the output in step 2, get and note down the node on which the disk group is imported by typing the following command:

```
# hares -display dg_resname -attribute State
```

The output displays the disk groups that are under VCS control and nodes on which the disk groups are imported.

Preparing for the upgrade when VCS agents are configured

If you have configured the VCS agents, it is recommended that you take backups of the configuration files, such as `main.cf` and `types.cf`, which are present in the `/etc/VRTSvcs/conf/config` directory.

To prepare a configuration with VCS agents for an upgrade

1. List the disk groups on each of the nodes by typing the following command on each node:

   ```
   # vxdisk -o alldgs list
   ```

   The output displays a list of the disk groups that are under VCS control and the disk groups that are not under VCS control.

   Note: The disk groups that are not locally imported are displayed in parentheses.

2. If any of the disk groups have not been imported on any node, import them. For disk groups in your VCS configuration, you can import them on any node. For disk groups that are not under VCS control, choose an appropriate node on which to import the disk group. Enter the following command on the appropriate node:

   ```
   # vxdg -t import diskgroup
   ```

3. If a disk group is already imported, then recover it by typing the following command on the node on which it is imported:

   ```
   # vxrecover -bs
   ```

4. Verify that all the Primary RLINKs are up to date.

   ```
   # vxrlink -g diskgroup status rlink_name
   ```

   Note: Do not continue until the Primary RLINKs are up-to-date.

Verifying that the file systems are clean

Verify that all file systems have been cleanly unmounted.

To make sure the file systems are clean

1 Verify that all file systems have been cleanly unmounted:

```
# echo "8192B.p S" | /opt/VRTSvxfs/sbin/fsdb filesystem | \
    grep clean
    flags 0 mod 0 clean clean_value
```

A *clean_value* value of `0x5a` indicates the file system is clean. A value of `0x3c` indicates the file system is dirty. A value of `0x69` indicates the file system is dusty. A dusty file system has pending extended operations.

2 If a file system is not clean, enter the following commands for that file system:

```
# fsck -V vxfs filesystem
# mount -V vxfs filesystem mountpoint
# umount mountpoint
```

These commands should complete any extended operations on the file system and unmount the file system cleanly.

A pending large fileset clone removal extended operation might be in progress if the `umount` command fails with the following error:

```
file system device busy
```

An extended operation is in progress if the following message is generated on the console:

```
Storage Checkpoint asynchronous operation on file_system
file system still in progress.
```

3 If an extended operation is in progress, you must leave the file system mounted for a longer time to allow the operation to complete. Removing a very large fileset clone can take several hours.

4 Repeat step 1 to verify that the unclean file system is now clean.

Upgrading the array support

The Storage Foundation 5.1 SP1 release includes all array support in a single fileset, VRTSaslapm. The array support fileset includes the array support previously included in the VRTSvxvm fileset. The array support fileset also includes support previously packaged as external array support libraries (ASLs) and array policy modules (APMs).

See the 5.1 SP1 Hardware Compatibility List for information about supported arrays.

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

When you upgrade Storage Foundation products with the product installer, the installer automatically upgrades the array support. If you upgrade Storage Foundation products with manual steps, you should remove any external ASLs or APMs that were installed previously on your system. The installation of the VRTSvxvm fileset exits with an error if external ASLs or APMs are detected.

After you have installed Storage Foundation 5.1 SP1, Symantec provides support for new disk arrays though updates to the `VRTSaslapm` package.

For more information about array support, see the *Veritas Volume Manager Administrator's Guide*.

Chapter 12

Performing a typical SFCFS upgrade using the installer

This chapter includes the following topics:

Peforming a full upgrade

Performing a full upgrade involves the following tasks:

- Ensuring that the file systems are clean
- Peforming the upgrade
- Updating the configuration and confirming startup
- Upgrading the remaining nodes

Ensuring the file systems are clean

Before upgrading to SFCFS 5.1 SP1, ensure that the file systems are clean. To ensure that the logs have been replayed and the file systems are marked clean:

To ensure the file systems are clean

1. Log in as superuser onto any node in the cluster.
2. Take the service group offline on each node of the cluster, which contains VxFS and CFS resources:

```
# hagrp -offline group -sys system01
# hagrp -offline group -sys system02
# hagrp -offline group -sys system03
# hagrp -offline group -sys system04
```

   where *group* is the VCS service group that has the CVMVolDg and CFSMount resource.

   Repeat this step for each SFCFS service group.

   Note: This unmounts the CFS file systems.

3. Unmount all VxFS file systems not under VCS control:

```
# umount mount_point
```

4. Check and repair each VxFS file system:

```
# fsck -V vxfs /dev/vx/dsk/diskgroup/volume
```

   The `fsck` command in `/opt/VRTS/bin` accepts either the block or character device (`/dev/vx/dsk/dg/vol`) or (`/dev/vx/rdsk/dg/vol`). The operating system version of `fsck` may limit the device types it accepts.

   For more information, see the `fsck` and `fsck_vxfs` man pages.

   Repeat this step for each file system.

Performing the upgrade

To perform the upgrade

1. Log in as superuser.
2. Insert the appropriate media disc into your system's DVD-ROM drive.

3 If volume management software is running on your system, the software disc automatically mounts as `/mnt/cdrom`.

If volume management software is not available to mount the CD-ROM, you must mount it manually, enter:

```
# mkdir -p /mnt/cdrom
# mount -V cdrfs -o ro /dev/cd0 /mnt/cdrom
```

4 Change to the top-level directory on the disc:

```
# cd /mnt/cdrom
```

5 Verify there are no VxFS file systems mounted on the nodes being upgraded:

```
# mount | grep vxfs
```

If any VxFS file systems are mounted, offline the group on each node of the cluster:

```
# hagrp -offline group -sys system01
# hagrp -offline group -sys system02
# hagrp -offline group -sys system03
# hagrp -offline group -sys system04
```

where *group* is the VCS service group that has the CVMVolDg and CFSMount resource.

If VxFS are not managed by VCS then unmount them manually:

```
# umount mount_point
```

Repeat this step for each SFCFS service group.

6 Start the upgrade from any node in the cluster. Enter the following command, and then press **y** to upgrade the cluster configuration.

```
# ./installsfcfs -upgrade
```

7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA).

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

8 You are prompted to enter the system names (in the following example, "host1" and "host2") on which the software is to be upgraded. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces on which to
install SFCFS: host1 host2
```

9 During the initial system check, the installer verifies that communication between systems has been set up.

If the installer hangs or asks for a login password, stop the installer and set up ssh or rsh. Then run the installer again.

See "About configuring secure shell or remote shell communication modes before installing products" on page 411.

10 After the system checks complete, the installer displays a list of the filesets that will be upgraded. Press Enter to continue with the upgrade.

11 Output shows information that Cluster Server must be stopped on a running system. Enter **y** to continue.

12 Press **Return** to begin removing the previous packages and installing the new.

13 Press **Return** again for summary information about logs and reboots.

Do not remove the log files until the Veritas products are working properly on your system. Technical Support will need these log files for debugging purposes.

14 Update the configuration.

Updating the configuration and confirming startup

Perform the following steps on each upgraded node.

To update the configuration and confirm startup

1 Remove the `/etc/VRTSvcs/conf/config/.stale` file, if it exists.

```
# rm -f /etc/VRTSvcs/conf/config/.stale
```

2 Reboot the upgraded nodes.

```
# /usr/sbin/shutdown -r
```

3 After the nodes reboot, verify that LLT is running:

```
# lltconfig
  LLT is running
```

4 Verify GAB is configured:

```
# gabconfig -l | grep 'Driver.state' | \
  grep Configured
  Driver state : Configured
```

5 Verify VxVM daemon is started and enabled:

```
# /opt/VRTS/bin/vxdctl mode
  mode: enabled
```

6 Confirm all upgraded nodes are in a running state.

```
# gabconfig -a
```

7 Log in as superuser.

8 Insert the appropriate media disc into your system's CD-ROM drive.

9 If volume management software is running on your system, the software disc automatically mounts as `/mnt/cdrom`.

If volume management software is not available to mount the CD-ROM, you must mount it manually, enter:

```
# mkdir -p /mnt/cdrom
# mount -V cdrfs -o ro /dev/cd0 /mnt/cdrom
```

10 Change to the top-level directory on the disc:

```
# cd /mnt/cdrom
```

11 Run `installsfcfs` from any node in the cluster:

```
# ./installsfcfs -start system01
       system02
```

12 After the configuration is complete, the CVM and SFCFS groups may come up frozen. To find out the frozen CVM and SFCFS groups, enter the following command:

```
# /opt/VRTS/bin/hastatus -sum
```

If the groups are frozen, unfreeze CVM and SFCFS groups using the following commands for each group:

- Make the configuration read/write:

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

- Unfreeze the group.

  ```
  # /opt/VRTS/bin/hagrp -unfreeze group -persistent
  ```

- Save the configuration.

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

13 If VVR is configured, and the CVM and SFCFS groups are offline, bring the groups online in the following order:

Bring online the CVM groups on all systems.

```
# /opt/VRTS/bin/hagrp -online group -sys system01
# /opt/VRTS/bin/hagrp -online group -sys system02
```

where *group* is the VCS service group that has the CVMVolDg resource.

Bring online the RVGShared groups and the virtual IP on the master node using the following commands:

```
# hagrp -online RVGShared -sys masterhost
# hares -online ip_name
       masterhost
```

Bring online the SFCFS groups on all systems.

```
# /opt/VRTS/bin/hagrp -online group -sys system01
# /opt/VRTS/bin/hagrp -online group -sys system02
```

where *group* is the VCS service group that has the CFSMount resource.

If the SFCFS service groups do not come online then your file system could be dirty.

14 Upgrade the remaining nodes.

Note: If you upgrade to SFCFS 5.1 SP1 and the file systems are dirty, you have to deport the shared disk group and import it as non-shared. After the import, run `fsck`. `fsck` should succeed. Then deport the disk group and import it back as shared.

Chapter 13

Performing a phased upgrade

This chapter includes the following topics:

Upgrading Storage Foundation Cluster File System and High Availability software from a release prior to 5.1 SP1

This section contains procedures for the Veritas Storage Foundation Cluster File System upgrade.

Performing a phased upgrade of SFCFSHA stack from version 5.0MP3

Performing a phased upgrade involves the following tasks:

- Moving the service groups to the second subcluster
- Upgrading the SFCFSHA stack on the first subcluster
- Preparing the second subcluster
- Activating the first subcluster
- Upgrading the operating system on the second subcluster
- Upgrading the second subcluster
- Finishing the phased upgrade

Before you start the upgrade on the first half of the cluster, back up the VCS configuration files `main.cf` and `types.cf` which are in the directory `/etc/VRTSvcs/conf/config/`.

Prerequisites for a phased upgrade

Before you start the upgrade, confirm that you have licenses for all the nodes that you plan to upgrade.

Planning for a phased upgrade

Plan out the movement of the service groups from node-to-node to minimize the downtime for any particular service group. Some basic guidelines follow:

- Split the cluster in half. If the cluster has an odd number of nodes, calculate (n+1)/2, and start the upgrade with the even number of nodes.
- Split the cluster so that your high priority service groups remain online during the upgrade of the first subcluster.

Phased upgrade limitations

The following limitations primarily describe not to tamper with configurations or service groups during the phased upgrade:

- While you perform the upgrades, do not start any modules. Also, do not add or remove service groups to any of the nodes.
- Depending on your configuration, you may find that you cannot upgrade multiple nodes at the same time. You may only be able to upgrade one node at a time.
- For very large clusters, you might have to repeat these steps multiple times to upgrade your cluster.
- You can perform a phased upgrade when the root disk is encapsulated.

Moving the service groups to the second subcluster

To move the service groups to the second subcluster

1. Switch failover groups from the first half of the cluster to one of the nodes in the second half of the cluster. In this procedure, `galaxy` is a node in the first half of the cluster and `jupiter` is a node in the second half of the cluster. Enter the following:

   ```
   # hagrp -switch failover_group -to jupiter
   ```

2. On the first half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the applications.
3. On the first half of the cluster, unmount the VxFS or CFS file systems that are not managed by VCS.

   ```
   # mount | grep vxfs
   ```

   Verify that no processes use the VxFS or CFS mount point. Enter the following:

   ```
   # fuser -c mount_point
   ```

   Stop any processes using a VxFS or CFS mount point with the mechanism provided by the application.

   Unmount the VxFS or CFS file system. Enter the following:

   ```
   # umount /mount_point
   ```

4. On the first half of the cluster, bring all the VCS service groups offline including CVM group. Enter the following:

   ```
   # hagrp -offline group_name -sys galaxy
   ```

   When the CVM group becomes OFFLINE, all the parallel service groups such as the CFS file system will also become OFFLINE on the first half of the cluster nodes.
5. Verify that the VCS service groups are offline on all the nodes in first half of the cluster. Enter the following:

   ```
   # hagrp -state group_name
   ```

6 Freeze the nodes in the first half of the cluster. Enter the following:

```
# haconf -makerw

# hasys -freeze -persistent galaxy

# haconf -dump -makero
```

7 If IO fencing is enabled, then on each node of the first half of the cluster, change the contents of the /etc/vxfenmode file to configure I/O fencing in disabled mode. Enter the following:

```
# cp /etc/vxfen.d/vxfenmode_disabled /etc/vxfenmode
# cat /etc/vxfenmode
[root@swlx08 ~]# cat /etc/vxfenmode
#
# 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=disabled
```

8 If the cluster-wide attribute UseFence is set to SCSI3, then reset the value to NONE in the /etc/VRTSvcs/conf/config/main.cf file, in first half of the cluster.

9 Verify that only GAB ports a, b, d and h are open. Enter the following:

```
# gabconfig -a
GAB Port Memberships
=======================================================
Port a gen 6b5901 membership 01
Port b gen 6b5904 membership 01
Port d gen 6b5907 membership 01
Port h gen ada40f membership 01
```

Do not stop VCS. Port h should be up and running.

10 In the first half of the cluster, stop all VxVM and CVM volumes. Enter the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open. Enter the following:

```
# vxprint -Aht -e v_open
```

11 On first half of the cluster, upgrade the operating system on all the nodes, if applicable. For instructions, see the upgrade paths for the operating system.

See "Supported AIX operating systems" on page 46.

Upgrading the SFCFSHA stack on the first subcluster

To upgrade the SFCFSHA stack on the first subcluster

- **Note:** This procedure is based on an "in-place" upgrade path; that is, if the operating system is upgraded, the release will be the same, but only the path level will change. If you are moving from major operating system release to another, you must uninstall the SFCFSHA stack before you upgrade the operating system. After the operating system is upgraded, you must reinstall SFCFSHA.

  On the first half of the cluster, upgrade SFCFSHA by using the installsfcfs script. For example use the installsfcfs script as shown below:

  ```
  # ./installsfcfs galaxy
  ```

  After the upgrade for first half of the cluster is complete, no GAB ports will be shown in gabconfig -a output.

  To upgrade your operating system, follow the normal procedures for your platform.

  Note: After the installation completes, you can safely ignore any instructions that the installer displays.

Preparing the second subcluster

To prepare the second subcluster

1. On the second half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the application. [Downtime starts now.]
2. On the second half of the cluster, unmount the VxFS and CFS file systems that are not managed by VCS. Enter the following:

   ```
   # mount | grep vxfs
   ```

   Verify that no processes use the VxFS and CFS mount point. Enter the following:

   ```
   # fuser -c mount_point
   ```

   Stop any processes using a VxFS and CFS mount point with the mechanism provided by the application.

   Unmount the VxFS and CFS file system. Enter the following:

   ```
   # umount /mount_point
   ```

3. On the second half of the cluster, unfreeze all the VCS service groups on all the nodes using the following commands:

   ```
   # haconf -makerw
   # hagrp -unfreeze group_name -persistent
   # haconf -dump -makero
   ```

4. On the second half of the cluster, bring all the VCS service groups offline, including CVM group. Enter the following:

   ```
   # hagrp -offline group_name -sys jupiter
   ```

5. On the second half of the cluster, verify that the VCS service groups are offline. Enter the following:

   ```
   # hagrp -state group_name
   ```

6. Stop VCS on the second half of the cluster. Enter the following:

   ```
   # hastop -local
   ```

7 On each node of the second half of the cluster, change the contents of the /etc/vxfenmode file to configure I/O fencing in disabled mode.

```
# cp /etc/vxfen.d/vxfenmode_disabled /etc/vxfenmode
# cat /etc/vxfenmode#
# 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=disabled
```

8 If the cluster-wide attribute UseFence is set to SCSI3, reset the value to NONE in the /etc/VRTSvcs/conf/config/main.cf file, in second half of the cluster.

9 On the second half on cluster, stop the following SFCFSHA modules: VCS, VxFEN, ODM, GAB, and LLT. Enter the following:

```
# /etc/methods/glmkextadm unload
# /etc/rc.d/rc2.d/s99odm stop
# /etc/methods/gmskextadm status
# /etc/init.d/vxfen.rc stop
# /etc/init.d/gab.rc stop
# /etc/init.d/llt.rc stop
```

10 On each node in the first half of the cluster, enable fencing. Enter the following:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
# cat /etc/vxfenmode
#
# 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
# sybase     - use scsi3 disks in kernel but coordinate membership
# with Sybase ASE
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=scsi3
#
# scsi3_disk_policy determines the way in which I/O Fencing
# communicates with the coordination disks.
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
scsi3_disk_policy=dmp
```

11 If the cluster-wide attribute UseFence is set to NONE, reset the value to SCSI3 in the `/etc/VRTSvcs/conf/config/main.cf` file, in first half of the cluster.

Activating the first subcluster

To activate the first subcluster

1 Restart the upgraded nodes in the first half of the cluster:

```
# /usr/sbin/shutdown -r
```

When the first half of the cluster nodes come up, no GAB ports are OPEN. The following command does not show any GAB ports:

```
# /sbin/gabconfig -a
GAB Port Memberships
===============================================================
```

2 Force gab to form a cluster after the upgraded nodes are rebooted in first half of the cluster.

```
# /sbin/gabconfig -xc
```

GAB ports a, b, d and h appear in **gabconfig -a** command output.

Note: If port b and h are not up, you need to bring fencing and VCS manually online.

---

3 On first half of the cluster, unfreeze all the upgraded nodes. Enter the following:

```
# haconf -makerw
# hasys -unfreeze -persistent node_name
# haconf -dump -makero
```

4 On the first half of the cluster, bring the VCS service groups online. Enter the following:

```
# hagrp -online group_name -sys node_name
```

After you bring the CVM service group ONLINE, all the GAB ports v, w and f come ONLINE and all the CFS mounts service groups also come ONLINE automatically. Only failover service groups need to be brought ONLINE manually.

5 Manually mount the VxFS and CFS file systems that are not managed by VCS. [Downtime ends now.]

Upgrading the operating system on the second subcluster

To upgrade the operating system on the second subcluster

- Enter the following.

  On the second half of the cluster, upgrade the operating system, if applicable. For instructions, see the upgrade paths for the operating system.

  See "Supported AIX operating systems" on page 46.

Upgrading the second subcluster

To upgrade the second subcluster

- Enter the following:

  ```
  # ./installsfcfs node_name
  ```

Completing the phased upgrade

To complete the phased upgrade

1 Verify that the cluster UUID on the nodes in the second subcluster is the same as the cluster UUID on the nodes in the first subcluster. Run the following command to display the cluster UUID:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -display nodename
```

If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -copy -from_sys \
node01 -to_sys node03 node04
```

2 On each node in the second half of the cluster, enable fencing. Enter the following:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
# cat /etc/vxfenmode
#
# 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
# sybase     - use scsi3 disks in kernel but coordinate membership with
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=scsi3
#
# scsi3_disk_policy determines the way in which I/O Fencing communicates
# the coordination disks.
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
scsi3_disk_policy=dmp
```

3 Restart the upgraded nodes in the second half of the cluster:

```
# /usr/sbin/shutdown -r
```

When second half of the nodes come up, all the GAB ports a, b, d, h, u, v, w and f are ONLINE. Also all the CFS mounts service groups come online automatically.

4 Manually mount the VxFS and CFS file systems that are not managed by VCS in the second half of the cluster.

Chapter 14

Performing a rolling upgrade

This chapter includes the following topics:

Performing a rolling upgrade using the installer

You can use rolling upgrades to upgrade one product from a release to the next with minimal application downtime.

About rolling upgrades

You can use rolling upgrades to upgrade one product from a release to the next. Rolling upgrades require less downtime. Rolling upgrades are not compatible with phased upgrades. Do not perform "mixed" rolling upgrades with phased upgrades.

Rolling upgrades take two discrete phases. In the first, you upgrade the product kernel filesets. In the second, you upgrade the non-kernel filesets such as VCS filesets and agent filesets.

You can perform a rolling upgrade from 5.1, 5.1 P1, 5.1 RP1, or 5.1 RP2 to 5.1 SP1.

Prerequisites for a rolling upgrade

Meet the following prerequisites before performing a rolling upgrade:

- Make sure the product that you want to upgrade supports rolling upgrades.
- Split your clusters into sub-clusters for the upgrade to keep the service groups available during upgrade.

- Make sure you logged in as superuser and have the media mounted.
- VCS must be running before performing the rolling upgrade.

Performing a rolling upgrade on kernel filesets: phase 1

Note that in the following instructions that a sub-cluster can represent one or more nodes in a full cluster, but is represented by nodeA.

To perform the rolling upgrade on kernel filesets: phase 1

1. On the first sub-cluster, start the installer for the rolling upgrade with the `-upgrade_kernelpkgs` option.

   ```
   ./installer -upgrade_kernelpkgs nodeA
   ```

2. The installer checks system communications, fileset versions, product versions, and completes prechecks.

   It then upgrades applicable product kernel filesets.

3. The installer loads new kernel modules.
4. The installer starts all the relevant processes and brings all the service groups online.
5. Before you proceed to phase 2, complete step 1 to 4 on the second subcluster.

Performing a rolling upgrade on non-kernel filesets: phase 2

In this phase installer installs all non-kernel filesets on all the nodes in cluster and restarts VCS cluster.

To perform the rolling upgrade on non-kernel filesets: phase 2

1. Start the installer for the rolling upgrade with the `-upgrade_nonkernelpkgs` option. Specify all the nodes in the cluster:

   ```
   ./installer -upgrade_nonkernelpkgs nodeA nodeB nodeC...
   ```

2. The installer checks system communications, fileset versions, product versions, and completes prechecks. It verifies completion of phase 1.
3. The installer upgrades non-kernel filesets.
4. The installer checks system communications, fileset versions, product versions, and completes prechecks. It verifies completion of phase 1. The installer loads the new kernel modules. It then starts all relevant processes and brings all the service groups online.

5 Verify the cluster's status:

```
# hastatus -sum
```

6 If you want to upgrade VCS or SFHA 5.1 on the CP server systems to version 5.1 SP1 PR1, make sure you upgraded all application clusters to 5.1 SP1 PR1. Then, upgrade VCS or SFHA on the CP server systems.

For instructions to upgrade VCS or SFHA on the CP server systems, see the VCS or SFHA installation guide.

Performing a rolling upgrade of SFCFS using the Web-based installer

This section describes using the Veritas Web-based installer to perform a rolling upgrade. The installer detects and upgrades the product that is currently installed on the specified system or systems. If you want to upgrade to a different product, you may need to perform additional steps.

The rolling upgrade is divided into two phases. In the first phase, the installer upgrade kernel filesets. In the second phase, it upgrades non-kernel filesets. The second phase is required for upgrades that have high-availability components. When you perform a rolling upgrade, you need to divide the number of systems that you plan to upgrade roughly in half. Half of the systems' available capacity is needed to take over processes during the rolling upgrade.

To start the rolling upgrade—phase 1

1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 65.

3 In the Task pull-down menu, select **Rolling Upgrade**.

In the Product pull-down menu, select the product that you want to upgrade using a rolling upgrade.

Note that the Upgrade Kernel packages for Rolling Upgrade Phase-1 radio button is selected.

Click the **Next** button to proceed.

4 In the Systems Names field, enter the sub-cluster's system names. Separate system names with a space.

The installer validates systems and stops processes. If it throws an error, address the error and return to the installer.

5 The installer removes old software and upgrades the software on the systems that you selected. Review the output and click the **Next** button when prompted.

6 When the upgrade completes, perform step 3 through step 6 on the second subcluster.

To upgrade the non-kernel components—phase 2

1 In the Task pull-down menu, make sure that **Rolling Upgrade** and the product are selected.

Note that the Upgrade Non-Kernel packages for Rolling Upgrade Phase-2 radio button is selected.

Click the **Next** button to proceed.

2 In the Systems Names field, enter the names of all the systems that you want to upgrade. Separate system names with a space.

The installer validates systems and stops processes. If it throws an error, address the error and return to the installer.

3 The installer removes old software and upgrades the software on the systems that you selected. Review the output and click the **Next** button when prompted.

Chapter 15

Upgrading the operating system

This chapter includes the following topics:

Upgrading the AIX operating system

Use this procedure to upgrade the AIX operating system if SFCFS 5.1 SP1 is installed. You must upgrade to a version that SFCFS 5.1 SP1 supports.

Before you upgrade AIX (after installing or upgrading SFCFS), you must temporarily disable SFCFS to prevent it from starting, until the AIX upgrade is complete. It is necessary to avoid SFCFS operation until AIX is upgraded to the required maintenance level. After the AIX upgrade is complete, you can then enable SFCFS operation.

To upgrade the AIX operating system

1 Create the install-db file.

```
# touch /etc/vx/reconfig.d/state.d/install-db
```

2 Stop activity to all file systems and raw volumes, for example by unmounting any file systems that have been created on volumes.

```
# umount mnt_point
```

3 Stop all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

4 If you are upgrading a high availability (HA) product, take all service groups offline.

List all service groups:

```
# /opt/VRTSvcs/bin/hagrp -list
```

For each service group listed, take it offline:

```
# /opt/VRTSvcs/bin/hagrp -offline service_group \
    -sys system_name
```

5 Stop the VEA backend service by entering the following command:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

6 Upgrade the AIX operating system. See the operating system documentation for more information.

7 Apply the necessary APARs.

For information about APARs required for Storage Foundation Cluster File System 5.1 SP1, refer to the *Veritas Storage Foundation Cluster File System Release Notes*.

8 Enable SFCFS to start after you reboot.

```
# rm /etc/vx/reconfig.d/state.d/install-db
```

9 Reboot the system.

```
# shutdown -Fr
```

Chapter 16

Upgrading using SMIT

This chapter includes the following topics:

Upgrading using SMIT

Upgrading using SMIT is not available for Storage Foundation and High Availability.

To uncompress the packages:

1. Log in as superuser.
2. Create an installation directory on your system large enough for all the Storage Foundation patches. Refer to the disk space requirements in the system requirements section.

   ```
   # mkdir /tmp/install
   ```

3. Place the Veritas software disc into a DVD drive connected to your system. If you downloaded the software, navigate to the top level of the download directory and perform the steps without the DVD.
4. Mount the disk by determining the device access name of the DVD drive. The format for the device access name is `cdN` where *N* is the device number. After inserting the disk into the DVD drive, enter:

   ```
   # mkdir -p /mnt/cdrom
   # mount -V cdrfs -o ro /dev/cdrom /mnt/cdrom
   ```

5. Change to the directory containing the Storage Foundation patches:

   ```
   # cd /mnt/cdrom/storage_foundation/patches
   ```

6 Copy the compressed patch files and the table of contents (`.toc`) file from the software disc to the temporary directory.

```
# cp -r * /tmp/install
# cp .toc /tmp/install/
```

The `.toc` specifies the order in which the Storage Foundation components must be installed, and is used by the `installp` command. In general `VRTSveki`, `VRTSvxvm`, and `VRTSvxfs` must be installed first in the specified order.

7 Change to the temporary directory and unzip the compressed package files:

```
# cd /tmp/install
# gunzip VRTS*.gz
```

8 Invoke SMIT from the command line to upgrade the system. First, upgrade the already installed components of Storage Foundation (formerly known as Foundation Suite):

```
# cd /tmp/install
# smit update_all
```

9 Once the existing components have been upgraded, add the new components added to the 5.1 SP1 release with this command:

```
# smit install
```

10 After successful upgrade, you must reboot the system. Reboot using the command:

```
# shutdown -r
```

11 To take advantage of new features, upgrade the VxVM disk group version (90) to the latest (140).

See the `vxdg` manual pages for more details.

Chapter 17

Upgrading Veritas Volume Replicator

This chapter includes the following topics:

Upgrading Veritas Volume Replicator

If a previous version of Veritas Volume Replicator (VVR) is configured, the product installer upgrades VVR automatically when you upgrade the Storage Foundation products.

When upgrading from 4.0 or later, you have the option to upgrade without disrupting replication.

See "Upgrading VVR without disrupting replication" on page 227.

Upgrading VVR without disrupting replication

This section describes the upgrade procedure from an earlier version of VVR to the current version of VVR when replication is in progress, assuming that you do not need to upgrade all the hosts in the RDS simultaneously.

You may also need to set up replication between versions.

See "Planning an upgrade from the previous VVR version" on page 191.

When both the Primary and the Secondary have the previous version of VVR installed, the upgrade can be performed either on the Primary or on the Secondary. We recommend that the Secondary hosts be upgraded before the Primary host in the RDS. This section includes separate sets of steps, for the Primary upgrade and for the Secondary upgrade.

Note: If you have a cluster setup, you must upgrade all the nodes in the cluster at the same time.

Upgrading VVR on the Secondary

Follow these instructions to upgrade the Secondary hosts.

To upgrade the Secondary

1. Stop replication to the Secondary host by initiating a Primary pause using the following command:

   ```
   # vradmin -g diskgroup pauserep local_rvgname
   ```

2. Upgrade from VVR 4.0 to VVR 5.1 SP1 on the Secondary.

3. Resume the replication from the Primary using the following command:

   ```
   # vradmin -g diskgroup resumerep local_rvgname sec_hostname
   ```

Upgrading VVR on the Primary

After you upgrade the Secondary, use the Veritas product installer to upgrade the Primary.

Note: Reduce application downtime while upgrading by planning your upgrade.

See "Planning an upgrade from the previous VVR version" on page 191.

Chapter 18

Migrating from SFHA to SFCFS or SFCFSHA

This chapter includes the following topics:

Migrating from SFHA to SFCFS or SFCFS HA 5.1 SP1

This section describes how to migrate Storage Foundation High Availability (SFHA) 5.1 SP1 to Storage Foundation Cluster File System (SFCFS) or Storage Foundation Cluster File System High Availability (SFCFSHA) 5.1 SP1.

The product installer does not support direct upgrades from a previous version of SFHA to SFCFS or SFCFSHA5.1 SP1. Ensure that you upgrade the existing SFHA to 5.1 SP1 before beginning this procedure.

To migrate from SFHA 5.1 SP1 to SFCFS 5.1 SP1 or SFCFS HA 5.1 SP1

1. Back up the `main.cf` file before beginning the upgrade.
2. Confirm that the storage disks are visible on all the nodes in the 5.1 SP1 SFHA cluster.
3. Bring all the failover service groups offline, using the following command:

   ```
   # hagrp -offline group_name -any
   ```

   The above command brings the service group offline on the node where the service group is currently online.

4 Unmount all the VxFS file systems which are not under VCS control. If the local file systems are under VCS control, then VCS unmounts the file systems when the failover service group is brought offline in step 3.

On the nodes that have any mounted VxFS local file systems that are not under VCS control:

```
# umount -V vxfs -a
```

5 Stop all the activity on the volumes and deport the local disk groups. If the local disk groups are part of VCS failover service groups, then VCS deports the disk groups when the failover service group is brought offline in step 3.

```
# vxvol -g diskgroup_name stopall
# vxdg deport diskgroup_name
```

6 Upgrade the existing SFHA to SFCFS or SFCFSHA 5.1 SP1:

For SFCFS:

```
# ./installsfcfs
```

For SFCFS HA:

```
# ./installsfcfsha
```

7 After installation is completed, the install script asks you to install licenses. Enter the correct license key to register the key.

8 The installer prompts to reconfigure the VCS. Provide the same cluster name, cluster ID, and LLT link interfaces details that were used during configuration of the SFHA cluster.

9 Find out which node is the CVM master, using the following command:

```
# vxdctl -c mode
```

10 On the CVM Master node, re-import all the required disk groups which must be in shared mode:

```
# vxdg -s import diskgroup_name
```

11 Start all the volumes whose disk groups have been imported as shared in step 10. Use the following command:

```
# vxdg -g diskgroup_name startall
```

12 Run the following command for each of the file systems you want to mount as CFS:

```
# cfsmntadm add diskgroup_name volume_name mount_point \
 all=cluster_mount_options
```

13 Run the following command to mount CFS file systems on all the nodes:

```
# cfsmount mount_point
```

14 Import all other local disk groups which have not been imported in shared mode in step 10.

```
# vxdg import diskgroup_name
```

Start all the volumes of these disk groups using:

```
# vxvol -g diskgroup_name startall
```

Mount these volumes.

15 For any of the file systems which VCS needs to monitor through failover service groups, create these failover service groups by adding the Mount, Diskgroup & Volume resources for VxFS file systems under VCS control.

Chapter 19

Upgrading SFCFS using an alternate disk

This chapter includes the following topics:

About upgrading SFCFS using an alternate disk

Use the alternate disk installation process to upgrade the operating system and SFCFS on a production server while the server runs. Perform the upgrade on an alternate or inactive boot environment. After the upgrade, you restart the system to use the updated environment. The instructions in this section assume a working knowledge of the alternate disk installation process. See the operating system documentation for detailed information on alternate disk installations.

Note: Only Technology Level (TL) and Service Pack (SP) releases of the operating system can be upgraded using this procedure.

Upgrading SFCFS on an alternate disk has the following advantages:

- The server remains active during the time the new boot environment is created and upgraded on the alternate boot device.

- The actual downtime for the upgrade is reduced to the period of time required for a single reboot.
- The original boot environment is still available for use if the updated environment fails to become active.

Supported upgrade scenarios

The following upgrade scenarios are supported on an alternate disk:

- Upgrading only SFCFS
  See " Upgrading SFCFS on an alternate disk" on page 236.
- Upgrading only the operating system (Technology Level (TL) and Service Pack (SP) releases)

  Note: For instructions, see the operating system documentation. No additional steps are required for SFCFS after the operating system upgrade.

- Upgrading the operating system (Technology Level (TL) and Service Pack (SP) releases) and SFCFS
  See " Upgrading SFCFS on an alternate disk" on page 236.

Supported upgrade paths

You can upgrade the operating system and SFCFS using an alternate disk from the following versions:

AIX version	Technology Level and Service Pack releases of AIX 5.3 and later
SFCFS version	5.1 and later

Preparing to upgrade SFCFS on an alternate disk

Complete the preparatory steps in the following procedure before you upgrade SFCFS on an alternate disk.

To prepare to upgrade SFCFS on an alternate disk

1 Make sure that the SFCFS installation media is available.

2 Check the status of the physical disks on your system.

Note: The alternate disk must have a physical identifier and must not contain any mounted volume groups.

```
# lspv
Output similar to the following displays:
hdisk0          0009710fa9c79877    rootvg    active
hdisk1          0009710f0b90db93    None
```

If the alternate disk does not have a physical identifier, set the physical identifier for the disk:

```
# chdev -l hdisk1 -a pv=yes
```

3 Make sure that the following filesets are installed on the primary disk:
`bos.alt_disk_install.boot_images, bos.alt_disk_install.rte`

4 Mount the SFCFS installation media.

Determine the filesets you want to install on the alternate disk.

```
# ./installsfcfs -install_option
```

where install_option is one of the following:

-minpkgs: For installing the minimum set of filesets

-recpkgs: For installing the recommended filesets

-allpkgs: For installing all filesets

Copy the required filesets from the patches directory on the product disc to a directory on the primary boot disk, for example `/tmp`

If you are upgrading the operating system along with SFCFS, copy the necessary operating system filesets and the SFCFS filesets to a directory on the primary disk, for example `/tmp`.

See the operating system documentation to determine the operating system filesets.

Upgrading SFCFS on an alternate disk

This section provides instructions to clone the primary boot environment to the alternate disk, upgrade SFCFS on the alternate disk, and reboot the system to start from the alternate disk. You may perform the steps manually or using the SMIT interface.

In the procedure examples, the primary or current boot environment resides on `hdisk0` and the alternate or inactive boot environment resides on `hdisk1`.

To upgrade Storage Foundation Cluster File System on an alternate disk

Perform the instructions on each node in the cluster.

1 Clone the primary boot disk `rootvg` to an alternate disk.

Manual

Run the following command:

```
# /usr/sbin/alt_disk_copy -I "acNgXY" -P "all" \
-l "/tmp" -w "all" -d "hdisk1"
```

Where:

- -d indicates the name of the target disk on which you clone the primary disk.
- -l indicates the full path of the directory that contains the filesets to be upgraded
- -w indicates the list of SFCFS filesets that you want to upgrade on the alternate boot disk. The option `all` indicates that all the filesets contained in the directory you specified (using option -l) must be installed to the alternate boot disk.

Using SMIT interface

Start the SMIT menu and enter the required information at the prompts:

```
# smit alt_clone
```

- Target disk to install: **hdisk1**
- Fileset(s) to install: **all**
- Directory or Device with images (full path of the directory that contains the filesets to be upgraded): **/tmp/**
- ACCEPT new license agreements? **yes**
- Set bootlist to boot from this disk on next reboot? **yes**

Press **Enter** to start the upgrade on the alternate disk. The upgrade process takes some time.

2 Use the following command to wake up the volume group on the alternate boot disk (hdisk1) that you cloned.

```
# /usr/sbin/alt_rootvg_op -W -d hdisk1
```

3 Verify that the alternate disk is created:

```
# lspv
Output similar to the following displays:
hdisk0          0009710fa9c79877    rootvg
hdisk1          0009710f0b90db93    altinst_rootvg
```

4 Change directory to /alt_inst/etc/VRTSvcs/conf/config.

```
# cd /alt_inst/etc/VRTSvcs/conf/config
```

5 Back up a copy of the old types.cf file and copy the new one for SFCFS to use.

```
# mv types.cf types.cf.ORIG
# cp ../types.cf .
```

6 If you have a secure cluster, perform the instructions in the following section:

See "Upgrading a cluster that is in secure mode" on page 238.

7 Copy the product installation scripts and libraries to the alternate disk:

```
# ./installer -copyinstallscripts -rootpath /alt_inst
```

The command copies the installation and uninstallation scripts and required libraries to the alternate disk.

8 Move to root and run the `alt_rootvg_op -S` command to put the alternate root to sleep.

```
# cd /
# alt_rootvg_op -S
```

9 Verify that the normal boot list includes the name of the alternate boot disk. By default, the alternate disk installation process changes the boot list to enable the system to boot from the alternate disk.

```
# bootlist -m normal -o
hdisk1
```

10 Restart all the nodes in the cluster. The boot environment on the alternate disk is activated when you restart the nodes.

```
# shutdown -r
```

11 Verify the upgrade.

See "Verifying the upgrade" on page 240.

12 If you want to upgrade CP server systems that use VCS or SFHA to 5.1 SP1, make sure that you upgraded all application clusters to version 5.1 SP1. Then, upgrade VCS or SFHA on the CP server systems.

For instructions to upgrade VCS or SFHA on the CP server systems, see the VCS or SFHA installation guide.

Upgrading a cluster that is in secure mode

If your existing cluster is a secure cluster, perform the steps in the following procedure.

To enable security for the upgraded secure cluster

1 Change directory to VRTSat.

```
# cd /alt_inst/var/VRTSat
```

2 Edit the /alt_inst/var/VRTSat/ABAuthSource file. Delete all HA_SERVICES-related entries in it. Remove text similar to the following:

```
[HA_SERVICES@symantecexample]
"PD_state"=dword:00000001
"PD_expiryinterval"=dword:00000000
[HA_SERVICES@symantecexample\admin]
"PD_password"=hex:8d,ab,d2,a3,fe, . . . c4,17,5d,6f,35,3c,12,40
"IsDomainAdmin"=dword:00000001
[HA_SERVICES@symantecexample\_HA_VCS_symantecexample]
"PD_principaltype"=dword:00000002
"PD_password"=hex:7f,31,af,c0,b2, . . . 6c,48,33,fe,13,2d,4e,56
"IsBrokerAdmin"=dword:00000000
"IsDomainAdmin"=dword:00000000
"CanAcceptProxyFlag"=dword:00000000
"CanProxyFlag"=dword:00000000
[HA_SERVICES@symantecexample\_CMDSERVER_VCS_symantecexample]
"PD_principaltype"=dword:00000002
"PD_password"=hex:da,79,b1,9d,fe, . . . 24,54,e1,90,fb,fb,fb,82
"IsDomainAdmin"=dword:00000000
"IsBrokerAdmin"=dword:00000000
"CanProxyFlag"=dword:00000000
"CanAcceptProxyFlag"=dword:00000000
[HA_SERVICES@symantecexample\webserver_VCS_symantecexample.com]
"PD_principaltype"=dword:00000002
"PD_password"=hex:38,29,ba,6d,57, . . . d1,c1,1d,ca,34,0c,82,9f
"IsDomainAdmin"=dword:00000000
"IsBrokerAdmin"=dword:00000000
"CanProxyFlag"=dword:00000001
"CanAcceptProxyFlag"=dword:00000000
"PD_expiryinterval"=dword:00000000
```

3 Touch /alt_inst/var/VRTSat/LocalAuthSource.

```
# touch /alt_inst/var/VRTSat/LocalAuthSource
```

4 Ensure that DNS has the IPv6 address for localhost. Add the following lines into /etc/hosts.

```
127.0.0.1 localhost
::1 localhost
```

Verifying the upgrade

To ensure that alternate disk installation has completed successfully, verify that all the nodes have booted from the alternate boot environment and joined the cluster.

To verify the upgrade

1 Verify that the alternate boot environment is active:

```
# lspv
hdisk0          0009710fa9c79877    old_rootvg
hdisk1          0009710f0b90db93    rootvg          active
```

2 Verify that the version of the upgraded filesets on the alternate boot disk is 5.1.100.0.

```
# lslpp -h VRTSvxvm
```

If you upgraded the operating system:

```
# oslevel -s
```

Verifying that the cluster is in secure mode

Perform the following procedure to verify that the cluster's security (VxAT) works after the reboot.

To verify that VxAT works

1 Make sure that the vxatd process is running. Grep the vxatd process.

```
# ps -ef | grep vxatd
```

For a running process, output resembles:

```
root 139410      1   0 13:01:19      -  0:02 /opt/VRTSat/bin/vxatd
root 176206 229686   0 17:22:39  pts/0  0:00 grep vxatd
```

If the process is not running, enter the following command to start it.

```
# /opt/VRTSvcs/bin/vxatd
```

2 Make sure that the CmdServer process is running. Grep the CmdServer process.

```
# ps -ef | grep CmdServer
```

For a running process, output resembles:

```
root 176142 229686   0 17:24:04  pts/0  0:00 grep CmdServer
root 262272      1   0 13:05:42      -  0:00 /opt/VRTSvcs
/bin/CmdServer
```

If the process is not running, enter the following command to start it.

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

3 For secure communication with Veritas Operations Manager, you may have to restart HAD.

- Stop HAD, at the prompt type:

```
# hastop -local -force
# ps -ef | grep had
    root 426094 319550   0 15:06:44  pts/0  0:00 grep had
```

- Start HAD, at the prompt type:

```
# hastart
```

Section 5

Verification of the installation or the upgrade

Chapter 20

Verifying the Storage Foundation Cluster File System installation

This chapter includes the following topics:

Verifying that the products were installed

Verify that the SFCFS products are installed.

Use the `lslpp` command to check which filesets have been installed:

```
# lslpp -L | grep VRTS
```

The filesets should be in the COMMITTED state.

Use the following sections to further verify the product installation.

Installation log files

After every product installation, the installer creates three text files:

- Installation log file
- Response file
- Summary file

The name and location of each file is displayed at the end of a product installation, and are always located in the `/opt/VRTS/install/logs` directory. It is recommended that you keep the files for auditing, debugging, and future use.

Using the installation log file

The installation log file contains all commands executed during the procedure, their output, and errors generated by the commands. This file is for debugging installation problems and can be used for analysis by Veritas Support.

Using the summary file

The summary file contains the results of the installation by the installer or product installation scripts. The summary includes the list of the packages, and the status (success or failure) of each package. The summary also indicates which processes were stopped or restarted during the installation. After installation, refer to the summary file to determine whether any processes need to be started.

About enabling LDAP authentication for clusters that run in secure mode

Symantec Product Authentication Service (AT) supports LDAP (Lightweight Directory Access Protocol) user authentication through a plug-in for the

authentication broker. AT supports all common LDAP distributions such as Sun Directory Server, Netscape, OpenLDAP, and Windows Active Directory.

For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain.

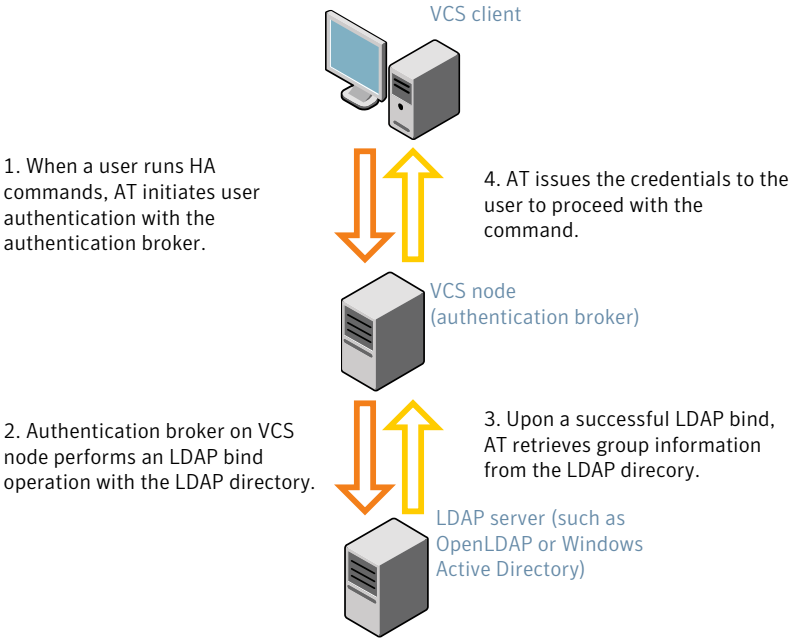
See "Enabling LDAP authentication for clusters that run in secure mode" on page 248.

If you have not already added VCS users during installation, you can add the users later.

See the *Veritas Cluster Server Administrator's Guide* for instructions to add VCS users.

Figure 20-1 depicts the SFCFS cluster communication with the LDAP servers when clusters run in secure mode.

Figure 20-1 Client communication with LDAP servers



See the *Symantec Product Authentication Service Administrator's Guide*.

The LDAP schema and syntax for LDAP commands (such as, ldapadd, ldapmodify, and ldapsearch) vary based on your LDAP implementation.

Before adding the LDAP domain in Symantec Product Authentication Service, note the following information about your LDAP environment:

- The type of LDAP schema used (the default is RFC 2307)
  - UserObjectClass (the default is posixAccount)
  - UserObject Attribute (the default is uid)
  - User Group Attribute (the default is gidNumber)
  - Group Object Class (the default is posixGroup)
  - GroupObject Attribute (the default is cn)
  - Group GID Attribute (the default is gidNumber)
  - Group Membership Attribute (the default is memberUid)
- URL to the LDAP Directory
- Distinguished name for the user container (for example, UserBaseDN=ou=people,dc=comp,dc=com)
- Distinguished name for the group container (for example, GroupBaseDN=ou=group,dc=comp,dc=com)

Enabling LDAP authentication for clusters that run in secure mode

The following procedure shows how to enable the plug-in module for LDAP authentication. This section provides examples for OpenLDAP and Windows Active Directory LDAP distributions.

Before you enable the LDAP authentication, complete the following steps:

- Make sure that the cluster runs in secure mode.

  ```
  # haclus -value SecureClus
  ```

  The output must return the value as 1.

- Make sure that the AT version is 5.0.32.0 or later.

  ```
  # /opt/VRTSat/bin/vssat showversion
  vssat version: 5.0.32.0
  ```

See the `vssat.1m` and the `atldapconf.1m` manual pages.

To enable OpenLDAP authentication for clusters that run in secure mode

1 Add the LDAP domain to the AT configuration using the `vssat` command.

The following example adds the LDAP domain, MYENTERPRISE:

```
# /opt/VRTSat/bin/vssat addldapdomain \
--domainname "MYENTERPRISE.symantecdomain.com"\
--server_url "ldap://my_openldap_host.symantecexample.com"\
--user_base_dn "ou=people,dc=symantecdomain,dc=myenterprise,dc=com"\
--user_attribute "cn" --user_object_class "account"\
--user_gid_attribute "gidNumber"\
--group_base_dn "ou=group,dc=symantecdomain,dc=myenterprise,dc=com"\
--group_attribute "cn" --group_object_class "posixGroup"\
--group_gid_attribute "member"\
--admin_user "cn=manager,dc=symantecdomain,dc=myenterprise,dc=com"\
--admin_user_password "password" --auth_type "FLAT"
```

2 Verify that you can successfully authenticate an LDAP user on the SFCFS nodes.

You must have a valid LDAP user ID and password to run the command. In the following example, authentication is verified for the MYENTERPRISE domain for the LDAP user, vcsadmin1.

```
galaxy# /opt/VRTSat/bin/vssat authenticate
--domain ldap:MYENTERPRISE.symantecdomain.com
--prplname vcsadmin1 --broker galaxy:2821

Enter password for vcsadmin1: ##########

authenticate
----------------------
----------------------

Authenticated User vcsadmin1
----------------------
```

3 Add the LDAP user to the main.cf file.

```
# haconf makerw
# hauser -add "CN=vcsadmin1/CN=people/\
DC=symantecdomain/DC=myenterprise/\
DC=com@myenterprise.symantecdomain.com" -priv Administrator
# haconf -dump -makero
```

If you want to enable group-level authentication, you must run the following command:

```
# hauser -addpriv \
ldap_group@ldap_domain AdministratorGroup
```

4 Verify that the main.cf file has the following lines:

```
# cat /etc/VRTSvcs/conf/config/main.cf
...
...
cluster clus1 (
  SecureClus = 1
  Administrators = {
    "CN=vcsadmin1/CN=people/DC=symantecdomain/DC=myenterprise/
    DC=com@myenterprise.symantecdomain.com" }
  AdministratorGroups = {
    "CN=symantecusergroups/DC=symantecdomain/DC=myenterprise/
    DC=com@myenterprise.symantecdomain.com " }
  )
...
...
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=myenterprise.symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh or ksh), run the following commands:

```
# export VCS_DOMAIN=myenterprise.symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
galaxy     Attribute  RUNNING
nebula     Attribute  RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the SFCFS node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.

To enable Windows Active Directory authentication for clusters that run in secure mode

1 Run the LDAP configuration tool atldapconf using the -d option. The -d option discovers and retrieves an LDAP properties file which is a prioritized attribute list.

```
# /opt/VRTSat/bin/atldapconf -d\
-s domain_controller_name_or_ipaddress\
-u domain_user -g domain_group
```

For example:

```
# /opt/VRTSat/bin/atldapconf -d -s 192.168.20.32 \
-u Administrator -g "Domain Admins"
Search User provided is invalid or Authentication is required to
proceed further.
Please provide authentication information for LDAP server.

Username/Common Name: symantecdomain\administrator
Password:

Attribute file created.
```

2 Run the LDAP configuration tool atldapconf using the -c option. The -c option creates a CLI file to add the LDAP domain.

```
# /opt/VRTSat/bin/atldapconf -c -d windows_domain_name
```

For example:

```
# /opt/VRTSat/bin/atldapconf -c -d symantecdomain.com
Attribute list file not provided, using default AttributeList.txt.
CLI file name not provided, using default CLI.txt.

CLI for addldapdomain generated.
```

3 Run the LDAP configuration tool atldapconf using the -x option. The -x option reads the CLI file and executes the commands to add a domain to the AT.

```
# /opt/VRTSat/bin/atldapconf -x
```

4 List the LDAP domains to verify that the Windows Active Directory server integration is complete.

```
# /opt/VRTSat/bin/vssat listldapdomains

Domain Name :          symantecdomain.com
Server URL :           ldap://192.168.20.32:389
SSL Enabled :          No
User Base DN :         CN=people,DC=symantecdomain,DC=com
User Object Class :    account
User Attribute :       cn
User GID Attribute :   gidNumber
Group Base DN :        CN=group,DC=symantecdomain,DC=com
Group Object Class :   group
Group Attribute :      cn
Group GID Attribute :  cn
Auth Type :            FLAT
Admin User :
Admin User Password :
Search Scope :         SUB
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh or ksh), run the following commands:

```
# export VCS_DOMAIN=symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
galaxy     Attribute  RUNNING
nebula     Attribute  RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the SFCFS node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.

Starting and stopping processes for the Veritas products

After the installation and configuration is complete, the Veritas product installer starts the processes that are used by the installed products. You can use the product installer to stop or start the processes, if required.

To stop the processes

- Use the `-stop` option to stop the product installation script.

  For example, to stop the product's processes, enter the following command:

  ```
  # ./installer -stop
  ```

To start the processes

- Use the `-start` option to start the product installation script.

  For example, to start the product's processes, enter the following command:

  ```
  # ./installer -start
  ```

Checking Veritas Volume Manager processes

Use the following procedure to verify that Volume Manager processes are running.

To confirm that key Volume Manager processes are running

- Type the following command:

  ```
  # ps -ef | grep vx
  ```

  Entries for the `vxconfigd`, `vxnotify`, `vxesd`, `vxrelocd`, `vxcached`, and `vxconfigbackupd` processes should appear in the output from this command. If you disable hot-relocation, the `vxrelocd` and `vxnotify` processes are not displayed.

Checking Veritas File System installation

After the Storage Foundation software has been successfully installed, you can confirm successful Veritas File System installation.

To confirm the File System installation

- Use the `lsvfs` command as follows:

  ```
  # lsvfs vxfs
  ```

  Entries for these processes appear in output similar to the following:

  ```
  vxfs 32 /sbin/helpers/vxfs /sbin/helpers/vxfs
  ```

Verifying agent configuration for Storage Foundation Cluster File System

This section describes how to verify the agent configuration.

To verify the agent configuration

- Enter the cluster status command from any node in the cluster:

```
# cfscluster status
```

Output resembles:

```
Node             :  system01
Cluster Manager  :  running
CVM state        :  running
No mount point registered with cluster configuration

Node             :  system02
Cluster Manager  :  running
CVM state        :  running
No mount point registered with cluster configuration
```

Synchronizing time on Cluster File Systems

SFCFS requires that the system clocks on all nodes are synchronized using some external component such as the Network Time Protocol (NTP) daemon. If the nodes are not in sync, timestamps for change (`ctime`) and modification (`mtime`) may not be consistent with the sequence in which operations actually happened.

Configuring VCS for Storage Foundation Cluster File System

Configuring VCS means conveying to the VCS engine the definitions of the cluster, service groups, resources, and resource dependencies. VCS uses two configuration files in a default configuration:

- The `main.cf` file defines the entire cluster.
- The `types.cf` file defines the resource types.

By default, both files reside in the directory `/etc/VRTSvcs/conf/config`. Additional files similar to `types.cf` may be present if agents have been added, such as `OracleTypes.cf`.

In a VCS cluster, the first system to be brought online reads the configuration file and creates an internal (in-memory) representation of the configuration. Systems brought online after the first system derive their information from systems running in the cluster. You must stop the cluster while you are modifying the files

from the command line. Changes made by editing the configuration files take effect when the cluster is restarted. The node on which the changes were made should be the first node to be brought back online.

main.cf file

The VCS configuration file `main.cf` is created during the installation procedure. After installation, the `main.cf` file contains the base definitions of the cluster and its nodes. Additionally, the file `types.cf` listed in the include statement defines the bundled agents for VCS resources.

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

A typical VCS configuration file for SFCFS file resembles:

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleASMTypes.cf"
include "Db2udbTypes.cf"
include "OracleTypes.cf"
include "SybaseTypes.cf"

cluster sfcfs_1 (
        HacliUserLevel = COMMANDROOT
        )

system thor150 (
        )

system thor151 (
        )

group cvm (
        SystemList = { thor150 = 0, thor151 = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { thor150, thor151 }
        )
CFSfsckd vxfsckd (
        )
        CVMCluster cvm_clus (
                CVMClustName = sfcfs_1
                CVMNodeId = { thor150 = 0, thor151 = 1 }
```

```
        CVMTransport = gab
        CVMTimeout = 200
        )

CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )

cvm_clus requires cvm_vxconfigd
vxfsckd requires cvm_clus

// resource dependency tree
//
//      group cvm
//      {
//      CVMCluster cvm_clus
//          {
//          CVMVxconfigd cvm_vxconfigd
//          }
//      }
```

Storage Foundation Cluster File System HA Only

If you configured VCS Cluster Manager (Web Console), a service group, "ClusterService," was created that includes IP, Process, and Notifier resources. These resources were configured according to information you provided during the installation procedure. A resource dependency was also created.

Veritas Cluster Server application failover services

If you installed SFCFS HA, you can begin implementing the application monitoring failover services provided by the Veritas Cluster Server. Information about setting up VCS services is beyond the scope of this document.

See the *Veritas Cluster Server* documentation.

Configuring the cluster UUID when creating a cluster manually

You need to configure the cluster UUID when you manually create a cluster.

To configure the cluster UUID when you create a cluster manually

- On one node in the cluster, perform the following command to populate the cluster UUID on each node in the cluster.

```
# /opt/VRTSvcs/bin/uuidconfig.pl -clus -configure nodeA
        nodeB ... nodeN
```

Where *nodeA*, *nodeB*, through *nodeN* are the names of the cluster nodes.

About the cluster UUID

You can verify the existence of the cluster UUID.

To verify the cluster UUID exists

- From the prompt, run a more command.

```
cat /etc/vx/.uuids/clusuuid
```

About the LLT and GAB configuration files

Low Latency Transport (LLT) and Group Membership and Atomic Broadcast (GAB) are VCS communication services. LLT requires `/etc/llthosts` and `/etc/llttab` files. GAB requires `/etc/gabtab` file.

Table 20-1 lists the LLT configuration files and the information that these files contain.

Table 20-1 LLT configuration files

File	Description
/etc/default/llt	This file stores the start and stop environment variables for LLT: ■ LLT_START—Defines the startup behavior for the LLT module after a system reboot. Valid values include: 1—Indicates that LLT is enabled to start up. 0—Indicates that LLT is disabled to start up. ■ LLT_STOP—Defines the shutdown behavior for the LLT module during a system shutdown. Valid values include: 1—Indicates that LLT is enabled to shut down. 0—Indicates that LLT is disabled to shut down. The installer sets the value of these variables to 1 at the end of Storage Foundation Cluster File System configuration.

Table 20-1 LLT configuration files *(continued)*

File	Description

/etc/llthosts	The file `llthosts` is a database that contains one entry per system. This file links the LLT system ID (in the first column) with the LLT host name. This file must be identical on each node in the cluster. A mismatch of the contents of the file can cause indeterminate behavior in the cluster.
	For example, the file `/etc/llthosts` contains the entries that resemble:
	`0 galaxy`
	`1 nebula`

/etc/lltab	The file `lltab` contains the information that is derived during installation and used by the utility `lltconfig(1M)`. After installation, this file lists the LLT network links that correspond to the specific system.
	For example, the file `/etc/lltab` contains the entries that resemble:
	`set-node galaxy`
	`set-cluster 2`
	`link en1 /dev/dlpi/en:1 - ether - -`
	`link en2 /dev/dlpi/en:2 - ether - -`
	`set-node galaxy`
	`set-cluster 2`
	`link en1 /dev/en:1 - ether - -`
	`link en2 /dev/en:2 - ether - -`
	The first line identifies the system. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines begin with the `link` command. These lines identify the two network cards that the LLT protocol uses.
	If you configured a low priority link under LLT, the file also includes a "link-lowpri" line.
	Refer to the `lltab(4)` manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the `lltab` file.

Table 20-2 lists the GAB configuration files and the information that these files contain.

Table 20-2 GAB configuration files

File	Description
/etc/default/gab	This file stores the start and stop environment variables for GAB: ■ GAB_START—Defines the startup behavior for the GAB module after a system reboot. Valid values include: 1—Indicates that GAB is enabled to start up. 0—Indicates that GAB is disabled to start up. ■ GAB_STOP—Defines the shutdown behavior for the GAB module during a system shutdown. Valid values include: 1—Indicates that GAB is enabled to shut down. 0—Indicates that GAB is disabled to shut down. The installer sets the value of these variables to 1 at the end of Storage Foundation Cluster File System configuration.
/etc/gabtab	After you install SFCFS, the file /etc/gabtab contains a `gabconfig(1)` command that configures the GAB driver for use. The file `/etc/gabtab` contains a line that resembles: `/sbin/gabconfig -c -nN` The `-c` option configures the driver for use. The `-nN` specifies that the cluster is not formed until at least *N* nodes are ready to form the cluster. Symantec recommends that you set N to be the total number of nodes in the cluster. **Note:** Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`. Using `-c -x` can lead to a split-brain condition.

Verifying the LLT, GAB, and VCS configuration files

Make sure that the LLT, GAB, and VCS configuration files contain the information you provided during VCS installation and configuration.

To verify the LLT, GAB, and VCS configuration files

1 Navigate to the location of the configuration files:

- LLT

  `/etc/llthosts`

  `/etc/llttab`

- GAB

  `/etc/gabtab`

- VCS
  `/etc/VRTSvcs/conf/config/main.cf`

2 Verify the content of the configuration files.

See "About the LLT and GAB configuration files" on page 259.

Verifying LLT, GAB, and cluster operation

Verify the operation of LLT, GAB, and the cluster using the VCS commands.

To verify LLT, GAB, and cluster operation

1 Log in to any node in the cluster as superuser.

2 Make sure that the PATH environment variable is set to run the VCS commands.

3 Verify LLT operation.

See "Verifying LLT" on page 262.

4 Verify GAB operation.

See "Verifying GAB" on page 264.

5 Verify the cluster operation.

See "Verifying the cluster" on page 266.

Verifying LLT

Use the `lltstat` command to verify that links are active for LLT. If LLT is configured correctly, this command shows all the nodes in the cluster. The command also returns information about the links for LLT for the node on which you typed the command.

Refer to the `lltstat(1M)` manual page for more information.

To verify LLT

1 Log in as superuser on the node galaxy.

2 Run the `lltstat` command on the node galaxy to view the status of LLT.

```
lltstat -n
```

The output on galaxy resembles:

```
LLT node information:
    Node             State           Links
```

```
        *0 galaxy          OPEN           2
         1 nebula          OPEN           2
```

Each node has two links and each node is in the OPEN state. The asterisk (*) denotes the node on which you typed the command.

If LLT does not operate, the command does not return any LLT links information: If only one network is connected, the command returns the following LLT statistics information:

```
LLT node information:
    Node                State    Links
   * 0 galaxy           OPEN        2
     1 nebula           OPEN        2
     2 saturn           OPEN        1
```

3 Log in as superuser on the node nebula.

4 Run the `lltstat` command on the node nebula to view the status of LLT.

```
lltstat -n
```

The output on nebula resembles:

```
    LLT node information:
        Node             State           Links
         0 galaxy          OPEN           2
        *1 nebula          OPEN           2
```

5 To view additional information about LLT, run the `lltstat -nvv` command on each node.

For example, run the following command on the node galaxy in a two-node cluster:

```
lltstat -nvv active
```

The output on galaxy resembles:

```
    Node          State      Link    Status      Address
    *0 galaxy      OPEN
                             en1 UP     08:00:20:93:0E:34
                             en2 UP     08:00:20:93:0E:38
    1 nebula       OPEN
                             en1 UP     08:00:20:8F:D1:F2
                             en2 DOWN
```

The command reports the status on the two active nodes in the cluster, galaxy and nebula.

For each correctly configured node, the information must show the following:

- A state of OPEN
- A status for each link of UP
- A MAC address for each link

However, the output in the example shows different details for the node nebula. The private network connection is possibly broken or the information in the `/etc/lltab` file may be incorrect.

6 To obtain information about the ports open for LLT, type `lltstat -p` on any node.

For example, type `lltstat -p` on the node galaxy in a two-node cluster:

```
lltstat -p
```

The output resembles:

```
LLT port information:
  Port  Usage       Cookie
  0     gab          0x0
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
  7     gab          0x7
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
  31    gab          0x1F
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
```

Verifying GAB

Verify the GAB operation using the `gabconfig -a` command. This command returns the GAB port membership information.

The ports indicate the following:

a	GAB
b	I/O fencing
d	Oracle Disk Manager (ODM)

f	Cluster File System (CFS)
h	Veritas Cluster Server (VCS: High Availability Daemon)
u	Cluster Volume Manager (CVM) (to ship commands from slave node to master node) Port u in the `gabconfig` output is visible with CVM protocol version >= 100.
v	Cluster Volume Manager (CVM)
w	vxconfigd (module for CVM)

For more information on GAB, refer to the *Veritas Cluster Server Administrator's Guide*.

To verify GAB

1 To verify that GAB operates, type the following command on each node:

```
/sbin/gabconfig -a
```

2 Review the output of the command:

- If GAB operates, the following GAB port membership information is returned:

```
GAB Port Memberships
===================================
Port a gen  ada401 membership 01
Port b gen  ada40d membership 01
Port d gen  ada409 membership 01
Port f gen  ada41c membership 01
Port h gen  ada40f membership 01

Port u gen  ada41a membership 01

Port v gen  ada416 membership 01
Port w gen  ada418 membership 01
```

Note that port b in the `gabconfig` command output may not indicate that I/O fencing feature is configured. After you configure Storage Foundation Cluster File System using the installer, the installer starts I/O fencing in disabled mode. You can use the `vxfenadm -d` command to verify the I/O fencing configuration.

- If GAB does not operate, the command does not return any GAB port membership information:

```
GAB Port Memberships
===================================
```

Verifying the cluster

Verify the status of the cluster using the `hastatus` command. This command returns the system state and the group state.

Refer to the `hastatus(1M)` manual page.

Refer to the *Veritas Cluster Server Administrator's Guide* for a description of system states and the transitions between them.

To verify the cluster

1 To verify the status of the cluster, type the following command:

```
hastatus -summary
```

The output resembles:

```
-- SYSTEM STATE
-- System               State                Frozen

A  galaxy                RUNNING               0
A  nebula                RUNNING               0

-- GROUP STATE
-- Group           System         Probed  AutoDisabled   State

B  cvm             galaxy          Y       N              ONLINE
B  cvm             nebula          Y       N              ONLINE

B  VxSS            galaxy          Y       N              ONLINE
B  VxSS            nebula          Y       N              ONLINE
```

Note that the VxSS service group is displayed only if you have configured the cluster in secure mode.

2 Review the command output for the following information:

- The system state
  If the value of the system state is RUNNING, the cluster is successfully started.

Verifying the cluster nodes

Verify the information of the cluster systems using the `hasys -display` command. The information for each node in the output should be similar.

Refer to the `hasys(1M)` manual page.

Refer to the *Veritas Cluster Server Administrator's Guide* for information about the system attributes for VCS.

To verify the cluster nodes

- On one of the nodes, type the `hasys -display` command:

  ```
  hasys -display
  ```

  The example shows the output when the command is run on the node galaxy. The list continues with similar information for nebula (not shown) and any other nodes in the cluster.

  ```
  #System    Attribute             Value

  galaxy     AgentsStopped         0

  galaxy     AvailableCapacity     100

  galaxy     CPUUsage              0

  galaxy     CPUUsageMonitoring    Enabled 0 ActionThreshold 0
                                   ActionTimeLimit 0 Action NONE
                                   NotifyThreshold 0 NotifyTimeLimit 0


  galaxy     Capacity              100

  galaxy     ConfigBlockCount      117

  galaxy     ConfigCheckSum        10844

  galaxy     ConfigDiskState       CURRENT

  galaxy     ConfigFile            /etc/VRTSvcs/conf/config

  galaxy     ConfigInfoCnt         0

  galaxy     ConfigModDate         Wed 14 Oct 2009 17:22:48

  galaxy     ConnectorState        Down

  galaxy     CurrentLimits

  galaxy     DiskHbStatus
  ```

```
#System    Attribute             Value

galaxy     DynamicLoad           0

galaxy     EngineRestarted       0

galaxy     EngineVersion         5.1.00.0

galaxy     Frozen                0

galaxy     GUIIPAddr

galaxy     HostUtilization       CPU 0 Swap 0

galaxy     LLTNodeId             0

galaxy     LicenseType           DEMO

galaxy     Limits

galaxy     LinkHbStatus

galaxy     LoadTimeCounter       0

galaxy     LoadTimeThreshold     600

galaxy     LoadWarningLevel      80

galaxy     NoAutoDisable         0

galaxy     NodeId                0

galaxy     OnGrpCnt              1

galaxy     ShutdownTimeout

galaxy     SourceFile            ./main.cf

galaxy     SysInfo               Aix:galaxy,5,2,00023BDA4C00

galaxy     SysName               galaxy

galaxy     SysState              RUNNING

galaxy     SystemLocation

galaxy     SystemOwner

galaxy     TFrozen               0

galaxy     TRSE                  0
```

```
#System    Attribute             Value

galaxy     UpDownState           Up

galaxy     UserInt               0

galaxy     UserStr

galaxy     VCSFeatures           DR

galaxy     VCSMode               VCS_CFS_VRTS
```

Section 6

Adding and removing nodes

Chapter 21

Adding a node to a cluster

This chapter includes the following topics:

About adding a node to a cluster

After you install SFCFS and create a cluster, you can add and remove nodes from the cluster.You can create clusters of up to 64 nodes.

You can add a node:

- Using the product installer
- Using the Web installer
- Manually

The example procedures describe how to add a node to an existing cluster with two nodes.

Before adding a node to a cluster

Before preparing to add the node to an existing SFCFS cluster, verify the following:

- Hardware and software requirements are met.
  See "Meeting hardware and software requirements" on page 274.
- Hardware is set up for the new node.
  See "Setting up the hardware" on page 274.
- The existing cluster is an SFCFS cluster and that SFCFS is running on the cluster.
- The new system has the same identical operating system versions and patch levels as that of the existing cluster.

Meeting hardware and software requirements

The system you add to the cluster must meet the hardware and software requirements.

See "Assessing system preparedness" on page 30.

If the cluster is upgraded from the previous SFCFS version, you must check the cluster protocol version to make sure it has the same version as the node to be added. If there is a protocol mismatch, the node is unable to join the existing cluster.

To verify there is no protocol version mismatch between the cluster and the new node

- Check the cluster protocal version using:

```
# vxdctl list |grep protocol
```

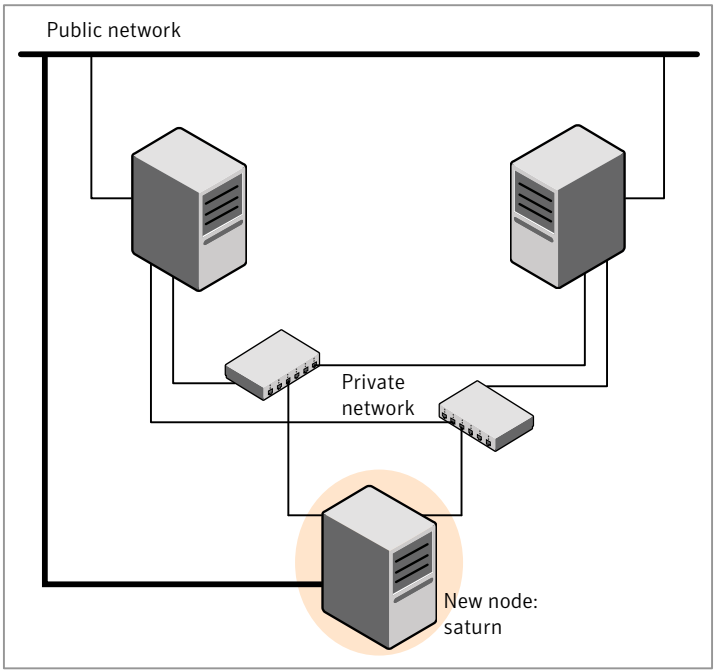
On the master node, check the upgrade protocol using:

```
# vxdctl upgrade
```

Setting up the hardware

Figure 21-1 shows that before you configure a new system on an existing cluster, you must physically add the system to the cluster.

Figure 21-1 Adding a node to a two-node cluster using two switches



To set up the hardware

1 Connect the SFCFS private Ethernet controllers.

Perform the following tasks as necessary:

- When you add nodes to a cluster, use independent switches or hubs for the private network connections. You can only use crossover cables for a cluster, so you might have to swap out the cable for a switch or hub.
- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

Figure 21-1 illustrates a new node being added to an existing two-node cluster using two independent hubs.

2 Make sure that you meet the following requirements:

- The node must be connected to the same shared storage devices as the existing nodes.
- The node must have private network connections to two independent switches for the cluster.
  For more information, see the *Veritas Cluster Server Installation Guide*.

- The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster.

Preparing to add a node to a cluster

Complete the following preparatory steps on the new node before you add the node to an existing SFCFS cluster.

To prepare the new node

1 Verify that the new node meets installation requirements.

```
# ./installsfcfs -precheck saturn
```

2 Install SFCFS on the new system.

Note: Use the `-install` option to install SFCFS. Do not configure SFCFS after the installation.

```
Would you like to configure SFCFS on saturn [y, n, q] (n)
```

You can configure the new node later using the configuration from the existing cluster nodes.

See "About installation and configuration methods" on page 28.

Adding a node to a cluster

You can use one of the following methods to add a node to an existing SFCFS cluster:

SFCFS installer	See "Adding a node to a cluster using the SFCFS installer" on page 277.
	See "Adding a node using the Web-based installer" on page 280.
Manual	See "Adding the node to a cluster manually" on page 281.

Note: Before you add the node, make sure that SFCFS is not configured on the node.

Adding a node to a cluster using the SFCFS installer

You can add a node using the `-addnode` option with the SFCFS installer.

The SFCFS installer performs the following tasks:

- Verifies that the node and the existing cluster meet communication requirements.
- Verifies the products and packages installed on the new node.
- Discovers the network interfaces on the new node and checks the interface settings.
- Creates the following files on the new node:
  `/etc/llttab`
  `/etc/VRTSvcs/conf/sysname`
- Updates the following configuration files and copies them on the new node:
  `/etc/llthosts`
  `/etc/gabtab`
  `/etc/VRTSvcs/conf/config/main.cf`
- Copies the following files from the existing cluster to the new node:
  `/etc/vxfenmode`
  `/etc/vxfendg`
  `/etc/vx/.uuids/clusuuid`
  `/etc/default/llt`
  `/etc/default/gab`
- Configures security on the new node if the existing cluster is a secure cluster.

  Warning: If the root broker system has failed, then you must recover or reconfigure the root broker system before you add a new node to the cluster.

- Configures disk-based or server-based fencing depending on the fencing mode in use on the existing cluster.
- Adds the new node to the CVM, ClusterService, and VxSS service groups in the VCS configuration.

  Note: For other service groups configured under VCS, update the configuration for the new node manually.

- Starts SFCFS processes and configures CVM and CFS on the new node.

At the end of the process, the new node joins the SFCFS cluster.

Note: If you have configured server-based fencing on the existing cluster, make sure that the CP server does not contain entries for the new node. If the CP server already contains entries for the new node, remove these entries before adding the node to the cluster, otherwise the process may fail with an error.

To add the node to an existing cluster using the installer

1. Log in as the root user on one of the nodes of the existing cluster.
2. Run the SFCFS installer with the -addnode option.

   ```
   # cd /opt/VRTS/install

   # ./installsfcfs -addnode
   ```

   The installer displays the copyright message and the location where it stores the temporary installation logs.
3. Enter the name of a node in the existing SFCFS cluster. The installer uses the node information to identify the existing cluster.

   ```
   Enter a node name in the SFCFS cluster to which
   you want to add a node: galaxy
   ```

4. Review and confirm the cluster information.
5. Enter the name of the systems that you want to add as new nodes to the cluster.

   ```
   Enter the system names separated by spaces
   to add to the cluster: saturn
   ```

   The installer checks the installed products and packages on the nodes and discovers the network interfaces.

6 Enter the name of the network interface that you want to configure as the first private heartbeat link.

Note: The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster. The LLT configuration for the new node must be the same as that of the existing cluster.

```
Enter the NIC for the first private heartbeat
link on saturn: [b,q,?] en1
```

7 Enter **y** to configure a second private heartbeat link.

Note: At least two private heartbeat links must be configured for high availability of the cluster.

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

8 Enter the name of the network interface that you want to configure as the second private heartbeat link.

```
Enter the NIC for the second private heartbeat link
on saturn: [b,q,?] en2
```

9 Depending on the number of LLT links configured in the existing cluster, configure additional private heartbeat links for the new node.

The installer verifies the network interface settings and displays the information.

10 Review and confirm the information.

11 If you have configured SMTP, SNMP, or the global cluster option in the existing cluster, you are prompted for the NIC information for the new node.

```
Enter the NIC for VCS to use on saturn: en3
```

12 The installer prompts you with an option to mount the shared volumes on the new node. Select **y** to mount them.

When completed, the installer confirms the volumes are mounted and indicates the location of the log file with details of the actions performed.

13 If the existing cluster uses server-based fencing in secure mode, provide responses to the following installer prompts.

If you are using different root brokers for the CP server and the client SFCFS cluster, enter **y** to confirm the use of different root brokers. The installer attempts to establish trust between the new node being added to the cluster and the authentication broker of the CP server.

```
Are you using different Root Brokers for the CP Server(s) and the
client cluster? (If so then installer will try to establish trust
between the new node(s) being added and CP Server's
Authentication Broker) [y,n,q] (n) y
```

Enter the host name of the authentication broker used for any one of the CP servers.

```
Enter hostname of the Authentication Broker being used for any one
of the CP Server(s): [b] mycps1.symantecexample.com
```

Enter the port number where the authentication broker for the CP server listens to establish trust with the new node:

```
Enter the port where the Authentication Broker
mycps1.symantecexample.com for the CP Server(s) is listening
for establishing trust: [b] (2821)
```

The installer then starts all the required Veritas processes and joins the new node to cluster.

Note: Do not quit the installer if you want to perform the Oracle pre-installation tasks using the SFCFS installer.

---

14 Confirm using `lltstat -n` and `gabconfig -a`.

Adding a node using the Web-based installer

You can use the Web-based installer to add a node to a cluster.

To add a node to a cluster using the Web-based installer

1 From the Task pull-down menu, select **Add a Cluster** node.

From the product pull-down menu, select the product.

Click the **Next** button.

2 In the System Names field enter a name of a node in the cluster where you plan to add the node.

The installer program checks inter-system communications and compatibility. If the node fails any of the checks, review the error and fix the issue.

If prompted, review the cluster's name, ID, and its systems. Click the **Yes** button to proceed.

3 In the System Names field, enter the names of the systems that you want to add to the cluster as nodes. Separate system names with spaces. Click the **Validate** button to check if the system can work in the cluster.

The installer program checks inter-system communications and compatibility. If the system fails any of the checks, review the error and fix the issue.

Click the **Next** button. If prompted, click the **Yes** button to add the system and to proceed.

4 From the heartbeat NIC pull-down menus, select the heartbeat NICs for the cluster. Click the **Next** button.

5 Once the addition is complete, review the log files. Optionally send installation information to Symantec. Click the **Finish** button to complete the node's addition to the cluster.

Adding the node to a cluster manually

Perform this procedure after you install SFCFS only if you plan to add the node to the cluster manually.

To add the node manually to the cluster

1 Start the Volume Manager.

See "Starting Volume Manager on the new node" on page 282.

2 Configure LLT and GAB.

See "Configuring LLT and GAB on the new node" on page 282.

3 If the existing cluster is a secure cluster, set up the new node to run in secure mode.

See "Setting up the node to run in secure mode" on page 284.

4 If the existing cluster is configured to use server-based I/O fencing, configure server-based I/O fencing on the new node.

See "Starting fencing on the new node" on page 287.

5 Start VCS.

See "To start VCS on the new node" on page 288.

6 Configure CVM and CFS.

See "Configuring CVM and CFS on the new node" on page 288.

7 If the ClusterService group is configured on the existing cluster, add the node to the group.

See "Configuring the ClusterService group for the new node" on page 290.

Starting Volume Manager on the new node

Volume Manager uses license keys to control access. As you run the `vxinstall` utility, answer **n** to prompts about licensing. You installed the appropriate license when you ran the `installsfcfs` program.

To start Volume Manager on the new node

1 To start Veritas Volume Manager on the new node, use the vxinstall utility:

```
# vxinstall
```

2 Enter **n** when prompted to set up a system wide disk group for the system.

The installation completes.

3 Verify that the daemons are up and running. Enter the command:

```
# vxdisk list
```

Make sure the output displays the shared disks without errors.

Configuring LLT and GAB on the new node

Perform the steps in the following procedure to configure LLT and GAB on the new node.

To configure LLT and GAB on the new node

1. Edit the `/etc/llthosts` file on the existing nodes. Using vi or another text editor, add the line for the new node to the file. The file resembles:

   ```
   0 galaxy
   1 nebula
   2 saturn
   ```

2. Copy the `/etc/llthosts` file from one of the existing systems over to the new system. The `/etc/llthosts` file must be identical on all nodes in the cluster.

3. Create an `/etc/lltab` file on the new system. For example:

   ```
   set-node saturn
   set-cluster 101

   link en1 /dev/dlpi/en:1 - ether - -
   link en2 /dev/dlpi/en:2 - ether - -
   ```

   Except for the first line that refers to the node, the file resembles the `/etc/lltab` files on the existing nodes. The second line, the cluster ID, must be the same as in the existing nodes.

4. Use vi or another text editor to create the file `/etc/gabtab` on the new node. This file must contain a line that resembles the following example:

   ```
   /sbin/gabconfig -c -nN
   ```

   Where N represents the number of systems in the cluster. For a three-system cluster, N would equal 3.

5. Edit the `/etc/gabtab` file on each of the existing systems, changing the content to match the file on the new system.

6. Use vi or another text editor to create the file `/etc/VRTSvcs/conf/sysname` on the new node. This file must contain the name of the new node added to the cluster.

   For example:

   ```
   saturn
   ```

7 Create the Unique Universal Identifier file `/etc/vx/.uuids/clusuuid` on the new node:

```
# uuidconfig.pl -rsh -clus -copy \
-from_sys galaxy -to_sys saturn
```

8 Start the LLT, GAB, and ODM drivers on the new node:

```
# /etc/init.d/llt.rc start

# /etc/init.d/gab.rc start

# /etc/methods/gmskextadm load

# /etc/rc.d/rc2.d/S99odm start
```

9 On the new node, verify that the GAB port memberships are a and d:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen df204 membership 012
Port d gen df207 membership 012
```

Setting up the node to run in secure mode

You must follow this procedure only if you are adding a node to a cluster that is running in secure mode. If you are adding a node to a cluster that is not running in a secure mode, proceed with configuring LLT and GAB.

Table 21-1 uses the following information for the following command examples.

Table 21-1 The command examples definitions

Name	Fully-qualified host name (FQHN)	Function
saturn	saturn.nodes.example.com	The new node that you are adding to the cluster.
RB1	RB1.brokers.example.com	The root broker for the cluster
RB2	RB2.brokers.example.com	Another root broker, not the cluster's RB

To verify the existing security setup on the node

1. If node saturn is configured as an authentication broker (AB) belonging to a root broker, perform the following steps. Else, proceed to configuring the authentication broker on node saturn.

2. Find out the root broker to which the node saturn belongs using the following command.

```
# vssregctl -l -q -b \
"Security\Authentication\Authentication Broker" \
 -k "BrokerName"
```

3. If the node saturn already belongs to root broker RB1, it is configured as part of the cluster. Proceed to setting up VCS related security configuration.

4. If the node saturn belongs to a different root broker (for example RB2), perform the following steps to remove the security credentials from node saturn.

   - Kill `/opt/VRTSat/bin/vxatd` process.
   - Remove the credential that RB2 has given to AB on node saturn.

     ```
     # vssat deletecred --domain type:domainname \
     --prplname prplname
     ```

     For example:

     ```
     # vssat deletecred --domain vx:root@RB2.brokers.example.com \
     --prplname saturn.nodes.example.com
     ```

Configuring the authentication broker on node saturn

Configure a new authentication broker (AB) on node saturn. This AB belongs to root broker RB1.

To configure the authentication broker on node saturn

1 Create a principal for node saturn on root broker RB1. Execute the following command on root broker RB1.

```
# vssat addprpl --pdrtype root --domain domainname \
 --prplname prplname --password password \
 --prpltype service
```

For example:

```
# vssat addprpl --pdrtype root \
--domain root@RB1.brokers.example.com \
--prplname saturn.nodes.example.com \
--password flurbdicate --prpltype service
```

2 Ensure that there is no clock skew between the times on node saturn and RB1.

3 Copy the `/opt/VRTSat/bin/root_hash` file from RB1 to node saturn.

4 Configure AB on node saturn to talk to RB1.

```
# vxatd -o -a -n prplname -p password -x vx -y domainname -q \
rootbroker -z 2821 -h roothash_file_path
```

For example:

```
# vxatd -o -a -n saturn.nodes.example.com -p flurbdicate \
-x vx -y root@RB1.brokers.example.com -q RB1 \
-z 2821 -h roothash_file_path
```

5 Verify that AB is configured properly.

```
#  vssat showbrokermode
```

The command should return 1, indicating the mode to be AB.

Setting up SFCFS related security configuration

Perform the following steps to configure SFCFS related security settings.

Setting up SFCFS related security configuration

1 Start `/opt/VRTSat/bin/vxatd` process.

2 Create HA_SERVICES domain for SFCFS.

```
# vssat createpd --pdrtype ab --domain HA_SERVICES
```

3 Add SFCFS and webserver principal to AB on node saturn.

```
# vssat addprpl --pdrtype ab --domain HA_SERVICES --prplname
webserver_VCS_prplname --password new_password --prpltype
service --can_proxy
```

4 Create `/etc/VRTSvcs/conf/config/.secure` file.

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

Adding a node in a VxSS group

Perform the following procedure when adding a node in a VxSS group.

To add a node in the VxSS group using the CLI

1 Make a backup copy of the main.cf file. For example:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.cf.2node
```

2 On one of the nodes in the existing cluster, set the cluster configuration to read-write mode:

```
# haconf -makerw
```

3 Add the new node to the VCS configuration:

```
# hasys -add saturn
```

4 Add the node saturn to the existing VxSS group.

```
# hagrp -modify VxSS SystemList -add saturn 2

# hagrp -modify VxSS AutoStartList -add saturn
```

5 Save the configuration by running the following command from any node in the cluster:

```
# haconf -dump -makero
```

Starting fencing on the new node

Perform the following steps to start fencing on the new node.

To start fencing on the new node

1 If you are using disk-based fencing on at least one node, copy the following files from one of the nodes in the existing cluster to the new node:

```
/etc/default/vxfen
/etc/vxfendg
/etc/vxfenmode
```

If you are using pure CP server-based fencing on the existing cluster, then only the `/etc/vxfenmode` file needs to be copied on the new node.

2 Start fencing on the new node:

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

3 On the new node, verify that the GAB port memberships are a, b, and d:

```
# gabconfig -a

GAB Port Memberships
===============================================================
Port a gen    df204 membership 012
Port b gen    df20d membership 012
Port d gen    df20a membership 012
```

After adding the new node

Start VCS on the new node.

To start VCS on the new node

1 Start VCS on the new node:

```
# hastart
```

VCS brings the CVM and CFS groups online.

2 Verify that the CVM and CFS groups are online:

```
# hagrp -state
```

Configuring CVM and CFS on the new node

Modify the existing cluster configuration to configure CVM and CFS for the new node.

To configure CVM and CFS on the new node

1 Make a backup copy of the main.cf file on the existing node, if not backed up in previous procedures. For example:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.cf.2node
```

2 On one of the nodes in the existing cluster, set the cluster configuration to read-write mode:

```
# haconf -makerw
```

3 Add the new node to the VCS configuration, if not already added:

```
# hasys -add saturn
```

4 To enable the existing cluster to recognize the new node, run the following commands on one of the existing nodes:

```
# hagrp -modify cvm SystemList -add saturn 2

# hagrp -modify cvm AutoStartList -add saturn

# hares -modify cvm_clus CVMNodeId -add saturn 2

# haconf -dump -makero

# /etc/vx/bin/vxclustadm -m vcs reinit

# /etc/vx/bin/vxclustadm nidmap
```

5 On the remaining nodes of the existing cluster, run the following commands:

```
# /etc/vx/bin/vxclustadm -m vcs reinit

# /etc/vx/bin/vxclustadm nidmap
```

6 Copy the configuration files from one of the nodes in the existing cluster to the new node:

```
# rcp /etc/VRTSvcs/conf/config/main.cf \
saturn:/etc/VRTSvcs/conf/config/main.cf
# rcp /etc/VRTSvcs/conf/config/CFSTypes.cf \
saturn:/etc/VRTSvcs/conf/config/CFSTypes.cf
# rcp /etc/VRTSvcs/conf/config/CVMTypes.cf \
saturn:/etc/VRTSvcs/conf/config/CVMTypes.cf
```

Configuring the ClusterService group for the new node

If the ClusterService group is configured on the existing cluster, add the node to the group by performing the steps in the following procedure on one of the nodes in the existing cluster.

To configure the ClusterService group for the new node

1. On an existing node, for example galaxy, write-enable the configuration:

```
# haconf -makerw
```

2. Add the node saturn to the existing ClusterService group.

```
# hagrp -modify ClusterService SystemList -add saturn 2

# hagrp -modify ClusterService AutoStartList -add saturn
```

3. Modify the IP address and NIC resource in the existing group for the new node.

```
# hares -modify gcoip Device en0 -sys saturn

# hares -modify gconic Device en0 -sys saturn
```

4. Save the configuration by running the following command from any node.

```
# haconf -dump -makero
```

Configuring server-based fencing on the new node

Perform this step if your existing cluster uses server-based I/O fencing.

To configure server-based fencing on the new node

1. Log in to each CP server as the root user.
2. Update each CP server configuration with the new node information:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt \
-a add_node -c clus1 -u {f0735332-1dd1-11b2} -h saturn -n2
Node 2 (saturn) successfully added
```

3 Verify that the new node is added to the CP server configuration:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt -a list_nodes
```

The new node must be listed in the output.

4 Add the VCS user `cpsclient@saturn` to each CP server:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt \
-a add_user -e cpsclient@saturn \
-f cps_operator -g vx
User cpsclient@saturn successfully added
```

To configure server-based fencing with security on the new node

1 As the root user, create the VCS user and the domain on the new node:

- Create a dummy configuration file `/etc/VRTSvcs/conf/config/main.cf` that resembles the following example:

```
# cat main.cf
include "types.cf"
cluster clus1 {
    SecureClus = 1
   }
system saturn {
 }
```

- Start VCS in one node mode on the new node:

```
# /opt/VRTSvcs/bin/hastart -onenode
```

2 Verify that the VCS user and the domain are created on the new node:

```
# /opt/VRTScps/bin/cpsat showcred | grep _HA_VCS_
# /opt/VRTScps/bin/cpsat listpd -t local | grep HA_SERVICES
```

3 Stop VCS if the VCS user and domain are created successfully on the new node:

```
# /opt/VRTSvcs/bin/hastop
```

4 If the root broker for the CP server and the new node are different, run the following command to establish trust between the authentication broker of the CP Server and the new node:

```
# /usr/bin/echo y | /opt/VRTScps/bin/cpsat setuptrust \
-b thunderbolt -s high
```

5 Log in to each CP server as the root user.

6 Update each CP server configuration with the new node information:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt \
-a add_node -c clus1 -u {f0735332-1dd1-11b2} -h saturn -n2
Node 2 (saturn) successfully added
```

7 Verify that the new node is added to the CP server configuration:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt -a list_nodes
```

The new node must be listed in the output.

8 Add the VCS user `_HA_VCS_saturn@HA_SERVICES@saturn.veritas.com` to each CP server:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt \
-a add_user -e _HA_VCS_saturn@HA_SERVICES@saturn.veritas.com \
-f cps_operator -g vx
User _HA_VCS_saturn@HA_SERVICES@saturn.veritas.com successfully added
```

Updating the Storage Foundation for Databases (SFDB) repository after adding a node

If you are using Database Checkpoints, Database Flashsnap, or Adding a Node in your configuration, update the SFDB repository to enable access for the new node after it is added to the cluster.

To update the SFDB repository after adding a node

1 Run the following to change permission, owner, group of various SFDB directories on the newly added node:

```
# sfua_db_config
```

2 Run the `dbed_update` command on any one node in the cluster. For example:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME -G $ORACLE_SERVICE_GROUP
```

This completes the addition of the node to the SFDB repository.

For information on using SFDB tools features:

See the Storage Foundation guide:*Storage Foundation: Storage and Availability Management for Oracle Databases*.

Sample configuration file for adding a node to the cluster

You may use this sample file as reference information to understand the configuration changes that take place when you add a node to a cluster.

The existing sample configuration before adding the node `saturn` is as follows:

- The existing cluster `rac_cluster101` comprises two nodes `galaxy` and `nebula` and hosts a single database.
- The Oracle database is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- Only one private IP address is configured for Oracle Clusterware. The private IP address is managed by the PrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.

The following sample configuration file shows the changes (in **bold**) effected in the configuration after adding a node "saturn" to the cluster.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
```

```
include "OracleTypes.cf"
include "PrivNIC.cf"


cluster rac_cluster101 (
        UserNames = { admin = bopHo }
        Administrators = { admin }
        UseFence = SCSI3
        )


system galaxy (
        )
system nebula (
        )
system saturn (
       )
```

Note: In the following group oradb1_grp, the saturn node has been added.

```
group oradb1_grp (
        SystemList = { galaxy = 0, nebula = 1, saturn = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula, saturn }
        )
```

Note: In the following Oracle resource, the saturn node information has been added.

```
Oracle ora1 (
          Critical = 0
          Sid @galaxy = vrts1
          Sid @nebula = vrts2
          Sid @saturn = vrts3
          Owner = oracle
          Home = "/app/oracle/orahome"
          StartUpOpt = "SRVCTLSTART"
          ShutDownOpt = "SRVCTLSTOP"
          )

CFSMount oradata_mnt (
         Critical = 0
```

```
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
        )

CVMVolDg oradata_voldg (
        Critical = 0
        CVMDiskGroup = oradatadg
        CVMVolume = { oradatavol }
        CVMActivation = sw
        )

requires group cvm online local firm
ora1 requires oradata_mnt
oradata_mnt requires oradata_voldg
```

Note: In the following CVM and CVMCluster resources, the saturn node information has been added.

```
group cvm (
        SystemList = { galaxy = 0, nebula = 1, saturn =2}
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula, saturn }
        )

        Application cssd (
                Critical = 0
                StartProgram = "/opt/VRTSvcs/rac/bin/cssd-online"
                StopProgram = "/opt/VRTSvcs/rac/bin/cssd-offline"
                CleanProgram = "/opt/VRTSvcs/rac/bin/cssd-clean"
                MonitorProgram = "/opt/VRTSvcs/rac/bin/cssd-monitor"
                OnlineRetryLimit = 20
                )

       CFSMount ocrvote_mnt (
                Critical = 0
                MountPoint = "/ocrvote"
                BlockDevice = "/dev/vx/dsk/ocrvotedg/ocrvotevol"
                MountOpt= "mincache=direct"
                )
```

```
        CVMVolDg ocrvote_voldg (
                 Critical = 0
                 CVMDiskGroup = ocrvotedg
                 CVMVolume = { ocrvotevol }
                 CVMActivation = sw
                 )


        CFSfsckd vxfsckd (
                 )



        CVMCluster cvm_clus (
                CVMClustName = rac_cluster101
                CVMNodeId = { galaxy = 0, nebula = 1, saturn =2 }
                CVMTransport = gab
                CVMTimeout = 200
                )


        CVMVxconfigd cvm_vxconfigd (
                 Critical = 0
                 CVMVxconfigdArgs = { syslog }
                 )
```

Note: In the following PrivNIC resource, the saturn node information has been added.

```
PrivNIC ora_priv (
              Critical = 0
              Device@galaxy = { en1 = 0, en2 = 1}
              Device@nebula = { en1 = 0, en2 = 1}
              Device@saturn = { en1 = 0, en2 = 1}
              Address@galaxy = "192.168.12.1"
              Address@nebula = "192.168.12.2"
              Address@saturn = "192.168.12.5"
              NetMask = "255.255.255.0"
              )


cssd requires ocrvote_mnt
cssd requires ora_priv
```

```
ocrvote_mnt requires ocrvote_voldg
ocrvote_mnt requires vxfsckd
ocrvote_voldg requires cvm_clus
vxfsckd requires cvm_clus
cvm_clus requires cvm_vxconfigd
```

Chapter 22

Removing a node from Storage Foundation Cluster File System clusters

This chapter includes the following topics:

About removing a node from a cluster

You can remove one or more nodes from an SFCFS cluster if the node no longer needs to be part of the cluster.

Removing a node from a cluster requires:

- Stopping applications that use File System or Cluster File System mount points not configured under VCS.
- Stopping VCS on the node to be removed.

- Unmounting the File System and Cluster File System file systems not configured under VCS.
- Uninstalling SFCFS from the node.
  Modifying the VCS configuration files on the existing nodes.
- Removing the node configuration from the CP server if it is configured.
- Removing the security credentials from the node if it is part of a secure cluster.
- Updating the SFDB repository if you use SFDB tools.

The Veritas product installer does not support removing a node. You must remove a node manually. The example procedures describe how to remove a node from a cluster with three nodes.

Removing a node from a cluster

Perform the following steps to remove a node from a cluster. The procedure can be done from any node remaining in the cluster or from a remote host.

To remove a node from a cluster

1 Take your application service groups offline (if under VCS control) on the node you want to remove.

```
# hagrp -offline app_group -sys saturn
```

2 Stop the applications that use VxFS/CFS mount points and are not configured under VCS. Use native application commands to stop the applications.

3 Stop VCS on the node:

```
# hastop -local
```

4 Unmount the VxFS/CFS file systems that are not configured under VCS.

```
# umount mount_point
```

5 Uninstall SFCFS from the node using the SFCFS installer.

```
# cd /opt/VRTS/install

# ./uninstallsfcfs saturn
```

The installer stops all SFCFS processes and uninstalls the SFCFS packages.

6 Modify the VCS configuration files on the existing nodes to remove references to the deleted node.

See "Modifying the VCS configuration files on existing nodes" on page 301.

Modifying the VCS configuration files on existing nodes

Modify the configuration files on the remaining nodes of the cluster to remove references to the deleted nodes.

The process involves:

- Editing the /etc/llthosts file
- Editing the /etc/gabtab file
- Modifying the VCS configuration to remove the node

For an example main.cf:

See "Sample configuration file for removing a node from the cluster" on page 305.

Editing the /etc/llthosts file

On each of the existing nodes, edit the `/etc/llthosts` file to remove lines that contain references to the removed nodes.

For example, if saturn is the node removed from the cluster, remove the line "2 saturn" from the file:

```
0 galaxy
1 nebula
2 saturn
```

Change to:

```
0 galaxy
1 nebula
```

Editing the /etc/gabtab file

Modify the following command in the `/etc/gabtab` file to reflect the number of systems after the node is removed:

```
/sbin/gabconfig -c -nN
```

where N is the number of remaining nodes in the cluster.

For example, with two nodes remaining, the file resembles:

```
/sbin/gabconfig -c -n2
```

Modifying the VCS configuration to remove the node

Modify the VCS configuration file main.cf to remove all references to the deleted node.

Use one of the following methods to modify the configuration:

- Edit the `/etc/VRTSvcs/conf/config/main.cf` file
  This method requires application down time.
- Use the command line interface
  This method allows the applications to remain online on all remaining nodes.

The following procedure uses the command line interface and modifies the sample VCS configuration to remove references to the deleted node. Run the steps in the procedure from one of the existing nodes in the cluster. The procedure allows you to change the VCS configuration while applications remain online on the remaining nodes.

To modify the VCS configuration using the CLI

1. Back up the `/etc/VRTSvcs/conf/config/main.cf` file.

   ```
   # cd /etc/VRTSvcs/conf/config

   # cp main.cf main.cf.3node.bak
   ```

2. Change the cluster configuration to read-write mode:

   ```
   # haconf -makerw
   ```

3. Remove the node from the AutoStartList attribute of the service group by specifying the remaining nodes in the desired order:

   ```
   # hagrp -modify cvm AutoStartList galaxy nebula
   ```

4 Remove the node from the SystemList attribute of the service group:

```
# hagrp -modify cvm SystemList -delete saturn
```

5 Remove the node from the CVMNodeId attribute of the service group:

```
# hares -modify cvm_clus CVMNodeId -delete saturn
```

6 If you have the other service groups (such as the database service group or the ClusterService group) that have the removed node in their configuration, perform step 4 and step 5 for each of them.

7 Remove the deleted node from the NodeList attribute of all CFS mount resources:

```
# hares -modify CFSMount NodeList -delete saturn
```

8 Remove the deleted node from the system list of any other service groups that exist on the cluster. For example, to delete the node saturn:

```
# hagrp -modify crsgrp SystemList -delete saturn
```

9 Remove the deleted node from the cluster system list:

```
# hasys -delete saturn
```

10 Save the new configuration to disk:

```
# haconf -dump -makero
```

11 Verify that the node is removed from the VCS configuration.

```
# grep -i saturn main.cf
```

If the node is not removed, use the VCS commands as described in this procedure to remove the node.

Removing the node configuration from the CP server

After removing a node from a SFCFS cluster, perform the steps in the following procedure to remove that node's configuration from the CP server.

Note: The `cpsadm` command is used to perform the steps in this procedure. For detailed information about the `cpsadm` command, see the *Veritas Storage Foundation Cluster File System Administrator's Guide*.

To remove the node configuration from the CP server

1. Log into the CP server as the root user.
2. View the list of VCS users on the CP server, using the following command:

   ```
   # cpsadm -s cp_server -a list_users
   ```

   Where *cp_server* is the virtual IP/ virtual hostname of the CP server.
3. Remove the VCS user associated with the node you previously removed from the cluster.

   For CP server in secure mode:

   ```
   # cpsadm -s cp_server -a rm_user \
   -e _HA_VCS_saturn@HA_SERVICES@saturn.nodes.example.com \
   -f cps_operator  -g vx
   ```

   For CP server in non-secure mode:

   ```
   # cpsadm -s cp_server  -a rm_user \
   -e cpsclient@saturn  -f cps_operator  -g vx
   ```
4. Remove the node entry from the CP server:

   ```
   # cpsadm -s cp_server -a rm_node  -h saturn -c clus1 -n 2
   ```
5. View the list of nodes on the CP server to ensure that the node entry was removed:

   ```
   # cpsadm -s cp_server -a list_nodes
   ```

Removing security credentials from the leaving node

If the leaving node is part of a cluster that is running in a secure mode, you must remove the security credentials from node saturn. Perform the following steps.

To remove the security credentials

1 Kill the `/opt/VRTSat/bin/vxatd` process.

2 Remove the root credentials on node saturn.

```
# vssat deletecred --domain type:domainname --prplname prplname
```

Updating the Storage Foundation for Databases (SFDB) repository after removing a node

If you are using Database Checkpoints, Database Flashsnap, or SmartTier for Oracle in your configuration, update the SFDB repository to remove the reference for the node after removing the node from the cluster.

Note: If you have not created an SFDB repository, you do not need to perform the following steps.

To update the SFDB repository after removing a node

1 As Oracle user, list the nodes in the cluster:

```
$ /opt/VRTSdbed/bin/dbed_rept_node -S $ORACLE_SID -o list
```

2 Run the following command after physically removing the node from the cluster.

For example:

```
$ /opt/VRTSdbed/bin/dbed_rept_node -S $ORACLE_SID -n NODE -o remove
```

This completes the removal of the node from the SFDB repository.

Sample configuration file for removing a node from the cluster

You may use this sample file as reference information to understand the configuration changes involved when you remove a node from a cluster.

The existing sample configuration before removing the node *system3* is as follows:

- The existing cluster *cluster1* comprises three nodes *system1*, *system2*, and *system3* and hosts a single database.
- The database is stored on CFS.

- The database is managed by a VCS database agent.
  The agent starts, stops, and monitors the database.

Note: The following sample file shows in **bold** the configuration information that is removed when the node *system3* is removed from the cluster.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"

cluster cluster1 (
        UserNames = { admin = bopHo }
        Administrators = { admin }
        UseFence = SCSI3
        )

cluster cluster1 (
        UserNames = { admin = bopHo }
        Administrators = { admin }
        UseFence = SCSI3
        )

system system1 (
        )
system system2 (
        )
system system3 (
       )
```

Note: In the following group *app_grp*, the *system3* node must be removed.

```
group app_grp (
        SystemList = { system1 = 0, system2 = 1, system3 = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { system1, system2, system3 }
        )
```

Note: In the following application resource, the *system3* node information must be removed.

```
App app1 (
          Critical = 0
          Sid @system1 = vrts1
          Sid @system2 = vrts2
          Sid @system3 = vrts3
          )

CFSMount appdata_mnt (
         Critical = 0
         MountPoint = "/oradata"
         BlockDevice = "/dev/vx/dsk/appdatadg/appdatavol"
         )

CVMVolDg appdata_voldg (
         Critical = 0
         CVMDiskGroup = appdatadg
         CVMVolume = { appdatavol }
         CVMActivation = sw
         )

requires group cvm online local firm
app1 requires appdata_mnt
appdata_mnt requires appdata_voldg
```

Note: In the following CVM and CVMCluster resources, the *system3* node information must be removed.

```
group cvm (
        SystemList = { system1 = 0, system2 = 1, system3 =2}
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { system1, system2, system3 }
        )

        CFSfsckd vxfsckd (
                )



        CVMCluster cvm_clus (
              CVMClustName = rac_cluster101
              CVMNodeId = { system1 = 0, system2 = 1, system3 =2 }
```

```
                CVMTransport = gab
                CVMTimeout = 200
                )


        CVMVxconfigd cvm_vxconfigd (
                Critical = 0
                CVMVxconfigdArgs = { syslog }
                )

vxfsckd requires cvm_clus
cvm_clus requires cvm_vxconfigd
```

Section 7

Setting up and configuring replicated global cluster

Chapter 23

Setting up a replicated global cluster

This chapter includes the following topics:

Replication in the SFCFS environment

You can set up a primary SFCFS cluster for replication to a secondary SFCFS cluster by configuring global VCS service groups and using a replication technology. The application cluster at the secondary site can be a single node cluster. For example, you can have a two-node cluster on the primary site and a two-node or single-node cluster on the secondary site.

You can use one of the following replication technologies:

- Veritas Volume Replicator (VVR), which provides host-based volume replication. Using VVR you can replicate data volumes on a shared disk group in SFCFS.
- Supported hardware-based replication technologies. Using hardware-based replication you can replicate data from a primary array to a secondary array.
- Using SFCFS with VVR you can run a fire drill to verify the disaster recovery capability of your configuration.
  See the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

Requirements for SFCFS global clusters

Review the requirements information to make sure your configuration is supported for SFCFS.

For product licensing information:

See "About Veritas product licensing" on page 49.

Supported software and hardware for SFCFS

For supported hardware and software:

- See "Hardware overview and requirements for Veritas Storage Foundation Cluster File System" on page 38.
- See the current compatibility list in the Veritas Technical Support website to confirm the compatibility of your hardware:
  http://entsupport.symantec.com/docs/283161

Supported replication technologies for SFCFS

SFCFS supports the following replication technologies through the use of Veritas replication agents:

Table 23-1 Supported replication options for SFCFS global clusters

Replication technology	Supported modes	Supported software
Veritas Volume Replicator (VVR) Supporting agents ■ RVGShared ■ RVGSharedPri ■ RVGLogOwner	■ Asynchronous replication ■ Synchronous replication	Host-based replication
EMC SRDF Supporting agent: SRDF	■ Asynchronous replication ■ Synchronous replication	All versions of Solutions Enabler
Hitachi True Copy Supporting agent: HTC	■ Asynchronous replication ■ Synchronous replication	All versions of the Hitachi CCI
IBM Metro Mirror Supporting agent: MetroMirror	Synchronous replication	All versions of IBM DSCLI. The MetroMirror agent is supported for DS6000 and DS8000 arrays
IBM SVC SVC CopyServices	■ Asynchronous replication ■ Synchronous replication	SSH access to the SVC
EMC Mirror View Supporting agent:MirrorView	■ Asynchronous replication ■ Synchronous replication: only individual LUNs may be replicated	All versions of NaviCLI

Note: Check your vendor's compatibility list for the supported software versions. The support listed above only exists if the host, HBA, and array combination is in your vendor's hardware compatibility list. Check your array documentation.

Note: All arrays must support SCSI-3 persistent reservations for SFCFS.

You can use the Veritas replication agents listed in the table above for global clusters that run SFCFS. The Veritas replication agents provide application failover and recovery support to your replication configuration. The agents provide this support for environments where data is replicated between clusters.

VCS agents control the direction of replication. They do not monitor the progress or status of replication. The replication agents manage the state of replicated devices that are attached to SFCFS nodes. The agents make sure that the system which has the resource online also has safe and exclusive access to the configured devices.

This information is current at the time this document is released. For more current information on the replicated agents, see:

- *Veritas Cluster Server Agent for EMC SRDF Installation and Configuration Guide*
- *Veritas Cluster Server Agent for Hitachi TrueCopy Installation and Configuration Guide*
- *Veritas Cluster Server Agent for IBM Metro Mirror Installation and Configuration Guide*
- *Veritas Cluster Server Agent for IBM SVC Installation and Configuration Guide*
- *Veritas Cluster Server Agent for EMC MirrorView Installation and Configuration Guide*
- *Veritas Cluster Server Agent for Oracle Data Guard Installation and Configuration Guide*
- Technical Support TechNote for the latest updates or software issues for replication agents:
  http://entsupport.symantec.com/docs/282004htm

About setting up a global cluster in an SFCFS environment

Configuring a global cluster for application requires the coordination of many component setup tasks. The procedures provided in this document are guidelines.

The tasks required to set up a global cluster:

- Configure an SFCFS cluster at the primary site
- Configure an SFCFS cluster at the secondary site
- Configure replication on clusters at both sites
- Configure VCS service groups for replication

- Test the HA/DR configuration
- Upon successful testing, bring the environment into production

Some SFCFS HA/DR configuration tasks may require adjustments depending upon your particular starting point, environment, and configuration. Review the installation requirements and sample cluster configuration files for primary and secondary clusters.

For instructions for configuring AT in a global cluster:

See the *Veritas Cluster Server Administrator's Guide*

Configuring a cluster at the primary site

You can use an existing SFCFS cluster or you can install a new SFCFS cluster for your primary site.

For planning information:

See "About planning for SFCFS installation" on page 27.

If you are using an existing cluster as the primary and you want to set up a global cluster, skip the steps below and proceed to configure your secondary cluster.

See "Configuring a cluster at the secondary site" on page 317.

Note: You must have a GCO license enabled for a global cluster. If you are using VVR for replication, you must have a VVR license enabled.

If you do not have an existing cluster and you are setting up two new sites for an SFCFS global cluster, follow the steps below.

To set up the cluster and database at the primary site

1. Install and configure servers and storage.
2. If you are using hardware-based replication, install the sofware for managing your array.
3. Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster. If you are using VVR for replication, you must have it enabled.

4 Install and configure SFCFS. Prepare for your installation according to your configuration needs.

For preparation:

See "Prerequisites for Veritas Storage Foundation Cluster File System" on page 37.

For installation:

See "About the Web-based installer" on page 63.

5 For a multi-node cluster, configure I/O fencing.

- Verify the shared storage on the secondary site supports SCSI-3 reservations.
- Set up coordinator disks
- Configure I/O fencing

For instructions for setting up fencing:

See "About planning to configure I/O fencing" on page 90.

6 Verify the CVM group is online on all nodes in the primary cluster:

```
# hagrp -state cvm
```

7 Prepare systems and storage for a global cluster. Identify the hardware and storage requirements before installing your database software.

You will need to set up:

- Local storage for database software
- Shared storage for resources which are not replicated
- Replicated storage for database files

8 Install and configure the database binaries. Consult your database documentation.

Note: Resources which will not be replicated must be on non-replicated shared storage.

After successful database installation and configuration, verify that database resources are up on all nodes.

9 Identify the disks that will be replicated, create the required CVM disk group, volume, and file system.

10 Create the database on the file system you created in the previous step.

11 Configure the VCS service groups for the database.

12 Verify that all VCS service groups are online.

Configuring a cluster at the secondary site

To set up a multi-node or single-node cluster on the secondary site:

- Set up the cluster
- Set up the database

The setup requirements for the secondary site parallel the requirements for the primary site with a few additions or exceptions as noted below.

Important requirements for global clustering:

- Cluster names on the primary and secondary sites must be unique.
- Make sure that you use the same OS user and group IDs for Oracle for installation and configuration on both the primary and secondary clusters.

Setting up the cluster on the secondary site

To set up the cluster on secondary site

1 Install and configure servers and storage.

2 If you are using hardware-based replication, install the sofware for managing your array.

3 Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster. If you are using VVR for replication, you must have it enabled.

4 Install and configure SFCFS. Prepare for your installation according to your configuration needs.

For preparation:

See "Prerequisites for Veritas Storage Foundation Cluster File System" on page 37.

For installation:

See "About the Web-based installer" on page 63.

5 For a multi-node cluster, configure I/O fencing.

- Verify the shared storage on the secondary site supports SCSI-3 reservations.
- Set up coordinator disks
- Configure I/O fencing

For instructions for setting up fencing:

See "About planning to configure I/O fencing" on page 90.

6 For a single-node cluster, do not enable I/O fencing. Fencing will run in disabled mode.

7 Prepare systems and storage for a global cluster. Identify the hardware and storage requirements before installing your database software.

You will need to set up:

- Local storage for database software
- Shared storage for resources which are not replicated
- Replicated storage for database files

8 Install and configure the database binaries. Consult your database documentation.

Note: Resources which will not be replicated must be on non-replicated shared storage.

After successful database installation and configuration, verify that database resources are up on all nodes.

Setting up the database for the secondary site

To set up the database for the secondary site

1 Do not create the database. The database will be replicated from the primary site.

- If you are using hardware-based replication, the database, disk group, and volumes will be replicated from the primary site.
  Create the directory for the CFS mount point which will host the database data and control files.
- If you are using VVR for replication, create an identical disk group and volumes for the replicated content with the same names and size as listed on the primary site.

Create the directories for the CFS mount points as they are on the primary site. These will be used to host the database and control files when the failover occurs and the secondary is promoted to become the primary site.

2 Copy the init$ORACLE_SID.ora file from $ORACLE_HOME/dbs at the primary to $ORACLE_HOME/dbs at the secondary.

3 Create subdirectories for the database as you did on the primary site.

Configuring replication on clusters at both sites

You must configure replication for the database files. Once replication is configured, make sure it is functioning correctly by testing before proceeding.

To configure replication at both sites

1 At both sites, identify the disks on which the database resides at the primary site and associate them with the corresponding disks at the secondary site.

See "Setting up replication using VVR on the primary site" on page 326.

2 Start replication between the sites.

See "Starting replication of application database volume" on page 333.

Modifying the ClusterService group for global clusters

You have configured VCS service groups for the database on each cluster. Each cluster requires an additional virtual IP address associated with the cluster for cross-cluster communication. The VCS installation and creation of the ClusterService group typically involves defining this IP address.

Configure a global cluster by setting:

- Heartbeat
- Wide area cluster (wac)
- GCO IP (gcoip)
- remote cluster resources

See the *Veritas Cluster Server User's Guide* for complete details on global clustering.

Modifying the global clustering configuration using the wizard

The global clustering wizard completes the following tasks:

- Validates the ability of the current configuration to support a global cluster environment.
- Creates the components that enable the separate clusters, each of which contains a different set of GAB memberships, to connect and operate as a single unit.
- Creates the ClusterService group, or updates an existing ClusterService group.

Run the global clustering configuration wizard on each of the clusters; you must have the global clustering license in place on each node in the cluster.

To modify the ClusterService group for global clusters using the global clustering wizard

1. On the primary cluster, start the GCO Configuration wizard:

   ```
   # /opt/VRTSvcs/bin/gcoconfig
   ```

2. The wizard discovers the NIC devices on the local system and prompts you to enter the device to be used for the global cluster. Specify the name of the device and press Enter.
3. If you do not have NIC resources in your configuration, the wizard asks you whether the specified NIC will be the public NIC used by all the systems. Enter y if it is the public NIC; otherwise enter n. If you entered n, the wizard prompts you to enter the names of NICs on all systems.
4. Enter the virtual IP address for the local cluster.
5. If you do not have IP resources in your configuration, the wizard prompts you for the netmask associated with the virtual IP. The wizard detects the netmask; you can accept the suggested value or enter another one.

   The wizard starts running commands to create or update the ClusterService group. Various messages indicate the status of these commands. After running these commands, the wizard brings the ClusterService group online.

Defining the remote cluster and heartbeat objects

After configuring global clustering, add the remote cluster object to define the IP address of the cluster on the secondary site, and the heartbeat object to define the cluster-to-cluster heartbeat.

Heartbeats monitor the health of remote clusters. VCS can communicate with the remote cluster only after you set up the heartbeat resource on both clusters.

To define the remote cluster and heartbeat

1 On the primary site, enable write access to the configuration:

```
# haconf -makerw
```

2 Define the remote cluster and its virtual IP address.

In this example, the remote cluster is clus2 and its IP address is 10.11.10.102:

```
# haclus -add clus2 10.11.10.102
```

3 Complete step 1 and step 2 on the secondary site using the name and IP address of the primary cluster.

In this example, the primary cluster is clus1 and its IP address is 10.10.10.101:

```
# haclus -add clus1 10.10.10.101
```

4 On the primary site, add the heartbeat object for the cluster. In this example, the heartbeat method is ICMP ping.

```
# hahb -add Icmp
```

5 Define the following attributes for the heartbeat resource:

- ClusterList lists the remote cluster.
- Arguments enables you to define the virtual IP address for the remote cluster.

For example:

```
# hahb -modify Icmp ClusterList clus2
# hahb -modify Icmp Arguments 10.11.10.102 -clus clus2
```

6 Save the configuration and change the access to read-only on the local cluster:

```
# haconf -dump -makero
```

7 Complete step 4-6 on the secondary site using appropriate values to define the cluster on the primary site and its IP as the remote cluster for the secondary cluster.

8 Verify cluster status with the `hastatus -sum` command on both clusters.

```
# hastatus -sum
```

```
# hastatus -sum
.........
-- WAN HEARTBEAT STATE
-- Heartbeat       To                    State

L  Icmp            clus2          ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State

M  clus2     RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system       State                Frozen

N  clus2:mercury  RUNNING              0
N  clus2:jupiter  RUNNING              0
```

9 Display the global setup by executing haclus -list command.

```
# haclus -list
     clus1
     clus2
```

Example of heartbeat additions to the main.cf file on the primary site:

```
.
.
remotecluster clus2 (
Cluster Address = "10.11.10.102"
)
heartbeat Icmp (
    ClusterList = { clus2 }
    Arguments @clus2 = { "10.11.10.102" }
    )

system galaxy (
    )
.
.
```

Example heartbeat additions to the main.cf file on the secondary site:

```
.
.
remotecluster clus1 (
    Cluster Address = "10.10.10.101"
    )

heartbeat Icmp (
    ClusterList = { clus1 }
    Arguments @clus1 = { "10.10.10.101" }
    )

system mercury (
    )
.
.
```

See the *Veritas Cluster Server User's Guide* for details for configuring the required and optional attributes of the heartbeat object.

Configuring the VCS service groups for global clusters

To configure VCS service groups for global clusters

1. Configure and enable global groups for databases and resources.
   - Configure VCS service groups at both sites.
   - Configure the replication agent at both sites.
2. To test real data in an environment where HA/DR has been configured, schedule a planned migration to the secondary site for testing purposes.

   For example:

   See "Migrating the role of primary site to the secondary site" on page 347.

   See "Migrating the role of new primary site back to the original primary site" on page 348.
3. Upon successful testing, bring the environment into production.

For complete details on VVR in a shared disk environment:

See the *Veritas Volume Replicator Administrator's Guide*.

Chapter 24

Configuring a global cluster using VVR

This chapter includes the following topics:

About configuring global clustering using VVR

Before configuring clusters for global clustering, make sure both clusters have product and database software installed and configured.

Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster and VVR enabled.

See "About Veritas product licensing" on page 49.

After setting up two clusters running SFCFS, you can configure a global cluster environment with VVR. You must modify both cluster configurations to support replication in the global cluster environment.

Configuring SFCFS for global clusters requires:

- Setting up both clusters as part of a global cluster environment.
  See "About setting up a global cluster in an SFCFS environment" on page 314.
- Setting up replication for clusters at both sites.
  See "Setting up replication using VVR on the primary site" on page 326.
  See "Setting up replication using VVR on the secondary site" on page 329.
- Starting replication of the database.
  See "Starting replication of application database volume" on page 333.
- Configuring VCS for replication on clusters at both sites.
  See "Configuring VCS to replicate the database volume using VVR" on page 335.

Setting up replication using VVR on the primary site

Setting up replication with VVR in a global cluster environment involves the following tasks:

- If you have not already done so, create a disk group on the storage on the primary site.
- Creating the Storage Replicator Log (SRL) in the disk group for the database.
  See "Creating the SRL volume on the primary site" on page 326.
- Creating the Replicated Volume Group (RVG) on the primary site.
  See "Setting up the Replicated Volume Group (RVG) on the primary site" on page 327.

Creating the SRL volume on the primary site

Create the SRL. The SRL is a volume in the RVG. The RVG also holds the data volumes for replication.

- The data volume on the secondary site has the same name and the same size as the data volume on the primary site.
- The SRL on the secondary site has the same name and the same size as the SRL on the primary site.
- The data volume and SRL volume should exist in the same disk group.
- If possible, create SRLs on disks without other volumes.
- Mirror SRLs and data volumes in the absence of hardware-based mirroring.

To create the SRL volume on the primary site

1. On the primary site, determine the size of the SRL volume based on the configuration and amount of use.

   See the Veritas Volume Replicator documentation for details.

2. Using the following command, determine whether a node is the master or the slave:

   ```
   # vxdctl -c mode
   ```

3. From the master node, issue the following command:

   ```
   # vxassist -g oradatadg make rac1_srl 1500M nmirror=2 disk4 disk5
   ```

4. Using the following command, start the SRL volume by starting all volumes in the disk group:

   ```
   # vxvol -g oradatadg startall
   ```

Setting up the Replicated Volume Group (RVG) on the primary site

Before creating the RVG on the primary site, make sure the volumes and CVM group are active and online.

To review the status of replication objects on the primary site

1. Verify the volumes you intend to include in the group are active.
2. Review the output of the `hagrp -state cvm` command to verify that the CVM group is online.
3. On each site, verify vradmin is running:

```
#  ps -ef |grep vradmin
    root  536594  598036   0 12:31:25      0  0:00 grep vradmin
```

If vradmin is not running start it:

```
# vxstart_vvr
VxVM VVR INFO V-5-2-3935 Using following ports:
heartbeat: 4145
vradmind: 8199
vxrsyncd: 8989
data: Anonymous-Ports
To change, see vrport(1M) command
#  ps -ef |grep vradmin
    root  536782       1   0 12:32:47      -  0:00 /usr/sbin/vradmind
    root 1048622  598036   0 12:32:55      0  0:00 grep vradmin
# netstat -an |grep 4145
tcp4       0      0  *.4145                 *.*          LISTEN
udp4       0      0  *.4145                 *.*
```

To create the RVG

The command to create the primary RVG takes the form:

```
vradmin -g disk_group createpri rvg_name data_volume srl_volume
```

where:

- disk_group is the name of the disk group containing the database
- rvg_name is the name for the RVG
- data_volume is the volume that VVR replicates
- srl_volume is the volume for the SRL

For example, to create the rac1_rvg RVG, enter:

```
# vradmin -g oradatadg createpri rac1_rvg rac1_vol rac1_srl
```

The command creates the RVG on the primary site and adds a Data Change Map (DCM) for each data volume. In this case, a DCM exists for rac1_vol.

Setting up replication using VVR on the secondary site

To create objects for replication on the secondary site, use the `vradmin` command with the `addsec` option. To set up replication on the secondary site, perform the following tasks:

- If you have not already done so, create a disk group to hold data volume, SRL, and RVG on the storage on the secondary site.
- Create volumes for the database and SRL on the secondary site.
  See "Creating the data and SRL volumes on the secondary site" on page 329.
- Edit the /etc/vx/vras/.rdg file on the secondary site.
  See "Editing the /etc/vx/vras/.rdg files" on page 330.
- Use resolvable virtual IP addresses that set network RLINK connections as host names of the primary and secondary sites.
  See "Setting up IP addresses for RLINKs on each cluster" on page 330.
- Create the replication objects on the secondary site.
  See "Setting up the disk group on secondary site for replication" on page 331.

Creating the data and SRL volumes on the secondary site

Note the following when creating volumes for the data and SRL:

- The sizes and names of the volumes must reflect the sizes and names of the corresponding volumes in the primary site.
- Create the data and SRL volumes on different disks in the disk group. Use the `vxdisk -g diskgroup list` command to list the disks in the disk group.
- Mirror the volumes.

To create the data and SRL volumes on the secondary site

1. In the disk group created for the application database, create a data volume of same size as that in primary for data; in this case, the rac_vol1 volume on the primary site is 6.6 GB:

```
# vxassist -g oradatadg make rac_vol1 6600M nmirror=2 disk1 disk2
```

2 Create the volume for the SRL, using the same name and size of the equivalent volume on the primary site. Create the volume on different disks from the disks for the database volume, but on the same disk group that has the data volume:

```
# vxassist -g oradatadg make rac1_srl 1500M nmirror=2 disk4 disk6
```

Editing the /etc/vx/vras/.rdg files

Editing the /etc/vx/vras/.rdg file on the secondary site enables VVR to replicate the disk group from the primary site to the secondary site. On each node, VVR uses the /etc/vx/vras/.rdg file to check the authorization to replicate the RVG on the primary site to the secondary site. The file on each node in the secondary site must contain the primary disk group ID, and likewise, the file on each primary system must contain the secondary disk group ID.

To edit the /etc/vx/vras/.rdg files

1 On a node in the primary site, display the primary disk group ID:

```
# vxprint -l diskgroup

.....
```

2 On each node in the secondary site, edit the /etc/vx/vras/.rdg file and enter the primary disk group ID on a single line.

3 On each cluster node of the primary cluster, edit the /etc/vx/vras/.rdg file and enter the secondary disk group ID on a single line.

Setting up IP addresses for RLINKs on each cluster

Creating objects with the vradmin command requires resolvable virtual IP addresses that set network RLINK connections as host names of the primary and secondary sites.

To set up IP addresses for RLINKS on each cluster

1 For each RVG running on each cluster, set up a virtual IP address on one of the nodes of the cluster. These IP addresses are part of the RLINK.

The example assumes for the cluster on the primary site:

- The public network interface is en0:1
- The virtual IP address is 10.10.9.101

- The net mask is 255.255.255.0
- ```
  # ifconfig en0 10.10.9.101 netmask 255.255.255.0 \
    broadcast 10.180.95.255 alias
    # ifconfig en0 up
  ```

2 Use the same commands with appropriate values for the interface, IP address, and net mask on the secondary site.

The example assumes for the secondary site:

- The public network interface is en0:1
- virtual IP address is 10.11.9.102
- net mask is 255.255.255.0

3 Define the virtual IP addresses to correspond to a virtual cluster host name on the primary site and a virtual cluster host name on the secondary site.

Update the /etc/hosts file on all the nodes on both the primary and secondary sites.

The examples assume:

- clus1 has IP address 10.10.9.101
- clus2 has IP address 10.11.9.102

4 Use the ping command to verify the links are functional.

Setting up the disk group on secondary site for replication

Create the replication objects on the secondary site from the master node of the primary site, using the `vradmin` command.

To set up the disk group on the secondary site for replication

1 Issue the command in the following format from the cluster on the primary site:

```
# vradmin -g dg_pri addsec rvg_pri pri_host sec_host
```

where:

- dg_pri is the disk group on the primary site that VVR will replicate. For example: rac1_vol
- rvg_pri is the RVG on the primary site. For example: rac1_rvg
```

- pri_host is the virtual IP address or resolvable virtual host name of the cluster on the primary site.
  For example: clus1_1
- sec_host is the virtual IP address or resolvable virtual host name of the cluster on the secondary site.
  For example: clus2_1

For example, the command to add the cluster on the primary site to the Replicated Data Set (RDS) is:

```
vradmin -g oradatadg addsec rac1_rvg \
clus1_1
 clus2_1
```

On the secondary site, the above command performs the following tasks:

- Creates an RVG within the specified disk group using the same name as the one for the primary site
- Associates the data and SRL volumes that have the same names as the ones on the primary site with the specified RVG
- Adds a data change map (DCM) for the data volume
- Creates cluster RLINKS for the primary and secondary sites with the default names

2 Verify the list of RVGs in the RDS by executing the following command.

```
# vradmin -g oradatadg -l printrvg
```

For example:

```
Replicated Data Set: rac1_rvg
Primary:
HostName: 10.180.88.187 <localhost>
RvgName: rac1_rvg
DgName: rac1_vol
datavol_cnt: 1
vset_cnt: 0
srl: rac1_srl
RLinks:
name=rlk_clus2_1_rac1_rvg, detached=on,
synchronous=off
Secondary:
```

```
HostName: 10.190.99.197
RvgName: rac1_rvg
DgName: oradatadg
datavol_cnt: 1
vset_cnt: 0
srl: rac1_srl
RLinks:
name=rlk_clus1_1_rac1_rvg, detached=on,
synchronous=off
```

Note: Once the replication is started the value of the detached flag will change the status from OFF to ON.

Starting replication of application database volume

When you have both the primary and secondary sites set up for replication, you can start replication from the primary site to the secondary site.

Start with the default replication settings:

- Mode of replication: synchronous=off
- Latency Protection: latencyprot=off
- SRL overflow protection: srlprot_autodcm
- Packet size: `packet_size=8400`
- Network protocol: `protocol=UDP`

Method of initial synchronization:

- Automatic synchronization
- Full synchronization with Checkpoint

For guidelines on modifying these settings and information on choosing the method of replication for the initial synchronization:

See the *Veritas Volume Replicator Administrator's Guide*

Starting replication using automatic synchronization

Use the `vradmin` command to start replication or the transfer of data from the primary site to the secondary site over the network. Because the cluster on the secondary site uses only one host name, the command does not require the *sec_host* argument.

To start replication using automatic synchronization

- From the primary site, use the following command to automatically synchronize the RVG on the secondary site:

  ```
  vradmin -g disk_group -a startrep pri_rvg sec_host
  ```

  where:

  - disk_group is the disk group on the primary site that VVR will replicate
  - pri_rvg is the name of the RVG on the primary site
  - sec_host is the virtual host name for the secondary site

  For example:

  ```
  # vradmin -g oradatadg -a startrep rac1_rvg
        clus2
  ```

Starting replication using full synchronization with Checkpoint

Use the `vradmin` command with the Checkpoint option to start replication using full synchronization with Checkpoint.

To start replication using full synchronization with Checkpoint

1. From the primary site, synchronize the RVG on the secondary site with full synchronization (using the `-c checkpoint` option):

   ```
   vradmin -g disk_group -full -c ckpt_name syncrvg pri_rvg sec_host
   ```

   where:

   - disk_group is the disk group on the primary site that VVR will replicate
   - ckpt_name is the name of the checkpoint on the primary site
   - pri_rvg is the name of the RVG on the primary site
   - *sec_host* is the virtual host name for the secondary site

   For example:

```
# vradmin -g oradatadg -c rac1_ckpt syncrvg rac1_rvg
clus2
```

2 To start replication after full synchronization, enter the following command:

```
# vradmin -g oradatadg -c rac1_ckpt startrep rac1_rvg
clus2
```

Verifying replication status

Verify that replication is properly functioning.

To verify replication status

1 Check the status of VVR replication:

```
# vradmin -g disk_group_name repstatus rvg_name
```

2 Review the `flags` output for the status. The output may appear as `connected` and `consistent`. For example:

```
# vxprint -g oradatadg -l rlk_clus2_1_rac1_rvg
  Rlink: rlk_clus2_1_rac1_rvg
  info: timeout=500 packet_size=8400 rid=0.1078
      latency_high_mark=10000 latency_low_mark=9950
      bandwidth_limit=none
  state: state=ACTIVE
      synchronous=off latencyprot=off srlprot=autodcm
  .
  .
  protocol: UDP/IP
  checkpoint: rac1_ckpt
  flags: write enabled attached consistent connected
 asynchronous
```

Configuring VCS to replicate the database volume using VVR

After configuring both clusters for global clustering and setting up the application database for replication, configure VCS to provide high availability for the database. Specifically, configure VCS agents to control the cluster resources, including the replication resources.

About modifying the VCS configuration for replication

The following resources must be configured or modified for replication:

- Log owner group
- RVG group
- CVMVolDg resource
- RVGSharedPri resource
- application database service group

For more information on service replication resources:

See the *Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide*.

Log owner group

Create a log owner group including the RVGLogowner resources. The RVGLogowner resources are used by:

- RLINKs for the RVG
- RVGLogowner resource. The RVG and its associated disk group are defined as attributes for the RVGLogowner resource.

The RVG log owner service group has an online local firm dependency on the service group containing the RVG.

The VCS uses the following agents to control the folllowing resources:

- RVGLogowner agent to control the RVGLogowner resource
- RVGShared agent to control the RVGShared resource

RVG group

Create an RVG group that includes the RVGShared resource replication objects. Define the RVGShared resource and CVMVolDg resource together within a parallel service group. The group is defined as parallel because it may be online at the same time on all cluster nodes.

CVMVolDg resource

The CVMVolDg resource does not have volumes specified for the CVMVolume attribute; the volumes are contained in the RVG resource. The CVMVolume attribute for the CVMVolDg resource is empty because all volumes in the RVG are defined by the RVG attribute of the RVGShared resource. The RVG service group has an online local firm dependency on the CVM service group.

For a detailed description of the CVMVolDg agent in this guide:

See " CVMVolDg agent" on page 437.

RVGSharedPri resource

Add the RVGSharedPri resource to the existing application database service group. The CVMVolDg resource must be removed from the existing application database service group.

application database service group

The existing application database service group is a parallel group consisting of the application database resource, CVMVolDg resource, and CFSMount resource (if the database resides in a cluster file system). Define the application service group as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.

Modifying the VCS Configuration on the Primary Site

The following are the procedural highlights required to modify the existing VCS configuration on the primary site:

- Configure two service groups:
  - A log owner group including the RVGLogowner resource.
  - An RVG group including the RVGShared resource replication objects.
- Add the RVGSharedPri resource to the existing application database service group and define this group as a global group by setting the ClusterList and ClusterFailOverPolicy attributes.
- Move the CVMVolDg resource from the existing application database service group to the newly created RVG group.

To modify VCS on the primary site

1. Log into one of the nodes on the primary cluster.
2. Use the following command to save the existing configuration to disk, and make the configuration read-only while you make changes:

```
# haconf -dump -makero
```

3. Use the following command to make a backup copy of the main.cf file:

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

4 Use vi or another text editor to edit the main.cf file. Review the sample configuration file after the SFCFS installation.

Add a failover service group using the appropriate values for your cluster and nodes. Include the following resources:

- RVGLogowner resource. The node on which the group is online functions as the log owner (node connected to the second cluster for the purpose of replicating data).
- IP resource
- NIC resources

The following are examples of RVGLogowner service group for the different platforms.

```
group rlogowner (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoStartList = { galaxy,nebula }
    )

    IP logowner_ip (
        Device = en0
        Address = "10.10.9.101"
        NetMask = "255.255.255.0"
        )

    NIC nic (
        Device = en0
        NetworkType = ether
        NetworkHosts = "10.10.8.1"
        )

RVGLogowner logowner (
     RVG = rac1_rvg
     DiskGroup = oradatadg
     )
requires group RVGgroup online local firm
logowner requires logowner_ip
logowner_ip requires nic
```

5 Add the RVG service group using the appropriate values for your cluster and nodes.

Example `RVGgroup` service group:

```
group RVGgroup (
     SystemList = { galaxy = 0, nebula = 1 }
     Parallel = 1
     AutoStartList = { galaxy,nebula }
     )

RVGShared racdata_rvg (
     RVG = rac1_rvg
     DiskGroup = oradatadg
     )
     CVMVolDg racdata_voldg (
         CVMDiskGroup = oradatadg
         CVMActivation = sw
         )
requires group cvm online local firm
racdata_rvg requires racdata_voldg
```

6 Modify the application service group using the appropriate values for your cluster and nodes:

- Define the application service group as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute. See the bolded attribute in the example that follows.
- Add the ClusterFailOverPolicy cluster attribute. Symantec recommends using the Manual value. See the bolded attribute in the example.
- Add the RVGSharedPri resource to the group configuration.
- Remove the CVMVolDg resource, if it has been configured in your previous configuration. This resource is now part of the RVG service group.
- Specify the service group (online, local, firm) to depend on the RVG service group.
- Remove the existing dependency of the Database service group on the CVM service group. Remove the line:

  ```
  requires group CVM online local firm
  ```

- Remove the existing dependency between the CFSMount for the database and the CVMVoldg for the application database. Remove the line:

```
    oradata_mnt requires oradata_voldg
```

The following is an example of an application database service group configured for replication:

```
group database_grp (
    SystemList = { galaxy = 0, nebula = 1 }
    ClusterList = { clus1 = 0, clus2 = 1 }
    Parallel = 1
    ClusterFailOverPolicy = Manual
    Authority = 1
    AutoStartList = { galaxy,nebula }
    )

    CFSMount oradata_mnt (
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/rac1_vol"
        )

    RVGSharedPri ora_vvr_shpri (
       RvgResourceName = racdata_rvg
       OnlineRetryLimit = 0
       )

requires group RVGgroup online local firm
oradata_mnt requires ora_vvr_shpri
```

7 Save and close the main.cf file.

8 Use the following command to verify the syntax of the /etc/VRTSvcs/conf/config/main.cf file:

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

9 Stop and restart VCS.

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

Wait for port h to stop on all nodes, and then restart VCS with the new configuration on all primary nodes:

```
# hastart
```

Modifying the VCS Configuration on the Secondary Site

The following are highlights of the procedure to modify the existing VCS configuration on the secondary site:

- Add the log owner and RVG service groups.
- Add a service group to manage the application database and the supporting resources.
- Define the replication objects and agents, such that the cluster at the secondary site can function as a companion to the primary cluster.

The following steps are similar to those performed on the primary site.

To modify VCS on the secondary site

1. Log into one of the nodes on the secondary site as root.
2. Use the following command to save the existing configuration to disk, and make the configuration read-only while making changes:

   ```
   # haconf -dump -makero
   ```

3. Use the following command to make a backup copy of the main.cf file:

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

4. Use vi or another text editor to edit the main.cf file. Edit the CVM group on the secondary site.

   Review the sample configuration file after the SFCFS installation to see the CVM configuration.

   In our example, the secondary site has clus2 consisting of the nodes mercury and jupiter. To modify the CVM service group on the secondary site, use the CVM group on the primary site as your guide.

5. Add a failover service group using the appropriate values for your cluster and nodes. Include the following resources:

   - RVGLogowner resource. The node on which the group is online functions as the log owner (node connected to the second cluster for the purpose of replicating data).
   - IP resource
   - NIC resources

   Example `RVGLogowner` service group:

```
group rlogowner (
    SystemList = { mercury = 0, jupiter = 1 }
    AutoStartList = { mercury, jupiter }
    )

    IP logowner_ip (
       Device = en0
       Address = "10.11.9.102"
       NetMask = "255.255.255.0"
       )

NIC nic (
       Device = en0
       NetworkHosts = { "10.10.8.1" }
       NetworkType = ether
       )

RVGLogowner logowner (
       RVG = rac1_rvg
       DiskGroup = oradatadg
       )

requires group RVGgroup online local firm
logowner requires logowner_ip
logowner_ip requires nic
```

6 Add the RVG service group using the appropriate values for your cluster and nodes.

The following is an example `RVGgroup` service group:

```
group RVGgroup (
    SystemList = { mercury = 0, jupiter = 1 }
    Parallel = 1
    AutoStartList = { mercury, jupiter }
    )

RVGShared racdata_rvg (
    RVG = rac1_rvg
    DiskGroup = oradatadg
    )

    CVMVolDg racdata_voldg
        CVMDiskGroup = oradatadg
        CVMActivation = sw
        )

requires group cvm online local firm
racdata_rvg requires racdata_voldg
```

7 Add an application service group. Use the application service group on the primary site as a model for the application service group on the secondary site.

- Define the application service group as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.
- Assign this global group the same name as the group on the primary site; for example, *database_grp*.
- Include the ClusterList and ClusterFailOverPolicy cluster attributes. Symantec recommends using the Manual value.
- Add the RVGSharedPri resource to the group configuration.
- Remove the CVMVolDg resource, if it has been configured in your previous configuration. This resource is now part of the RVG service group.
- Specify the service group to depend (online, local, firm) on the RVG service group.

Example of the application group on the secondary site:

```
group database_grp (
    SystemList = { mercury = 0, jupiter = 1 }
    ClusterList = { clus2 = 0, clus1 = 1 }
    Parallel = 1
    OnlineRetryInterval = 300
    ClusterFailOverPolicy = Manual
    Authority = 1
    AutoStartList = { mercury, jupiter }
    )

    RVGSharedPri ora_vvr_shpri (
        RvgResourceName = racdata_rvg
        OnlineRetryLimit = 0
        )


    CFSMount oradata_mnt (
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/racdb_vol"
        Critical = 0
        )


      RVGSharedPri ora_vvr_shpri (
        RvgResourceName = racdata_rvg
        OnlineRetryLimit = 0
        )

requires group RVGgroup online local firm
oradata_mnt requires ora_vvr_shpri
```

8 Save and close the `main.cf` file.

9 Use the following command to verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file:

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

10 Stop and restart VCS.

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

Wait for port h to stop on all nodes, and then restart VCS with the new configuration on all primary nodes:

```
# hastart
```

11 Verify that VCS brings all resources online. On one node, enter the following command:

```
# hagrp -display
```

The application, RVG, and CVM groups are online on both nodes of the primary site. The RVGLogOwner group is online on one node of the cluster. If either the RVG group or the RVGLogOwner group is partially online, manually bring the groups online using the `hagrp -online` command. This information applies to the secondary site, except for the application group which must be offline.

On the primary site, enter the following commands:

```
# hagrp -online rlogowner -sys galaxy

# hagrp -online database_grp -sys galaxy

VCS WARNING V-16-1-50817 Please use hagrp -online -force to
online a global group for the first time

# hagrp -online -force database_grp -sys galaxy
```

On the secondary site, enter the following command:

```
# hagrp -online rlogowner -sys mercury
```

12 Verify the service groups and their resources that are brought online. On one node, enter the following command:

```
# hagrp -display
```

The application service group is offline on the secondary site, but the CVM, RVG log owner, and RVG groups are online.

This completes the setup for an SFCFS global cluster using VVR for replication. Symantec recommends testing a global cluster before putting it into production.

Using VCS commands on SFCFS global clusters

For information on the VCS commands for global clusters:

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

Using VVR commands on SFCFS global clusters

If you have two SFCFS clusters configured to use VVR for replication, the following administrative functions are available:

- Migration of the role of the primary site to the remote site
- Takeover of the primary site role by the secondary site

About migration and takeover of the primary site role

Migration is a planned transfer of the role of primary replication host from one cluster to a remote cluster. This transfer enables the application on the remote cluster to actively use the replicated data. The former primary cluster becomes free for maintenance or other activity.

Takeover occurs when an unplanned event (such as a disaster) causes a failure, making it necessary for the applications using the replicated data to be brought online on the remote cluster.

Migrating the role of primary site to the secondary site

After configuring the replication objects within VCS, you can use VCS commands to migrate the role of the cluster on the primary site to the remote cluster. In the procedure below, VCS takes the replicated database service group, *database_grp*, offline on the primary site and brings it online on the secondary site; the secondary site now assumes the role of the primary site.

Note: The `hagrp -switch` command cannot migrate a parallel group within a cluster or between clusters in a global cluster environment.

To migrate the role of primary site to the remote site

1. From the primary site, use the following command to take the Oracle service group offline on all nodes.

   ```
   # hagrp -offline database_grp -any
   ```

   Wait for VCS to take all Oracle service groups offline on the primary site.

2. Verify that the RLINK between the primary and secondary is up to date. Use the `vxrlink -g` command with the status option and specify the RLINK for the primary cluster. You can use the command from any node on the primary cluster.

   For example:

   ```
   # vxrlink -g data_disk_group status rlk_clus1_priv_rac1_rvg
   ```

   Where rlk_clus1_priv_rac1_rvg is the RLINK.

3. On the secondary site, which is now the new primary site, bring the Oracle service group online on all nodes:

   ```
   # hagrp -online database_grp -any
   ```

Migrating the role of new primary site back to the original primary site

After migrating the role of the primary site to the secondary site, you can use VCS commands to migrate the role of the cluster on the new primary site to the original primary site. In the procedure below, VCS takes the replicated database service group, *database_grp*, offline on the new primary (former secondary) site and brings it online on the original primary site; the original primary site now resumes the role of the primary site.

Note: The `hagrp -switch` command cannot migrate a parallel group within a cluster or between clusters in a global cluster environment.

To migrate the role of new primary site back to the original primary site

1 Make sure that all CRS resources are online, and switch back the group *database_grp* to the original primary site.

Issue the following command on the remote site:

```
# hagrp -offline database_grp -any
```

2 Verify that the RLINK between the primary and secondary is up to date. Use the `vxrlink -g` command with the status option and specify the RLINK for the primary cluster. You can use the command from any node on the primary cluster.

For example:

```
# vxrlink -g data_disk_group status rlk_clus1_priv_rac1_rvg
```

Where rlk_clus1_priv_rac1_rvg is the RLINK.

3 Make sure that *database_grp* is offline on the new primary site. Then, execute the following command on the original primary site to bring the *database_grp* online:

```
# hagrp -online database_grp -any
```

Taking over the primary role by the remote cluster

Takeover occurs when the remote cluster on the secondary site starts the application that uses replicated data. This situation may occur if the secondary site perceives the primary site as dead, or when the primary site becomes inaccessible (perhaps for a known reason). For a detailed description of concepts of taking over the primary role:

See the *Veritas Volume Replicator Administrator's Guide*.

Before enabling the secondary site to take over the primary role, the administrator on the secondary site must "declare" the type of failure at the remote (primary, in this case) site and designate the failure type using one of the options for the `haclus` command.

Takeover options are:

- Disaster
- Outage

- Disconnect
- Replica

Disaster

When the cluster on the primary site is inaccessible and appears dead, the administrator declares the failure type as "disaster." For example, fire may destroy a data center, including the primary site and all data in the volumes. After making this declaration, the administrator can bring the service group online on the secondary site, which now has the role as "primary" site.

Outage

When the administrator of a secondary site knows the primary site is inaccessible for a known reason, such as a temporary power outage, the administrator may declare the failure as an "outage." Typically, an administrator expects the primary site to return to its original state.

After the declaration for an outage occurs, the RVGSharedPri agent enables DCM logging while the secondary site maintains the primary replication role. After the original primary site becomes alive and returns to its original state, DCM logging makes it possible to use fast fail back resynchronization when data is resynchronized to the original cluster.

Before attempting to resynchronize the data using the fast fail back option from the current primary site to the original primary site, take the precaution at the original primary site of making a snapshot of the original data. This action provides a valid copy of data at the original primary site for use in the case the current primary site fails before the resynchronization is complete.

See “Examples for takeover and resynchronization” on page 351.

See “Replica” on page 351.

Disconnect

When both clusters are functioning properly and the heartbeat link between the clusters fails, a split-brain condition exists. In this case, the administrator can declare the failure as "disconnect," which means no attempt will occur to take over the role of the primary site at the secondary site. This declaration is merely advisory, generating a message in the VCS log indicating the failure results from a network outage rather than a server outage.

Replica

In the rare case where the current primary site becomes inaccessible while data is resynchronized from that site to the original primary site using the fast fail back method, the administrator at the original primary site may resort to using a data snapshot (if it exists) taken before the start of the fast fail back operation. In this case, the failure type is designated as "replica".

Examples for takeover and resynchronization

The examples illustrate the steps required for an outage takeover and resynchronization.

To take over after an outage

1 From any node of the secondary site, issue the `haclus` command:

```
# haclus -declare outage -clus rac_cluster101
```

2 After declaring the state of the remote cluster, bring the Oracle service group online on the secondary site. For example:

```
# hagrp -online -force database_grp -any
```

To resynchronize after an outage

1. On the original primary site, create a snapshot of the RVG before resynchronizing it in case the current primary site fails during the resynchronization. Assuming the disk group is *data_disk_group* and the RVG is rac1_rvg, type:

   ```
   # vxrvg -g data_disk_group -F snapshot rac1_rvg
   ```

   See the *Veritas Volume Replicator Administrator's Guide* for details on RVG snapshots.

2. Resynchronize the RVG. From the CVM master node of the current primary site, issue the `hares` command and the `-action` option with the fbsync action token to resynchronize the RVGSharedPri resource. For example:

   ```
   # hares -action ora_vvr_shpri fbsync -sys mercury
   ```

   To determine which node is the CVM master node, type:

   ```
   # vxdctl -c mode
   ```

3. Perform one of the following commands, depending on whether the resynchronization of data from the current primary site to the original primary site is successful:

   - If the resynchronization of data is successful, use the `vxrvg` command with the `snapback` option to reattach the snapshot volumes on the original primary site to the original volumes in the specified RVG:

     ```
     # vxrvg -g data_disk_group snapback rac1_rvg
     ```

   - A failed attempt at the resynchronization of data (for example, a disaster hits the primary RVG when resynchronization is in progress) could generate inconsistent data.
     You can restore the contents of the RVG data volumes from the snapshot taken in step 1:

     ```
     # vxrvg -g data_disk_group snaprestore rac1_rvg
     ```

Troubleshooting CVM and VVR components of SFCFS

The following topic is useful for troubleshooting the VVR component of SFCFS.

Updating the rlink

If the rlink is not up to date, use the `hares -action` command with the `resync` action token to synchronize the RVG.

The following command example is issued on any node (`galaxy`, in this case) in the primary cluster, specifying the RVGSharedPri resource, `ora_vvr_shpri`:

```
# hares -action ora_vvr_shpri resync -sys galaxy
```

VCS agents to manage wide-area failover

VCS agents now manage external objects that are part of wide-area failover. These objects include replication, DNS updates, and so on. These agents provide a robust framework for specifying attributes and restarts, and can be brought online upon fail over.

VCS provides agents for other array-based or application-based solutions. This section covers the replication agents that is bundled with VVR. See the VCS replication agent documentation for more details.

Note: See the Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide for more information about the RVG and RVGPrimary agents.

Note: The RVGSnapshot agent is not supported for SFCFS.

DNS agent

The DNS agent updates the canonical name-mapping in the domain name server after a wide-area failover. See the Veritas Cluster Server Bundled Agents Reference Guide for more information about the agent.

RVG agent

The RVG agent manages the Replicated Volume Group (RVG). Specifically, it brings the RVG online, monitors read-write access to the RVG, and takes the RVG offline. Use this agent when using VVR for replication.

RVGPrimary agent

The RVGPrimary agent attempts to migrate or take over a Secondary to a Primary following an application failover. The agent has no actions associated with the offline and monitor routines.

Section 8

Uninstallation of Storage Foundation Cluster File System

Chapter 25

Uninstalling Storage Foundation Cluster File System

This chapter includes the following topics:

Preparing to uninstall a SFCFS product

Complete the following preparations to uninstall a SFCFS product.

Warning: Failure to follow the preparations that are outlined in this chapter can result in loss of data.

To remove Veritas SFCFS, complete the following preparations before the uninstallation:

- Back up all VxFS file systems in full and move the files in all VxFS file systems to native file systems backed with LVM logical volumes. Raw application data stored in VxVM logical volumes must be moved to LVM logical volumes.
- Remove all but one copy of file systems and databases.
- Remove all but one plex from volumes that contain multiple plexes (mirrors). To display a list of all volumes, use the command:

  ```
  # vxprint -Ath
  ```

  To remove a plex, use the command:

  ```
  # vxplex -g diskgroup -o rm dis plex
  ```

- If a remaining plex contains multiple subdisks, consolidate the subdisks into a single subdisk using the commands:

  ```
  # vxassist -g diskgroup mirror volume layout=contig
    # vxplex -g diskgroup -o rm dis plex
  ```

  Sufficient space on another disk is required for this operation to complete.
- Modify `/etc/filesystems` to remove or change entries for VxFS file systems that were moved to native file systems.
- Move all data from volumes created from multiple regions of storage, including striped or spanned volumes, onto a single disk or appropriate LVM logical volume. This can be done using one of the following three methods:
  - Back up the system to tape or other media and recover the system from this.
  - Move volumes incrementally (evacuate) onto logical volumes. Evacuation moves subdisks from the source disks to target disks. The evacuated disks provide the initial free disk space for volumes to be moved to LVM volumes. See "Moving volumes to physical disks" on page 359.

Shutting down cluster operations

If the systems are running as an HA cluster, you have to take all service groups offline and shutdown VCS.

To take all service groups offline and shutdown VCS

- Use the `hastop` command as follows:

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

Warning: Do not use the `-force` option when executing `hastop`. This will leave all service groups online and shut down VCS, causing undesired results during uninstallation of the packages.

Moving volumes to physical disks

You can use the following steps to move data off of VxVM volumes.

To move data off of VxVM volumes

1. Evacuate as many disks as possible by using one of the following methods:
   - the "Remove a disk" option in `vxdiskadm`
   - the Veritas Enterprise Administrator
   - the `vxevac` script from the command line.
2. Remove the evacuated disks from Veritas Volume Manager control using the following commands:

```
# vxdg -g diskgroup rmdisk disk_media_name
# /usr/lib/vxvm/bin/vxdiskunsetup -C disk_access_name
# vxdisk rm disk_access_name
```

   For example:

```
# vxdg -g mydg rmdisk mydg01
# /usr/lib/vxvm/bin/vxdiskunsetup -C hdisk1
# vxdisk rm hdisk01
```

3. Decide which volume to move first. If the volume to be moved is mounted, unmount it. If the volume is being used as a raw partition for database applications, make sure that the application is not updating the volume and that data on the volume has been synchronized.

4 On the free disk space, create an LVM logical volume that is the same size as the VxVM volume. If there is not enough free space for the logical volume, add a new disk to the system for the first volume to be removed. For subsequent volumes, you can use the free space generated by the removal of the first volume.

5 Copy the data on the volume onto the newly created LVM logical volume using the following command:

```
# dd if=/dev/vx/dsk/diskgroup/volume of=/dev/vgvol
```

where *diskgroup* is the name of a VxVM disk group, *volume* is the old volume in that disk group, and *vgvol* is a newly created LVM volume.

If the volume contains a VxFS file system, the user data managed by VxFS in the volume must be backed up or copied to a native AIX file system in an LVM logical volume.

6 The entries in `/etc/filesystems` for volumes holding VxFS file systems, that were copied to native file systems in step 5, must be modified according to the change in step 5.

7 Mount the disk if the corresponding volume was previously mounted.

8 Remove the volume from VxVM using the following command:

```
# vxedit -g diskgroup -rf rm volume
```

9 Remove any disks that have become free (have no subdisks defined on them) by removing volumes from VxVM control. To check if there are still some subdisks remaining on a particular disk, use the following command:

```
# vxprint -g diskgroup -F "%sdnum" disk_media_name
```

10 If the return code is not 0, there are still some subdisks on this disk that must be subsequently removed. If the return code is 0, remove the disk from VxVM control using the following commands:

```
# vxdg -g diskgroup rmdisk disk_media_name
# vxdisk rm disk_access_name
```

11 Copy the data in the next volume to be removed to the newly created free space.

12 Reboot the system after all volumes have been converted successfully. Verify that no open volumes remain after the system reboot using the following command:

```
# vxprint -Aht -e v_open
```

13 If any volumes remain open, repeat the steps listed above.

Disabling the agents on a system

This section explains how to disable a VCS agent for VVR on a system. To disable an agent, you must change the service group containing the resource type of the agent to an OFFLINE state. Then, you can stop the application or switch the application to another system.

To disable the agents

1 Check whether any service group containing the resource type of the agent is online by typing the following command:

```
# hagrp -state service_group -sys system_name
```

If none of the service groups is online, skip to 3.

2 If the service group is online, take it offline.

To take the service group offline without bringing it online on any other system in the cluster, enter:

```
# hagrp -offline service_group -sys system_name
```

3 Stop the agent on the system by entering:

```
# haagent -stop agent_name -sys system_name
```

When you get the message `Please look for messages in the log file`, check the file `/var/VRTSvcs/log/engine_A.log` for a message confirming that each agent has stopped.

You can also use the `ps` command to confirm that the agent is stopped.

4 Remove the system from the `SystemList` of the service group. If you disable the agent on all the systems in the `SystemList`, you can also remove the service groups and resource types from the VCS configuration.

Read information on administering VCS from the command line.

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

Removing the Replicated Data Set

If you use VVR, you need to perform the following steps. This section gives the steps to remove a Replicated Data Set (RDS) when the application is either active or stopped.

To remove the Replicated Data Set

1. Verify that all RLINKs are up-to-date:

   ```
   # vxrlink -g diskgroup status rlink_name
   ```

   If the Secondary is not required to be up-to-date, proceed to 2 and stop replication using the `-f` option with the `vradmin stoprep` command.

2. Stop replication to the Secondary by issuing the following command on any host in the RDS:

   The `vradmin stoprep` command fails if the Primary and Secondary RLINKs are not up-to-date. Use the `-f` option to stop replication to a Secondary even when the RLINKs are not up-to-date.

   ```
   # vradmin -g diskgroup stoprep local_rvgname sec_hostname
   ```

   The argument `local_rvgname` is the name of the RVG on the local host and represents its RDS.

   The argument `sec_hostname` is the name of the Secondary host as displayed in the output of the `vradmin printrvg` command.

3. Remove the Secondary from the RDS by issuing the following command on any host in the RDS:

   ```
   # vradmin -g diskgroup delsec local_rvgname sec_hostname
   ```

   The argument local_rvgname is the name of the RVG on the local host and represents its RDS.

   The argument sec_hostname is the name of the Secondary host as displayed in the output of the `vradmin printrvg` command.

4 Remove the Primary from the RDS by issuing the following command on the Primary:

```
# vradmin -g diskgroup delpri local_rvgname
```

When used with the `-f` option, the `vradmin delpri` command removes the Primary even when the application is running on the Primary.

The RDS is removed.

5 If you want to delete the SRLs from the Primary and Secondary hosts in the RDS, issue the following command on the Primary and all Secondaries:

```
# vxedit -r -g diskgroup rm srl_name
```

Uninstalling SFCFS with the Veritas Web-based installer

This section describes how to uninstall Storage Foundation Cluster File System or Storage Foundation Cluster File System High Availability with the Veritas Web-based installer.

To uninstall SFCFS

1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 65.

3 On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.

4 Select Storage Foundation Cluster File System or Storage Foundation Cluster File System High Availability from the Product drop-down list, and click **Next**.

5 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Validate**.

6 After the validation completes successfully, click **Next** to uninstall SFCFS on the selected system.

7 If there are any processes running on the target system, the installer stops the processes. Click **Next**.

8 After the installer stops the processes, the installer removes the products from the specified system.

Click **Next**.

9 After the uninstall completes, the installer displays the location of the summary, response, and log files. If required, view the files to confirm the status of the removal.

10 Click **Finish**.

The Web-based installer prompts you for another task.

Uninstalling SFCFS filesets using the script-based installer

Use the following procedure to remove SFCFS products.

Not all filesets may be installed on your system depending on the choices that you made when you installed the software.

See "About configuring secure shell or remote shell communication modes before installing products" on page 411.

To shut down and remove the installed SFCFS filesets

1 Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/filesystems`. Failing to remove these entries could result in system boot problems later.

2 Unmount all mount points for VxFS file systems.

```
# umount /mount_point
```

3 If the VxVM package (`VRTSvxvm`) is installed, read and follow the uninstallation procedures for VxVM.

4 Stop the VEA Service.

```
# /opt/VRTS/bin/vxsvcctrl stop
```

5 Make sure you have performed all of the prerequisite steps.

6 In an HA configuration, stop VCS processes on either the local system or all systems.

To stop VCS processes on the local system:

```
# hastop -local
```

To stop VCS processes on all systems:

```
# hastop -all
```

7 Move to the `/opt/VRTS/install` directory and run the uninstall script.

```
# cd /opt/VRTS/install
```

For Veritas Storage Foundation Cluster File System

```
# ./uninstallsfcfs
```

8 The uninstall script prompts for the system name. Enter one or more system names, separated by a space, from which to uninstall SFCFS, for example, `host1`:

```
Enter the system names separated by spaces from which to
uninstall Storage Foundation: host1
```

9 The uninstall script prompts you to select Storage Foundation Cluster File System or Storage Foundation Cluster File System High Availability.

10 The uninstall script prompts you to stop the product processes. If you respond yes, the processes are stopped and the filesets are uninstalled.

The uninstall script creates log files and displays the location of the log files.

11 Most filesets have kernel components. In order to ensure complete removal, a system reboot is recommended after all filesets have been removed.

Removing Storage Foundation products using SMIT

Use the following procedure to remove Storage Foundation products using SMIT.

To remove the packages using SMIT

1 Enter this command to invoke SMIT:

```
# smit
```

2 In SMIT, select **Software Installation and Maintenance** > **Software Maintenance and Utilities** > **Remove Installed Software**.

3 Under the "SOFTWARE name" menu, press F4 or Esc-4 to list all software installed on the system.

4 Enter "/" for Find, type "VRTS" to find all Veritas packages, and select the packages that you want to remove.

5 Reboot the system after removing all Storage Foundation packages.

6 Depending on the choices that were made when Storage Foundation was originally installed, you may find that not all of the listed Storage Foundation packages are installed on the system. You may also choose to remove the `VRTSvlic` licensing package unless this is required by other Veritas software.

Uninstalling Storage Foundation Cluster File System

If you need to uninstall SFCFS software. Use the `uninstallsfcfs` script.

To uninstall SFCFS HA

1 Log in as superuser.

2 Stop the cluster:

```
# hastop -all
```

Do not use the `hastop -force` command to stop VCS.

3 Change directory to `/opt/VRTS/install`:

```
# cd /opt/VRTS/install
```

4 Run the `uninstallsfcfs` command to uninstall SFCFS. The `uninstallsfcfs` script uses ssh to communicate with remote nodes as default:

```
# ./uninstallsfcfs
```

If you want to use rsh you must specify on the command line:

```
# ./uninstallsfcfs -rsh
```

5 Enter the system names to uninstall SFCFS.

```
Enter the system names separated by spaces on which to
uninstall SFCFS: system01 system02
```

6 Enter **y** to uninstall SFCFS.

```
Are you sure you want to uninstall SFCFS? [y,n,q] (y)
```

Removing the CP server configuration using the removal script

This section describes how to remove the CP server configuration from a node or cluster hosting the CP server.

Warning: Ensure that no SFCFS cluster is using the CP server that will have its CP server configuration removed.

A configuration utility that is part of VRTScps package is used to remove the CP server configuration. When using the configuration utility, a configuration removal script is run and the following tasks are performed:

- All CP server configuration files are removed
- The VCS configuration for CP server is removed

After running the utility and script, you can then uninstall VCS from the node or cluster.

Note: The configuration script has to run only once per CP server (which can be on a single node or SFHA cluster), when removing the CP server configuration.

The configuration utility performs the following steps to remove the CP server configuration:

- Takes the the CP server service group (CPSSG) offline, if it is online
- Removes the CPSSG service group from the VCS configuration

The following procedure describes how to remove the CP server configuration.

To remove the CP server configuration

1 To run the configuration removal script, enter the following command on the node where you want to remove the CP server configuration:

```
root@mycps1.symantecexample.com # /opt/VRTScps/bin/configure_cps.pl
```

2 The Veritas Coordination Point Server Configuration utility appears with an option menu.

```
VERITAS COORDINATION POINT SERVER CONFIGURATION UTILITY
=======================================================

Select one of the following:

[1] Configure Coordination Point Server on single node VCS system

[2] Configure Coordination Point Server on SFHA cluster

[3] Unconfigure Coordination Point Server
```

3 Select option 3 to unconfigure the Coordination Point Server.

4 A warning appears and prompts you to confirm the action to unconfigure the Coordination Point Server.

Enter "y" to proceed.

```
WARNING: Unconfiguring Coordination Point Server stops the
vxcpserv process. VCS clusters using this server for
coordination purpose will have one less coordination point.

Are you sure you want to bring down the cp server? (y/n)
(Default:n) :y
```

5 After entering "y" to proceed, messages appear informing you of the progress in removing the CP server configuration.

When the CP server configuration has been unconfigured, a success message appears.

For an example of the messages from a single node VCS cluster:

```
A single node VCS cluster is currently configured.
Stopping the CP server ...

Removing the CP Server from VCS configuration..

Removing resource dependencies...
Deleting the resources configured under CPSSG service group...
Deleting the CPSSG service group...

Successfully unconfigured the Veritas Coordination Point Server.
```

For an example of the messages from a CP server on an SFHA cluster:

```
A multinode CP Server cluster is currently configured.
Stopping the CP server ...

Removing the CP Server from VCS configuration..

Removing resource dependencies...
Deleting the resources configured under CPSSG service group...
Deleting the CPSSG service group...

Successfully unconfigured the Veritas Coordination Point Server.
```

6 You are then prompted to delete the CP server database. Enter "y" to delete the database. For example:

```
Do you want to delete the CP Server database? (y/n) (Default:n) :
```

7 Enter "y" at the prompt to confirm the deletion of the CP server database.

```
Warning: This database won't be available if CP server
is reconfigured on the cluster. Are you sure you want to
proceed with the deletion of database? (y/n) (Default:n) :
```

8 Enter "y" to delete the CP server configuration file and log files. For example:

```
Do you want to delete the CP Server configuration file
(/etc/vxcps.conf) and log files (in /var/VRTScps)? (y/n)
(Default:n) : y
```

9 Run the `hagrp -state` command to ensure that the CPSSG service group has been removed from the node. For example:

```
root@mycps1.symantecexample.com # hagrp -state CPSSG

VCS WARNING V-16-1-40131 Group CPSSG does not exist
in the local cluster
```

Removing the Storage Foundation for Databases (SFDB) repository after removing the product

After removing the product, you can remove the SFDB repository file and any backups.

Removing the SFDB repository file will disable the SFDB tools.

To remove the SFDB repository

1 Change directories to the location of the local lookup information for the Oracle SID.

For example:

```
# cd /var/vx/vxdba/$ORACLE_SID
```

2 Identify the SFDB repository file and any associated links:

For example:

```
# ls -al

lrwxrwxrwx   1 oracle   oinstall      26 Jul 21 13:58 .sfdb_rept -> \
/ora_data1/TEST/.sfdb_rept

# cd /ora_data1/TEST
```

Follow the symlink of .sfdb_rept.

3 Remove the repository directory containing the repository file and all backups.

For example:

```
# rm -rf .sfdb_rept
```

4 Remove the local lookup directory for the Oracle SID:

```
# cd /var/vx/vxdba
```

```
# rm -rf $ORACLE_SID
```

This completes the removal of the SFDB repository.

Section 9

Installation reference

Appendix A

Installation scripts

This appendix includes the following topics:

About installation scripts

Veritas Storage Foundation and High Availability Solutions 5.1 SP1 provides several installation scripts.

An alternative to the `installer` script is to use a product-specific installation script. If you obtained a Veritas product from an electronic download site, which does not include the installer, use the appropriate product installation script.

The following product installation scripts are available:

Veritas Cluster Server (VCS)	`installvcs`
Veritas Storage Foundation (SF)	`installsf`
Veritas Storage Foundation and High Availability (SFHA)	`installsfha`
Veritas Storage Foundation Cluster File System (SFCFS)	`installsfcfs`
Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)	`installsfrac`
Symantec Product Authentication Service (AT)	`installat`
Veritas Dynamic Multi-pathing	`installdmp`

To use the installation script, enter the script name at the prompt. For example, to install Veritas Storage Foundation, type `./installsf` at the prompt.

Installation script options

Table A-1 shows command line options for the installation script. For an initial install or upgrade, options are not usually required. The installation script options apply to all Veritas Storage Foundation product scripts, except where otherwise noted.

See "About installation scripts" on page 375.

Table A-1 Available command line options

Command Line Option	Function
system1 system2...	Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.
–addnode	Adds a node to a high availability cluster.
–allpkgs	Displays all filesets and patches required for the specified product. The filesets and patches are listed in correct installation order. The output can be used to create scripts for command line installs, or for installations over a network.
–comcleanup	The `-comcleanup` option removes the ssh or rsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated.
–configure	Configures the product after installation.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
-copyinstallscripts	Use this option when you manually install products and want to use the intallation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `-rootpath` option. The following examples demonstrate the usage for this option: ■ `./installer -copyinstallscripts` Copies the installation and uninstallation scripts for all products in the release to `/opt/VRTS/install`. It also copies the installation Perl libraries to `/opt/VRTSperl/lib/site_perl/`*`release_name`*. ■ `./install`*`product_name`* `-copyinstallscripts` Copies the installation and uninstallation scripts for the specified product and any subset products for the product to `/opt/VRTS/install`. It also copies the installation Perl libraries to `/opt/VRTSperl/lib/site_perl/`*`release_name`*. ■ `./installer -copyinstallscripts -rootpath` *`alt_root_path`* The path *alt_root_path* can be a directory like `/rdisk2`. In that case, this command copies installation and uninstallation scripts for all the products in the release to `/rdisk2/opt/VRTS/install`. CPI perl libraries are copied to `/rdisk2/opt/VRTSperl/lib/site_perl/`*`release_name`*, where the *release_name* is a string that starts with UXRT and includes the release version with no punctuation.
–fencing	Configures I/O fencing in a running cluster.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
–hostfile *full_path_to_file*	Specifies the location of a file that contains a list of hostnames on which to install.
–ignorepatchreqs	The `-ignorepatchreqs` option is used to allow installation or upgrading even if the prerequisite filesets or patches are missed on the system.
–install	The `-install` option is used to install products on systems.
–installallpkgs	Specifies that all filesets are installed.
–installminpkgs	Specifies that the minimum fileset set is installed.
–installrecpkgs	Specifies that the required fileset set is installed.
–keyfile *ssh_key_file*	Specifies a key file for secure shell (SSH) installs. This option passes `-i ssh_key_file` to every SSH invocation.
–license	Registers or updates product licenses on the specified systems.
–listpatches	The `-listpatches` option displays product patches in correct installation order.
–logpath *log_path*	Specifies a directory other than `/opt/VRTS/install/logs` as the location where installer log files, summary files, and response files are saved.
–makeresponsefile	The `-makeresponsefile` generates a response file without doing an actual installation. Text displaying install, uninstall, start, and stop actions are simulations. These actions are not being performed on the system.
–minpkgs	Displays the minimal filesets and patches required for the specified product. The filesets and patches are listed in correct installation order. Optional filesets are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option.
–nim	Produces a NIM configuration file for installing with NIM.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
–patchpath *patch_path*	Designates the path of a directory that contains all patches to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
–pkginfo	Displays a list of filesets and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the -pkginfo option with the installvcs script to display VCS filesets.
–pkgpath *package_path*	Designates the path of a directory that contains all filesets to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
–pkgset	Discovers and displays the fileset group (minimum, recommended, all) and filesets that are installed on the specified systems.
–pkgtable	Displays product's filesets in correct installation order by group.
–postcheck	Checks for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups.
–precheck	Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.
–recpkgs	Displays the recommended filesets and patches required for the specified product. The filesets and patches are listed in correct installation order. Optional filesets are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option.
–redirect	Displays progress details without showing the progress bar.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
–requirements	The `-requirements` option displays required OS version, required patches, file system space, and other system requirements in order to install the product.
–responsefile *response_file*	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.
–rsh	Specify this option when you want to use rsh and rcp for communication between systems instead of the default ssh and scp. See "About configuring secure shell or remote shell communication modes before installing products" on page 411.
–security	Enable or disable Symantec Product Authentication Service in a VCS cluster that is running. You can specify this option with the `installvcs`, `installsfha` or `installsfcfs` scripts. For more information about Symantec Product Authentication Service in a VCS cluster, see the *Veritas Cluster Server Installation Guide*.
–serial	Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems.
–start	Starts the daemons and processes for the specified product.
–stop	Stops the daemons and processes for the specified product.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
–tmppath *tmp_path*	Specifies a directory other than `/var/tmp` as the working directory for the installation scripts. This destination is where initial logging is performed and where filesets are copied on remote systems before installation.
–uninstall	The `-uninstall` option is used to uninstall products from systems.
–upgrade	Specifies that an existing version of the product exists and you plan to upgrade it.
–upgrade_kernelpkgs	The `-upgrade_kernelpkgs` option is used to perform rolling upgrade Phase-I. In the phase, the product kernel filesets get upgraded to the latest version
–upgrade_nonkernelpkgs	The `-upgrade_nonkernelpkgs` option is used to perform rolling upgrade Phase-II. In the phase, VCS and other agent filesets upgrade to the latest version. Product kernel drivers are rolling-upgraded to the latest protocol version."
–version	Checks and reports the installed products and their versions. Identifies the installed and missing filesets and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing filesets and patches where applicable.

Appendix B

Response files

This appendix includes the following topics:

About response files

The installer or product installation script generates a response file during any installation, configuration, upgrade, or uninstall procedure. The response file contains the configuration information that you entered during the procedure. When the procedure completes, the installation script displays the location of the response files.

You can use the response file for future installation procedures by invoking an installation script with the `responsefile` option. The response file passes arguments to the script to automate the installation of that product. You can edit the file to automate installation and configuration of additional systems.

You can generate a response file using the `makeresponsefile` option.

See "Installation script options" on page 376.

Installing SFCFS using response files

Typically, you can use the response file that the installer generates after you perform SFCFS installation on one cluster to install SFCFS on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To install SFCFS using response files

1. Make sure the systems where you want to install SFCFS meet the installation requirements.
2. Make sure the preinstallation tasks are completed.
3. Copy the response file to one of the cluster systems where you want to install SFCFS.
4. Edit the values of the response file variables as necessary.
5. Mount the product disc and navigate to the directory that contains the installation program.
6. Start the installation from the system to which you copied the response file. For example:

   ```
   # ./installer -responsefile /tmp/response_file

   # ./installsfcfs -responsefile /tmp/response_file
   ```

   Where `/tmp/response_file` is the response file's full path name.

Configuring SFCFS using response files

Typically, you can use the response file that the installer generates after you perform SFCFS configuration on one cluster to configure SFCFS on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To configure SFCFS using response files

1. Make sure the SFCFS filesets are installed on the systems where you want to configure SFCFS.
2. Copy the response file to one of the cluster systems where you want to configure SFCFS.
3. Edit the values of the response file variables as necessary.

   To configure optional features, you must define appropriate values for all the response file variables that are related to the optional feature.

   See "Response file variables to configure Storage Foundation Cluster File System" on page 389.
4. Start the configuration from the system to which you copied the response file. For example:

   ```
   # /opt/VRTS/install/installsfcfs -responsefile /tmp/response_file
   ```

   Where /tmp/*response_file* is the response file's full path name.

Upgrading SFCFS using response files

Typically, you can use the response file that the installer generates after you perform SFCFS upgrade on one cluster to upgrade SFCFS on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To perform automated SFCFS upgrade

1. Make sure the systems where you want to upgrade SFCFS meet the upgrade requirements.
2. Make sure the pre-upgrade tasks are completed.
3. Copy the response file to one of the cluster systems where you want to upgrade SFCFS.
4. Edit the values of the response file variables as necessary.

5 Mount the product disk, and navigate to the folder that contains the installation program.

6 Start the upgrade from the system to which you copied the response file. For example:

```
# ./installer -responsefile /tmp/response_file

# ./installsfcfs -responsefile /tmp/response_file
```

Where /tmp/*response_file* is the response file's full path name.

Uninstalling SFCFS using response files

Typically, you can use the response file that the installer generates after you perform SFCFS uninstallation on one cluster to uninstall SFCFS on other clusters.

To perform an automated uninstallation

1 Make sure that you meet the prerequisites to uninstall SFCFS.

2 Copy the response file to one of the cluster systems where you want to uninstall SFCFS.

3 Edit the values of the response file variables as necessary.

4 Start the uninstallation from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/uninstallsfcfs -responsefile /tmp/response_file
```

Where /tmp/*response_file* is the response file's full path name.

Syntax in the response file

The syntax of the Perl statements that are included in the response file variables varies. It can depend on whether the variables require scalar or list values.

For example, in the case of a string value:

```
$CFG{Scalar_variable}="value";
```

or, in the case of an integer value:

```
$CFG{Scalar_variable}=123;
```

or, in the case of a list:

```
$CFG{List_variable}=["value", "value", "value"];
```

Response file variables to install, upgrade, or uninstall Storage Foundation Cluster File System

Table B-1 lists the response file variables that you can define to configure SFCFS.

Table B-1 Response file variables specific to installing, upgrading, or uninstalling SFCFS

Variable	Description
CFG{opt}{install}	Installs SFCFS filesets. Configuration can be performed at a later time using the `-configure` option. List or scalar: scalar Optional or required: optional
CFG{accepteula}	Specifies whether you agree with the `EULA.pdf` file on the media. List or scalar: scalar Optional or required: required
$CFG{opt}{vxkeyless}	Installs the product with keyless license. List of scalar: scalar Optional or required: optional
CFG{systems}	List of systems on which the product is to be installed or uninstalled. List or scalar: list Optional or required: required
CFG{systemscfs}	List of systems for configuration if secure environment prevents the installer to install SFCFS on all systems at once. List or scalar: list Optional or required: required
CFG{prod}	Defines the product to be installed or uninstalled. List or scalar: scalar Optional or required: required

Table B-1 Response file variables specific to installing, upgrading, or uninstalling SFCFS *(continued)*

Variable	Description
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional
CFG{at_rootdomain}	Defines the name of the system where the root broker is installed. List or scalar: scalar Optional or required: optional
CFG{opt}{patchpath}	Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems. List or scalar: scalar Optional or required: optional
CFG{opt}{pkgpath}	Defines a location, typically an NFS mount, from which all remote systems can install product filesets. The location must be accessible from all target systems. List or scalar: scalar Optional or required: optional
CFG{opt}{tmppath}	Defines the location where a working directory is created to store temporary files and the filesets that are needed during the install. The default location is `/var/tmp`. List or scalar: scalar Optional or required: optional
CFG{opt}{rsh}	Defines that *rsh* must be used instead of ssh as the communication method between systems. List or scalar: scalar Optional or required: optional

Table B-1 Response file variables specific to installing, upgrading, or uninstalling SFCFS *(continued)*

Variable	Description
CFG{donotinstall} {fileset}	Instructs the installation to not install the optional filesets in the list. List or scalar: list Optional or required: optional
CFG{donotremove} {fileset}	Instructs the uninstallation to not remove the optional filesets in the list. List or scalar: list Optional or required: optional
CFG{opt}{logpath}	Mentions the location where the log files are to be copied. The default location is `/opt/VRTS/install/logs`. List or scalar: scalar Optional or required: optional
$CFG{opt}{prodmode}	List of modes for product List or scalar: list Optional or required: optional
CFG{opt}{upgrade}	Upgrades all filesets installed, without configuration. List or scalar: list Optional or required: optional
CFG{opt}{uninstall}	Uninstalls SFCFS filesets. List or scalar: scalar Optional or required: optional

Response file variables to configure Storage Foundation Cluster File System

Table B-2 lists the response file variables that you can define to configure Storage Foundation Cluster File System.

Table B-2 Response file variables specific to configuring Storage Foundation Cluster File System

Variable	List or Scalar	Description
CFG{opt}{configure}	Scalar	Performs the configuration if the filesets are already installed. (Required)
CFG{accepteula}	Scalar	Specifies whether you agree with `EULA.pdf` on the media. (Required)
CFG{systems}	List	List of systems on which the product is to be configured. (Required)
CFG{prod}	Scalar	Defines the product to be configured. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is `/opt/VRTS/install/logs`. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)

Table B-2 Response file variables specific to configuring Storage Foundation Cluster File System *(continued)*

Variable	List or Scalar	Description
$CFG{uploadlogs}	Scalar	Defines Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site. (Optional)

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (the csgnic, csgvip, and csgnetmask variables) must be defined if any are defined. The same is true for the SMTP notification (the smtpserver, smtprecp, and smtprsev variables), the SNMP trap notification (the snmpport, snmpcons, and snmpcsev variables), and the Global Cluster Option (the gconic, gcovip, and gconetmask variables).

Table B-3 lists the response file variables that specify the required information to configure a basic Storage Foundation Cluster File System cluster.

Table B-3 Response file variables specific to configuring a basic Storage Foundation Cluster File System cluster

Variable	List or Scalar	Description
CFG{vcs_clusterid}	Scalar	An integer between 0 and 65535 that uniquely identifies the cluster. (Required)
CFG{vcs_clustername}	Scalar	Defines the name of the cluster. (Required)
CFG{vcs_allowcomms}	Scalar	Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)

Table B-3 Response file variables specific to configuring a basic Storage Foundation Cluster File System cluster *(continued)*

Variable	List or Scalar	Description
$CFG{fencingenabled}	Scalar	In a Storage Foundation Cluster File System configuration, defines if fencing is enabled. Valid values are 0 or 1. (Required)

Table B-4 lists the response file variables that specify the required information to configure LLT over Ethernet.

Table B-4 Response file variables specific to configuring private LLT over Ethernet

Variable	List or Scalar	Description
CFG{vcs_lltlink#} {"system"}	Scalar	Defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (lltlink1 and lltlink2). You can configure up to four LLT links. You must enclose the system name within double quotes. (Required)
CFG{vcs_lltlinklowpri#} {"system"}	Scalar	Defines a low-priority heartbeat link. Typically, lltlinklowpri is used on a public network link to provide an additional layer of communication. If you use different media speed for the private NICs, you can configure the NICs with lesser speed as low-priority links to enhance LLT performance. For example, lltlinklowpri1, lltlinklowpri2, and so on. You must enclose the system name within double quotes. (Optional)

Table B-5 lists the response file variables that specify the required information to configure LLT over UDP.

Table B-5 Response file variables specific to configuring LLT over UDP

Variable	List or Scalar	Description
CFG{lltoverudp}=1	Scalar	Indicates whether to configure heartbeat link using LLT over UDP. (Required)
CFG{vcs_udplink<n>_address} {<system1>}	Scalar	Stores the IP address (IPv4 or IPv6) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required)
CFG {vcs_udplinklowpri<n>_address} {<system1>}	Scalar	Stores the IP address (IPv4 or IPv6) that the low-priority heartbeat link uses on node1. You can have four low-priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low-priority heartbeat links. (Required)
CFG{vcs_udplink<n>_port} {<system1>}	Scalar	Stores the UDP port (16-bit integer value) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required)
CFG{vcs_udplinklowpri<n>_port} {<system1>}	Scalar	Stores the UDP port (16-bit integer value) that the low-priority heartbeat link uses on node1. You can have four low-priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low-priority heartbeat links. (Required)

Table B-5 Response file variables specific to configuring LLT over UDP *(continued)*

Variable	List or Scalar	Description
CFG{vcs_udplink<n>_netmask} {<system1>}	Scalar	Stores the netmask (prefix for IPv6) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required)
CFG{vcs_udplinklowpri<n>_netmask} {<system1>}	Scalar	Stores the netmask (prefix for IPv6) that the low-priority heartbeat link uses on node1. You can have four low-priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low-priority heartbeat links. (Required)

Table B-6 lists the response file variables that specify the required information to configure virtual IP for Storage Foundation Cluster File System cluster.

Table B-6 Response file variables specific to configuring virtual IP for Storage Foundation Cluster File System cluster

Variable	List or Scalar	Description
CFG{vcs_csgnic} {system}	Scalar	Defines the NIC device to use on a system. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional)
CFG{vcs_csgvip}	Scalar	Defines the virtual IP address for the cluster. (Optional)
CFG{vcs_csgnetmask}	Scalar	Defines the Netmask of the virtual IP address for the cluster. (Optional)

Table B-7 lists the response file variables that specify the required information to configure the Storage Foundation Cluster File System cluster in secure mode.

Table B-7 Response file variables specific to configuring Storage Foundation Cluster File System cluster in secure mode

Variable	List or Scalar	Description
CFG{at_rootdomain}	Scalar	Defines the name of the system where the root broker is installed. (Optional)
CFG{at_rootbroker}	Scalar	Defines the root broker's name.
CFG{vcs_securitymenuopt}	Scalar	Specifies the menu option to choose to configure the cluster in secure mode. ■ 1—Automatic ■ 2—Semi-automatic ■ 3—Manual (Optional)
CFG{vcs_vssdefport}	Scalar	Specifies the default port address of the root broker. (Optional)
CFG{vcs_roothashpath}	Scalar	Specifies the path of the root hash file. (Optional)
CFG{vcs_ab_prplname} {system}	Scalar	Specifies the authentication broker's principal name on system. (Optional)
CFG{vcs_ab_password} {system}	Scalar	Specifies the authentication broker's password on system. (Optional)
CFG{vcs_blobpath} {system}	Scalar	Specifies the path of the encrypted BLOB file for system. (Optional)

Table B-8 lists the response file variables that specify the required information to configure VCS users.

Table B-8 Response file variables specific to configuring VCS users

Variable	List or Scalar	Description
CFG{vcs_userenpw}	List	List of encoded passwords for VCS users. The value in the list can be "Administrators Operators Guests." **Note:** The order of the values for the vcs_userenpw list must match the order of the values in the vcs_username list. (Optional)
CFG{vcs_username}	List	List of names of VCS users. (Optional)
CFG{vcs_userpriv}	List	List of privileges for VCS users. **Note:** The order of the values for the vcs_userpriv list must match the order of the values in the vcs_username list. (Optional)

Table B-9 lists the response file variables that specify the required information to configure VCS notifications using SMTP.

Table B-9 Response file variables specific to configuring VCS notifications using SMTP

Variable	List or Scalar	Description
CFG{vcs_smtpserver}	Scalar	Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for Web notification. (Optional)
CFG{vcs_smtprecp}	List	List of full email addresses (example: user@symantecexample.com) of SMTP recipients. (Optional)

Table B-9 Response file variables specific to configuring VCS notifications using SMTP *(continued)*

Variable	List or Scalar	Description
CFG{vcs_smtprsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, and SevereError) that listed SMTP recipients are to receive. Note that the ordering of severity levels must match that of the addresses of SMTP recipients. (Optional)

Table B-10 lists the response file variables that specify the required information to configure VCS notifications using SNMP.

Table B-10 Response file variables specific to configuring VCS notifications using SNMP

Variable	List or Scalar	Description
CFG{vcs_snmpport}	Scalar	Defines the SNMP trap daemon port (default=162). (Optional)
CFG{vcs_snmpcons}	List	List of SNMP console system names. (Optional)
CFG{vcs_snmpcsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, and SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names. (Optional)

Table B-11 lists the response file variables that specify the required information to configure Storage Foundation Cluster File System global clusters.

Table B-11 Response file variables specific to configuring Storage Foundation Cluster File System global clusters

Variable	List or Scalar	Description
CFG{vcs_gconic} {system}	Scalar	Defines the NIC for the Virtual IP that the Global Cluster Option uses. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional)
CFG{vcs_gcovip}	Scalar	Defines the virtual IP address to that the Global Cluster Option uses. (Optional)
CFG{vcs_gconetmask}	Scalar	Defines the Netmask of the virtual IP address that the Global Cluster Option uses. (Optional)

Sample response file for SFCFS install

The following example shows a response file for installing Storage Foundation Cluster File System.

```
##############################################
#Auto generated sfcfs responsefile #
##############################################


our %CFG;
$CFG{accepteula}=1;
$CFG{opt}{rsh}=1;
$CFG{opt}{trace}=0;
$CFG{opt}{gco}=1;
$CFG{opt}{vvr}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{prod}="SFCFS51SP1";
$CFG{systems}=[ qw( system01 system02 ) ];
$CFG{opt}{logpath}="/opt/VRTS/install/logs/installsfcfs-xxxxxx/installsfcfs-xxxxxx.response";

1;
```

Sample response file for SFCFS configure

The following example shows a response file for configuring Storage Foundation Cluster File System.

```
##############################################
#Auto generated sfcfs responsefile #
##############################################


our %CFG;
$CFG{accepteula}=1;
$CFG{opt}{rsh}=1;
$CFG{opt}{trace}=0;
$CFG{vcs_allowcomms}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vvr}=1;
$CFG{opt}{configure}=1;
$CFG{prod}="SFCFS51SP1";
$CFG{systems}=[ qw( system01 system02 ) ];
$CFG{sfcfs_cvmtimeout}=200;
$CFG{sfcfs_fencingenabled}=0;
$CFG{vm_newnames_file}{system01}=0;
$CFG{vm_restore_cfg}{system01}=0;
$CFG{vm_newnames_file}{system02}=0;
$CFG{vm_restore_cfg}{system02}=0;
$CFG{obc_mode}="STANDALONE";
$CFG{opt}{noextrapkgs}=1;
$CFG{vcs_clusterid}=127;
$CFG{vcs_clustername}="uxrt5_aix";
$CFG{vcs_username}=[ qw(admin operator) ];
$CFG{vcs_userenpw}=[ qw(JlmElgLimHmmKumGlj bQOsOUnVQoOUnTQsOSnUQuOUnPQtOS) ];
$CFG{vcs_userpriv}=[ qw(Administrators Operators) ];
$CFG{vcs_lltlink1}{system01}="en1";
$CFG{vcs_lltlink2}{system01}="en2";
$CFG{vcs_lltlink1}{system02}="en1";
$CFG{vcs_lltlink2}{system02}="en2";
$CFG{vcs_enabled}=1;
$CFG{opt}{logpath}="/opt/VRTS/install/logs/installsfcfs-xxxxxx/installsfcfs-xxxxxx.response";

1;
```

Appendix C

Configuring I/O fencing using a response file

This appendix includes the following topics:

Configuring I/O fencing using response files

Typically, you can use the response file that the installer generates after you perform I/O fencing configuration to configure I/O fencing for Storage Foundation Cluster File System.

To configure I/O fencing using response files

1. Make sure that Storage Foundation Cluster File System is configured.
2. Based on whether you want to configure disk-based or server-based I/O fencing, make sure you have completed the preparatory tasks.

   See "About planning to configure I/O fencing" on page 90.

3 Copy the response file to one of the cluster systems where you want to configure I/O fencing.

See "Sample response file for configuring disk-based I/O fencing" on page 403.

See "Sample response file for configuring server-based I/O fencing" on page 406.

4 Edit the values of the response file variables as necessary.

See "Response file variables to configure disk-based I/O fencing" on page 402.

See "Response file variables to configure server-based I/O fencing" on page 404.

5 Start the configuration from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/installsfcfs -responsefile /tmp/response_file
```

Where /tmp/*response_file* is the response file's full path name.

Response file variables to configure disk-based I/O fencing

Table C-1 lists the response file variables that specify the required information to configure disk-based I/O fencing for SFCFS.

Table C-1 Response file variables specific to configuring disk-based I/O fencing

Variable	List or Scalar	Description
CFG{opt}{fencing}	Scalar	Performs the I/O fencing configuration. (Required)
CFG{vxfen_config_fencing_option}	Scalar	Specifies the I/O fencing configuration mode. ■ 1—Coordination Point Server-based I/O fencing ■ 2—Coordinator disk-based I/O fencing ■ 3—Disabled mode (Required)

Table C-1 Response file variables specific to configuring disk-based I/O fencing *(continued)*

Variable	List or Scalar	Description
CFG {vxfen_config _fencing_mechanism}	Scalar	Specifies the I/O fencing mechanism. This variable is not required if you had configured fencing in disabled mode. For disk-based fencing, you must configure the vxfen_config _fencing_mechanism variable and either the vxfen_config_fencing_dg variable or the vxfen_config _fencing_newdg_disks variable. (Optional)
CFG{vxfen_config_fencing_dg}	Scalar	Specifies the disk group for I/O fencing. (Optional) **Note:** You must define the vxfen_config_fencing_dg variable to use an existing disk group. If you want to create a new disk group, you must use both the vxfen_config_fencing_dg variable and the vxfen_config_fencing_newdg_disks variable.
CFG{vxfen_config _fencing_newdg_disks}	List	Specifies the disks to use to create a new disk group for I/O fencing. (Optional) **Note:** You must define the vxfen_config_fencing_dg variable to use an existing disk group. If you want to create a new disk group, you must use both the vxfen_config_fencing_dg variable and the vxfen_config_fencing_newdg_disks variable.

Sample response file for configuring disk-based I/O fencing

Review the disk-based I/O fencing response file variables and their definitions.

See "Response file variables to configure disk-based I/O fencing" on page 402.

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

$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;

$CFG{prod}="SFCFS51";

$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=13221;
$CFG{vcs_clustername}="clus1";
$CFG{vxfen_config_fencing_dg}="fendg";
$CFG{vxfen_config_fencing_mechanism}="dmp";
$CFG{vxfen_config_fencing_newdg_disks}=
 [ qw(rhdisk75 rhdisk76 rhdisk77) ];
$CFG{vxfen_config_fencing_option}=2;
```

Response file variables to configure server-based I/O fencing

You can use a CP server response file to configure server-based customized I/O fencing. The installer uses the CP server response file for the following types of I/O fencing configurations:

- Client cluster fencing (server-based I/O fencing configuration itself)
  The installer configures server-based customized I/O fencing on the SFCFS cluster without prompting for user input.
- Disk-based fencing with the disk group already created
  The installer configures fencing in disk-based mode on the SFCFS cluster without prompting for user input.
  Disk-based fencing configuration is one in which SCSI-3 disks are used as the only coordination points.
  Disk-based fencing with the disk group already created means that the disk group consisting of the coordinating disks already exists on the SFCFS cluster nodes.
- Disk-based fencing with the disk group to be created
  The installer creates the disk group and configures fencing properly on all the nodes in the SFCFS cluster without user intervention.

Disk-based fencing with the disk group to be created means that the disk group does not exist yet, but will be created with the disks mentioned as coordination point.

Table C-2 lists the fields in the response file that are relevant for server-based customized I/O fencing.

Table C-2 CP server response file definitions

Response file field	Definition
fencing_cpc_config_cpagent	Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter "0" if you do not want to configure the Coordination Point agent using the installer. Enter "1" if you want to use the installer to configure the Coordination Point agent.
fencing_cpc_cpagentgrp	Name of the service group which will have the Coordination Point agent resource as part of it. **Note:** This field is obsolete if the `fencing_cpc_config_cpagent` field is given a value of '0'.
fencing_cpc_cps	Virtual IP address or Virtual hostname of the CP servers.
fencing_cpc_reusedg	This response file field indicates whether to reuse an existing DG name for the fencing configuration in customized fencing (CP server and coordinator disks). Enter either a "1" or "0". Entering a "1" indicates reuse, and entering a "0" indicates do not reuse. When reusing an existing DG name for the mixed mode fencing configuration. you need to manually add a line of text , such as "$CFG{fencing_cpc_reusedg}=0" or "$CFG{fencing_cpc_reusedg}=1" before proceeding with a silent installation.
fencing_cpc_dgname	The name of the disk group to be used in the customized fencing, where at least one disk is being used.

Table C-2 CP server response file definitions *(continued)*

Response file field	Definition
fencing_cpc_diffab	This response field indicates whether the CP servers and SFCFS clusters use different root brokers. Entering a "1" indicates that they are using different root brokers. Entering a "0" indicates that they are not using different root brokers.
fencing_cpc_disks	The disks being used as coordination points if any.
fencing_cpc_ncps	Total number of coordination points being used, including both CP servers and disks.
fencing_cpc_ndisks	The number of disks being used.
fencing_cpc_ports	The port of the CP server that is denoted by *cps* .
fencing_cpc_ccab	The name of the authentication broker (AB) for any one of the SFCFS cluster nodes.
fencing_cpc_cpsabport	The port at which the authentication broker (AB) mentioned above listens for authentication..
fencing_cpc_ccabport	The port at which the authentication broker (AB) mentioned above listens for authentication.
fencing_cpc_mechanism	The disk mechanism that is used by customized fencing. The value for this field is either "raw" or "dmp"
fencing_cpc_cpsab	The name of the authentication broker (AB) for any one of the CP servers.
fencing_cpc_security	This field indicates whether security is enabled or not Entering a "1" indicates that security is enabled. Entering a "0" indicates that security has not been enabled.

Sample response file for configuring server-based I/O fencing

The following is a sample response file used for server-based I/O fencing :

```
$CFG{fencing_cpc_config_cpagent}=0;
$CFG{fencing_cpc_cps}=[ qw(10.200.117.145) ];
$CFG{fencing_cpc_dgname}="vxfencoorddg";
$CFG{fencing_cpc_diffab}=0;
$CFG{fencing_cpc_disks}=[ qw(emc_clariion0_37 emc_clariion0_13) ];
$CFG{fencing_cpc_mechanism}="raw";
$CFG{fencing_cpc_ncps}=3;
$CFG{fencing_cpc_ndisks}=2;
$CFG{fencing_cpc_ports}{"10.200.117.145"}=14250;
$CFG{fencing_cpc_reusedg}=1;
$CFG{fencing_cpc_security}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="SFCFS51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{vxfen_config_fencing_option}=1;
```

Response file variables to configure non-SCSI3 server-based I/O fencing

Table C-3 lists the fields in the response file that are relevant for non-SCSI3 server-based customized I/O fencing.

See "About I/O fencing for Storage Foundation Cluster File System in virtual machines that do not support SCSI-3 PR" on page 85.

Table C-3 Non-SCSI3 server-based I/O fencing response file definitions

Response file field	Definition
CFG{non_scsi3_fencing}	Defines whether to configure non-SCSI3 server-based I/O fencing. Valid values are 1 or 0. Enter 1 to configure non-SCSI3 server-based I/O fencing.

Table C-3 Non-SCSI3 server-based I/O fencing response file definitions *(continued)*

Response file field	Definition
CFG {fencing_cpc_config_cpagent}	Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter "0" if you do not want to configure the Coordination Point agent using the installer. Enter "1" if you want to use the installer to configure the Coordination Point agent.
CFG {fencing_cpc_cpagentgrp}	Name of the service group which will have the Coordination Point agent resource as part of it. **Note:** This field is obsolete if the `fencing_cpc_config_cpagent` field is given a value of '0'.
CFG {fencing_cpc_cps}	Virtual IP address or Virtual hostname of the CP servers.
CFG {fencing_cpc_diffab}	This response field indicates whether the CP servers and SFCFS clusters use different root brokers. Entering a "1" indicates that they are using different root brokers. Entering a "0" indicates that they are not using different root brokers.
CFG {fencing_cpc_ncps}	Total number of coordination points (CP servers only) being used.
CFG {fencing_cpc_ports}	The port of the CP server that is denoted by *cps* .
CFG {fencing_cpc_ccab}	The name of the authentication broker (AB) for any one of the SFCFS cluster nodes.
CFG {fencing_cpc_cpsabport}	The port at which the authentication broker (AB) mentioned above listens for authentication..
CFG {fencing_cpc_ccabport}	The port at which the authentication broker (AB) mentioned above listens for authentication.
CFG {fencing_cpc_cpsab}	The name of the authentication broker (AB) for any one of the CP servers.

Table C-3 Non-SCSI3 server-based I/O fencing response file definitions *(continued)*

Response file field	Definition
CFG {fencing_cpc_security}	This field indicates whether security is enabled or not Entering a "1" indicates that security is enabled. Entering a "0" indicates that security has not been enabled.

Sample response file for configuring non-SCSI3 server-based I/O fencing

The following is a sample response file used for non-SCSI3 server-based I/O fencing :

```
$CFG{fencing_cpc_config_cpagent}=0;
$CFG{fencing_cpc_cps}=[ qw(10.198.89.251 10.198.89.252 10.198.89.253) ];
$CFG{fencing_cpc_ncps}=3;
$CFG{fencing_cpc_ndisks}=0;
$CFG{fencing_cpc_ports}{"10.198.89.251"}=14250;
$CFG{fencing_cpc_ports}{"10.198.89.252"}=14250;
$CFG{fencing_cpc_ports}{"10.198.89.253"}=14250;
$CFG{fencing_cpc_security}=1;
$CFG{non_scsi3_fencing}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="SFCFS51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{vxfen_config_fencing_option}=1;
```

Appendix D

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

About configuring secure shell or remote shell communication modes before installing products

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 installer is run must have permissions to run `rsh` (remote shell) or `ssh` (secure shell) utilities. You need to run the installer with superuser privileges on the systems where you plan to install Veritas software.

You can install products to remote systems using either secure shell (ssh) or remote shell (rsh). Symantec recommends that you use ssh as it is more secure than rsh.

This section contains an example of how to set up ssh password free communication. The example sets up ssh between a source system (system1) that

contains the installation directories, and a target system (system2). This procedure also applies to multiple target systems.

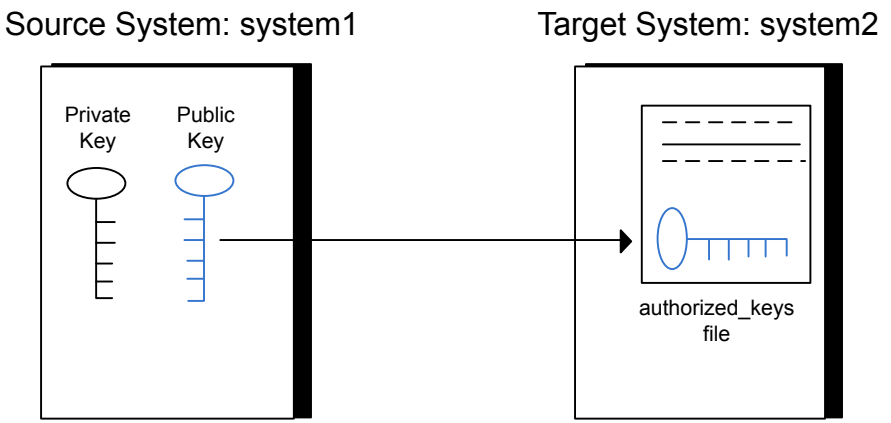
Configuring and enabling ssh

The ssh program enables you to log into and execute commands on a remote system. ssh enables encrypted communications and an authentication process between two untrusted hosts over an insecure network.

In this procedure, you first create a DSA key pair. From the key pair, you append the public key from the source system to the authorized_keys file on the target systems.

Figure D-1 illustrates this procedure.

Figure D-1 Creating the DSA key pair and appending it to target systems



Read the ssh documentation and online manual pages before enabling ssh. Contact your operating system support provider for issues regarding ssh configuration.

Visit the OpenSSH website that is located at: http://openssh.org to access online manuals and other resources.

To create the DSA key pair

1. On the source system (system1), log in as root, and navigate to the root directory.

   ```
   system1 # cd /
   ```

2. To generate a DSA key pair on the source system, type the following command:

   ```
   system1 # ssh-keygen -t dsa
   ```

   System output similar to the following is displayed:

   ```
   Generating public/private dsa key pair.
   Enter file in which to save the key (//.ssh/id_dsa):
   ```

3. Press Enter to accept the default location of `/.ssh/id_dsa`.
4. When the program asks you to enter the passphrase, press the Enter key twice.

   ```
   Enter passphrase (empty for no passphrase):
   ```

   Do not enter a passphrase. Press Enter.

   ```
   Enter same passphrase again:
   ```

   Press Enter again.
5. Make sure the `/.ssh` directory is on all the target installation systems (system2 in this example). If that directory is not present, create it on all the target systems and set the write permission to root only:

   ```
   system2 # mkdir /.ssh
   ```

   Change the permissions of this directory, to secure it.

   ```
   system2 # chmod go-w /.ssh
   ```

To append the public key from the source system to the authorized_keys file on the target system, using secure file transfer

1 From the source system (system1), move the public key to a temporary file on the target system (system2).

Use the secure file transfer program.

In this example, the file name `id_dsa.pub` in the root directory is the name for the temporary file for the public key.

Use the following command for secure file transfer:

```
system1 # sftp system2
```

If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

```
Connecting to system2 ...
The authenticity of host 'system2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

2 Enter `yes`.

Output similar to the following is displayed:

```
Warning: Permanently added 'system2,10.182.00.00'
(DSA) to the list of known hosts.
root@system2 password:
```

3 Enter the root password of system2.

4 At the `sftp` prompt, type the following command:

```
sftp> put /.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /.ssh/id_dsa.pub to /id_dsa.pub
```

5 To quit the SFTP session, type the following command:

```
sftp> quit
```

6 To begin the ssh session on the target system (system2 in this example), type the following command on system1:

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

7 After you log in to system2, enter the following command to append the id_dsa.pub file to the authorized_keys file:

```
system2 # cat /id_dsa.pub >> /.ssh/authorized_keys
```

8 After the id_dsa.pub public key file is copied to the target system (system2), and added to the authorized keys file, delete it. To delete the id_dsa.pub public key file, enter the following command on system2:

```
system2 # rm /id_dsa.pub
```

9 To log out of the ssh session, enter the following command:

```
system2 # exit
```

10 When you install from a source system that is also an installation target, also add the local system id_dsa.pub key to the local authorized_keys file. The installation can fail if the installation source system is not authenticated.

To add the local system id_dsa.pub key to the local authorized_keys file, enter the following command:

```
system1 # cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys
```

11 Run the following commands on the source installation system. If your ssh session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and make the key globally available to the user root:

```
system1 # exec /usr/bin/ssh-agent $SHELL
system1 # ssh-add

  Identity added: //.ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

To verify that you can connect to a target system

1 On the source system (system1), enter the following command:

```
system1 # ssh -l root system2 uname -a
```

where system2 is the name of the target system.

2 The command should execute from the source system (system1) to the target system (system2) without the system requesting a passphrase or password.

3 Repeat this procedure for each target system.

Restarting the ssh session

After you complete this procedure, ssh can be restarted in any of the following scenarios:

- After a terminal session is closed
- After a new terminal session is opened
- After a system is restarted
- After too much time has elapsed, to refresh ssh

To restart ssh

1 On the source installation system (system1), bring the private key into the shell environment.

```
system1 # exec /usr/bin/ssh-agent $SHELL
```

2 Make the key globally available for the user `root`

```
system1 # ssh-add
```

Enabling rsh for AIX

To enable `rsh`, create a `/.rhosts` file on each target system. Then add a line to the file specifying the full domain name of the source system. For example, add the line:

sysname.domainname`.com root`

Change permissions on the `/.rhosts` file to 600 by typing the following command:

```
# chmod 600 /.rhosts
```

After you complete an installation procedure, delete the `.rhosts` file from each target system to ensure security:

```
# rm -f /.rhosts
```

Appendix E

Storage Foundation Cluster File System components

This appendix includes the following topics:

Veritas Storage Foundation Cluster File System installation filesets

Table E-1 shows the fileset name and contents for each English language fileset for Veritas Storage Foundation Cluster File System. The table also gives you guidelines for which filesets to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Veritas Storage Foundation Cluster File System and Veritas Cluster Server (VCS) filesets, the combined functionality is called Veritas Storage Foundation Cluster File System and High Availability.

See "Veritas Cluster Server installation filesets" on page 421.

Table E-1 Veritas Storage Foundation Cluster File System filesets

filesets	Contents	Configuration
VRTSaslapm	Veritas Array Support Library (ASL) and Array Policy Module(APM) binaries Required for the support and compatibility of various storage arrays.	Minimum
VRTSat	Symantec Product Authentication Service Installs the Symantec Product Authentication Service, which provides authentication services to other Symantec products. This fileset contains a server and client component. The server provides services for a root broker, authentication broker, or both. The client allows Symantec products to communicate with the brokers. Required to use Symantec Product Authentication Service.	All
VRTSperl	Perl 5.10.0 for Veritas	Minimum
VRTSveki	Veritas Kernel Interface Contains a common set of modules that other Veritas drivers use.	Minimum
VRTSvlic	Veritas License Utilities Installs the license key layout files required to decode the Storage Foundation license keys. Provides the standard license key utilities vxlicrep, vxlicinst, and vxlictest.	Minimum
VRTSvxfs	Veritas File System binaries Required for VxFS file system support.	Minimum
VRTSvxvm	Veritas Volume Manager binaries	Minimum
VRTSdbed	Veritas Storage Foundation for Oracle	Recommended
VRTSob	Veritas Enterprise Administrator	Recommended

Table E-1 Veritas Storage Foundation Cluster File System filesets *(continued)*

filesets	Contents	Configuration
VRTSodm	ODM Driver for VxFS Veritas Extension for Oracle Disk Manager is a custom storage interface designed specifically for Oracle9i and 10g. Oracle Disk Manager allows Oracle 9i and 10g to improve performance and manage system bandwidth.	Recommended
VRTSsfmh	Veritas Storage Foundation Managed Host Discovers configuration information on a Storage Foundation managed host. This information is stored on a central database, which is not part of this release. You must download the database separately at: http://www.symantec.com/business/storage-foundation-manager	Recommended
VRTSspt	Veritas Software Support Tools	Recommended
VRTSfssdk	Veritas File System Software Developer Kit For VxFS APIs, the fileset contains the public Software Developer Kit (headers, libraries, and sample code). It is required if some user programs use VxFS APIs.	All

Veritas Cluster Server installation filesets

Table E-2 shows the fileset name and contents for each English language fileset for Veritas Cluster Server (VCS). The table also gives you guidelines for which filesets to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Storage Foundation and VCS filesets, the combined functionality is called Storage Foundation and High Availability.

See "Veritas Storage Foundation Cluster File System installation filesets" on page 419.

Table E-2 VCS installation filesets

fileset	Contents	Configuration
VRTSgab	Veritas Cluster Server group membership and atomic broadcast services	Minimum
VRTSllt	Veritas Cluster Server low-latency transport	Minimum
VRTSamf	Veritas Cluster Server Asynchronous Monitoring Framework	Minimum
VRTSvcs	Veritas Cluster Server	Minimum
VRTSvcsag	Veritas Cluster Server Bundled Agents	Minimum
VRTSvxfen	Veritas I/O Fencing	Minimum
VRTSvcsea	Consolidated database and enterprise agent filesets	Recommended
VRTScps	Veritas Coordination Point Server The Coordination Point Server is an alternate mechanism for I/O fencing. It implements I/O fencing through a client/server architecture and can provide I/O fencing for multiple VCS clusters.	All

Veritas Cluster File System installation filesets

Table E-3 shows the fileset name and contents for each English language fileset for Veritas Cluster File System (CFS). The table also gives you guidelines for whichfilesets to install based whether you want the minimum, recommended, or advanced configuration.

When you install all CFS filesets and all the filesets that comprise Storage Foundation and Veritas Cluster Server, the resulting functionality is called Storage Foundation Cluster File System.

See "Veritas Storage Foundation Cluster File System installation filesets" on page 419.

See "Veritas Cluster Server installation filesets" on page 421.

Table E-3 CFS installation filesets

fileset	Contents	Configuration
VRTScavf	Veritas Cluster Server Agents for Storage Foundation Cluster File System	Minimum
VRTSglm	Veritas Group Lock Manager for Storage Foundation Cluster File System	Minimum
VRTSgms	Veritas Group Messaging Services for Storage Foundation Cluster File System	Recommended

Veritas Storage Foundation obsolete and reorganized installation filesets

Table E-4 lists the filesets that are obsolete or reorganized for Storage Foundation and Storage Foundation High Availability.

Table E-4 Veritas Storage Foundation obsolete and reorganized filesets

fileset	Description
Infrastructure	
SYMClma	Obsolete
VRTSaa	Included in VRTSsfmh
VRTSccg	Included in VRTSsfmh
VRTSdbms3	Obsolete
VRTSicsco	Obsolete
VRTSjre	Obsolete
VRTSjre15	Obsolete
VRTSmh	Included in VRTSsfmh
VRTSobc33	Obsolete
VRTSobgui	Obsolete
VRTSpbx	Obsolete
VRTSsfm	Obsolete

Table E-4 Veritas Storage Foundation obsolete and reorganized filesets *(continued)*

fileset	Description
VRTSweb	Obsolete
Product filesets	
VRTSacclib	Obsolete The following information is for installations, upgrades, and uninstallations using the script- or Web-based installer. ■ For fresh installations VRTSacclib is not installed. ■ For upgrades, the existing VRTSacclib is uninstalled and a new VRTSacclib is installed. ■ For uninstallation, VRTSacclib is not uninstalled.
VRTSalloc	Obsolete
VRTScmccc	Obsolete
VRTScmcs	Obsolete
VRTScscm	Obsolete
VRTScscw	Obsolete
VRTScsocw	Obsolete
VRTScssim	Obsolete
VRTScutil	Obsolete
VRTSd2gui	Included in VRTSdbed
VRTSdb2ed	Included in VRTSdbed
VRTSdbcom	Included in VRTSdbed
VRTSdbed	Included in VRTSdbed
VRTSdcli	Obsolete
VRTSddlpr	Obsolete
VRTSdsa	Obsolete

Table E-4 Veritas Storage Foundation obsolete and reorganized filesets *(continued)*

fileset	Description
VRTSfsman	Included in mainpkg
VRTSfsmnd	Included in mainpkg
VRTSfspro	Included in VRTSsfmh
VRTSgapms	Obsolete
VRTSmapro	Included in VRTSsfmh
VRTSorgui	Obsolete
VRTSvail	Obsolete
VRTSvcsdb	Included in VRTSvcsea
VRTSvcsor	Included in VRTSvcsea
VRTSvcsvr	Included in VRTSvcs
VRTSvdid	Obsolete
VRTSvmman	Included in mainpkg
VRTSvmpro	Included in VRTSsfmh
VRTSvrpro	Included in VRTSob
VRTSvrw	Obsolete
VRTSvxmsa	Obsolete
Documentation	All Documentation filesets obsolete

Appendix F

High availability agent information

This appendix includes the following topics:

About agents

An agent is defined as a process that starts, stops, and monitors all configured resources of a type, and reports their status to Veritas Cluster Server (VCS). Agents have both entry points and attributes. Entry points are also known as agent functions and are referred to as "agent functions" throughout the document.

Attributes contain data about the agent. An attribute has a definition and a value. You change attribute values to configure resources, which are defined as the individual components that work together to provide application services to the public network. For example, a resource may be a physical component such as a disk or a network interface card, a software component such as Oracle or a Web server, or a configuration component such as an IP address or mounted file system.

Attributes are either optional or required, although sometimes the attributes that are optional in one configuration may be required in other configurations. Many optional attributes have predefined or default values, which you should change as required. A variety of internal use only attributes also exist. Do not modify these attributes—modifying them can lead to significant problems for your clusters. Attributes have type and dimension. Some attribute values can accept numbers, others can accept alphanumeric values or groups of alphanumeric values, while others are simple boolean on/off values.

The entry points and attributes for each SFCFS agent are described in this appendix.

VCS agents included within SFCFS

SFCFS includes the following VCS agents:

- CVMCluster agent
- CVMVxconfigd agent
- CVMVolDg agent
- CFSMount agent
- CFSfsckd
- Coordination Point agent

An SFCFS installation automatically configures the CVMCluster resource and the CVMVxconfigd resource.

You must configure the CVMVolDg agent for each shared disk group. If the database uses cluster file systems, configure the CFSMount agent for each volume in the disk group.

Use the information in this appendix about the entry points and attributes of the listed agents to make necessary configuration changes. For information on how to modify the VCS configuration:

See the *Veritas Cluster Server Administrator's Guide*

Enabling and disabling intelligent resource monitoring

Review the following procedures to enable or disable intelligent resource monitoring. The intelligent resource monitoring feature is disabled by default. The IMF resource type attribute determines whether an IMF-aware agent must perform intelligent resource monitoring.

To enable intelligent resource monitoring

1 Make the VCS configuration writable.

```
# haconf -makerw
```

2 Run the following command to enable intelligent resource monitoring.

- To enable intelligent monitoring of offline resources:

```
hatype -modify resource_type IMF -update Mode 1
```

- To enable intelligent monitoring of online resources:

```
hatype -modify resource_type IMF -update Mode 2
```

- To enable intelligent monitoring of both online and offline resources:

```
hatype -modify resource_type IMF -update Mode 3
```

3 Change the values of the MonitorFreq key and the RegisterRetryLimit key of the IMF attribute.

Review the agent-specific recommendations in the attribute definition tables to set these attribute key values.

See "Attribute definition for CVMVxconfigd agent" on page 434.

See "Attribute definition for CFSMount agent" on page 442.

See "Attribute definition for CFSfsckd agent" on page 448.

4 Save the VCS configuration.

```
# haconf -dump -makero
```

5 Make sure that the AMF kernel driver is configured on all nodes in the cluster.

```
/etc/init.d/amf.rc status
```

Configure the AMF driver if the command output returns that the AMF driver is not loaded or not configured.

See "Administering the AMF kernel driver" on page 430.

6 Restart the agent. Run the following commands on each node.

```
haagent -stop agent_name -force -sys sys_name
haagent -start agent_name -sys sys_name
```

To disable intelligent resource monitoring

1 Make the VCS configuration writable.

```
# haconf -makerw
```

2 To disable intelligent resource monitoring for all the resources of a certain type, run the following command:

```
hatype -modify resource_type IMF -update Mode 0
```

3 To disable intelligent resource monitoring for a specific resource, run the following command:

```
hares -override resource_name IMF
hares -modify resource_name IMF -update Mode 0
```

4 Save the VCS configuration.

```
# haconf -dump -makero
```

Administering the AMF kernel driver

Review the following procedures to start or stop the AMF kernel driver:

To start the AMF kernel driver

1 Set the value of the AMF_START variable to 1 in the following file:

```
/etc/default/amf
```

2 Start the AMF kernel driver. Run the following command:

```
/etc/init.d/amf.rc start
```

To stop the AMF kernel driver

1 Stop the AMF kernel driver. Run the following command:

```
/etc/init.d/amf.rc stop
```

2 Set the value of the AMF_START variable to 0 in the following file:

```
/etc/default/amf
```

CVMCluster agent

The CVMCluster agent controls system membership on the cluster port that is associated with Veritas Volume Manager (VxVM).

The CVMCluster agent performs the following functions:

- Joins a node to the CVM cluster port.
- Removes a node from the CVM cluster port.
- Monitors the node's cluster membership state.

Entry points for CVMCluster agent

Table F-1 describes the entry points used by the CVMCluster agent.

Table F-1 CVMCluster agent entry points

Entry Point	Description
Online	Joins a node to the CVM cluster port. Enables the Volume Manager cluster functionality by automatically importing the shared disk groups.
Offline	Removes a node from the CVM cluster port.
Monitor	Monitors the node’s CVM cluster membership state.

Attribute definition for CVMCluster agent

Table F-2 describes the user-modifiable attributes of the CVMCluster resource type.

Table F-2 CVMCluster agent attributes

Attribute	Dimension	Description
CVMClustName	string-scalar	Name of the cluster.
CVMNodeAddr	string-association	List of host names and IP addresses.
CVMNodeId	string-association	Associative list. The first part names the system; the second part contains the LLT ID number for the system.

Table F-2 CVMCluster agent attributes *(continued)*

Attribute	Dimension	Description
CVMTransport	string-scalar	Specifies the cluster messaging mechanism. Default = gab **Note:** Do not change this value.
PortConfigd	integer-scalar	The port number that is used by CVM for vxconfigd-level communication.
PortKmsgd	integer-scalar	The port number that is used by CVM for kernel-level communication.
CVMTimeout	integer-scalar	Timeout in seconds used for CVM cluster reconfiguration. Default = 200

CVMCluster agent type definition

The following type definition is included in the file, `CVMTypes.cf`:

```
type CVMCluster (
        static int InfoTimeout = 0
        static int NumThreads = 1
        static int OnlineRetryLimit = 2
        static int OnlineTimeout = 400
        static str ArgList[] = { CVMTransport, CVMClustName,
           CVMNodeAddr, CVMNodeId, PortConfigd, PortKmsgd,
           CVMTimeout }
        NameRule = ""
        str CVMClustName
        str CVMNodeAddr{}
        str CVMNodeId{}
        str CVMTransport
        int PortConfigd
        int PortKmsgd
        int CVMTimeout
  )
```

Note: The attributes `CVMNodeAddr`, `PortConfigd`, and `PortKmsgd` are not used in an SFCFS environment. GAB, the required cluster communication messaging mechanism, does not use them.

CVMCluster agent sample configuration

The following is an example definition for the CVMCluster service group:

```
CVMCluster cvm_clus (
        Critical = 0
        CVMClustName = clus1
        CVMNodeId = { galaxy = 0, nebula = 1 }
        CVMTransport = gab
        CVMTimeout = 200
         )
```

CVMVxconfigd agent

The CVMVxconfigd agent starts and monitors the vxconfigd daemon. The vxconfigd daemon maintains disk and disk group configurations, communicates configuration changes to the kernel, and modifies the configuration information that is stored on disks. CVMVxconfigd must be present in the CVM service group.

The CVMVxconfigd agent is an OnOnly agent; the agent starts the resource when the cluster starts up and VCS restarts the resource when necessary. The Operations attribute specifies these default aspects of startup.

Symantec recommends starting the vxconfigd daemon with the `syslog` option, which enables logging of debug messages. Note that the SFCFS installation configures the `syslog` option for the CVMVxconfigd agent.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

Entry points for CVMVxconfigd agent

Table F-3 describes the entry points for the CVMVxconfigd agent.

Table F-3 CVMVxconfigd entry points

Entry Point	Description
Online	Starts the `vxconfigd` daemon
Offline	N/A
Monitor	Monitors whether `vxconfigd` daemon is running

Table F-3 CVMVxconfigd entry points *(continued)*

Entry Point	Description
imf_init	Initializes the agent to interface with the AMF kernel module. This function runs when the agent starts up.
imf_getnotification	Gets notification about the `vxconfigd` process state. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification. If the `vxconfigd` process fails, the function initiates a traditional CVMVxconfigd monitor entry point.
imf_register	Registers or unregisters the `vxconfigd` process id (pid) with the AMF kernel module. This function runs after the resource goes into steady online state.

Attribute definition for CVMVxconfigd agent

Table F-4 describes the modifiable attributes of the CVMVxconfigd resource type.

Table F-4 CVMVxconfigd agent attribute

Attribute	Dimension	Description
CVMVxconfigdArgs	keylist	List of the arguments that are sent to the `online` entry point. Symantec recommends always specifying the `syslog` option.

Table F-4 CVMVxconfigd agent attribute *(continued)*

Attribute	Dimension	Description
IMF	integer-association	

Table F-4 CVMVxconfigd agent attribute *(continued)*

Attribute	Dimension	Description
		This resource-type level attribute determines whether the CVMVxconfigd agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 0—Does not perform intelligent resource monitoring ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources Default: 0 ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 1 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources ■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the oracle_imf_register agent function to register the resource with the AMF kernel driver. The value of the

Table F-4 CVMVxconfigd agent attribute *(continued)*

Attribute	Dimension	Description
		RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3. For more details of IMF attribute for the agent type, refer to the *Veritas Cluster Server Administrator's Guide*.

CVMVxconfigd agent type definition

The following type definition is included in the CVMTypes.cf file:

```
type CVMVxconfigd (
         static int FaultOnMonitorTimeouts = 2
         static int RestartLimit = 5
         static str ArgList[] { CVMVxconfigdArgs }
         static str Operations = OnOnly
         keylist CVMVxconfigdArgs
         )
```

CVMVxconfigd agent sample configuration

The following is an example definition for the `CVMVxconfigd` resource in the CVM service group:

```
CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )
```

CVMVolDg agent

The CVMVolDg agent manages the CVM disk groups and CVM volumes and volume sets within the disk groups by performing the following functions:

- Imports the shared disk group from the CVM master node
- Starts the volumes and volume sets in the disk group
- Monitors the disk group, volumes, and volume sets
- Optionally, deports the disk group when the dependent applications are taken offline. The agent deports the disk group only if the appropriate attribute is set.

Configure the CVMVolDg agent for each disk group used by a Oracle service group. A disk group must be configured to only one Oracle service group.If cluster file systems are used for the database, configure the CFSMount agent for each volume or volume set in the disk group.

Entry points for CVMVolDg agent

Table F-5 describes the entry points used by the CVMVolDg agent.

Table F-5 CVMVolDg agent entry points

Entry Point	Description
Online	Imports the shared disk group from the CVM master node, if the disk group is not already imported. Starts all volumes and volume sets in the shared disk group specified by the CVMVolume attribute. Sets the disk group activation mode to shared-write if the value of the CVMActivation attribute is sw. You can set the activation mode on both slave and master systems.
Offline	Removes the temporary files created by the online entry point. If the `CVMDeportOnOffline` attribute is set to 1 and if the shared disk group does not contain open volumes on any node in the cluster, the disk group is deported from the CVM master node.

Table F-5 CVMVolDg agent entry points *(continued)*

Entry Point	Description
Monitor	Determines whether the disk group, the volumes, and the volume sets are online. The agent takes a volume set offline if the file system metadata volume of a volume set is discovered to be offline in a monitor cycle. **Note:** If the CFSMount resource goes offline and the file system on the volume set is unmounted, the agent retains the online state of the volume set even if the file system metadata volume in the volume set is offline. This is because the CVMVolDg agent is unable to determine whether or not the volumes that are offline are metadata volumes.
Clean	Removes the temporary files created by the online entry point.

Attribute definition for CVMVolDg agent

Table F-6 describes the user-modifiable attributes of the CVMVolDg resource type.

Table F-6 CVMVolDg agent attributes

Attribute	Dimension	Description
CVMDiskGroup (required)	string-scalar	Shared disk group name.
CVMVolume (required)	string-keylist	Name of shared volumes or volume sets. This list is used to check that the volumes or volume sets are in the correct state before allowing the resource to come online, and that the volumes remain in an enabled state.
CVMActivation (required)	string-scalar	Activation mode for the disk group. Default = `sw (shared-write)` This is a localized attribute.

Table F-6 CVMVolDg agent attributes *(continued)*

Attribute	Dimension	Description
CVMVolumeIoTest(optional)	string-keylist	List of volumes and volume sets that will be periodically polled to test availability. The polling is in the form of 4 KB reads every monitor cycle to a maximum of 10 of the volumes or volume sets in the list. For volume sets, reads are done on a maximum of 10 component volumes in each volume set.
CVMDeportOnOffline (optional)	integer-scalar	Indicates whether or not the shared disk group must be deported when the last online CVMVolDg resource for a disk group is taken offline. The value 1 indicates that the agent will deport the shared disk group from the CVM master node, if not already deported, when the last online CVMVolDg resource for the disk group is taken offline. The value 0 indicates that the agent will not deport the shared disk group when the CVMVolDg resource is taken offline. The default value is set to 0. **Note:** If multiple CVMVolDg resources are configured for a shared disk group, set the value of the attribute to either 1 or 0 for all of the resources. The CVM disk group is deported based on the order in which the CVMVolDg resources are taken offline. If the CVMVolDg resources in the disk group contain a mixed setting of 1 and 0 for the `CVMDeportOnOffline` attribute, the disk group is deported only if the attribute value is 1 for the last CVMVolDg resource taken offline. If the attribute value is 0 for the last CVMVolDg resource taken offline, the disk group is not deported. The deport operation fails if the shared disk group contains open volumes.

CVMVolDg agent type definition

The CVMTypes.cf file includes the CVMVolDg type definition:

```
type CVMVolDg (
        static keylist RegList = { CVMActivation, CVMVolume }
        static int OnlineRetryLimit = 2
        static int OnlineTimeout = 400
        static str ArgList[] = { CVMDiskGroup, CVMVolume, CVMActivation,
        CVMVolumeIoTest, CVMDGAction, CVMDeportOnOffline }
        str CVMDiskGroup
        str CVMDGAction
        keylist CVMVolume
        str CVMActivation
        keylist CVMVolumeIoTest
        int CVMDeportOnOffline
        temp int voldg_stat
)
```

CVMVolDg agent sample configuration

Each Oracle service group requires a CVMVolDg resource type to be defined. The following is a sample configuration:

```
CVMVolDg cvmvoldg1 (
 Critical = 0
 CVMDiskgroup = testdg
 CVMVolume = { vol1, vol2, mvol1, mvol2, snapvol, vset1 }
 CVMVolumeIoTest = { snapvol, vset1 }
 CVMActivation @system1 = sw
 CVMActivation @system2 = sw
 CVMDeportOnOffline = 1
)
```

CFSMount agent

The CFSMount agent brings online, takes offline, and monitors a cluster file system mount point.

The agent executable is located in /opt/VRTSvcs/bin/CFSMount/CFSMountAgent.

The CFSMount type definition is described in the /etc/VRTSvcs/conf/config/CFSTypes.cf file.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

Entry points for CFSMount agent

Table F-7 provides the entry points for the CFSMount agent.

Table F-7 CFSMount agent entry points

Entry Point	Description
Online	Mounts a block device in cluster mode.
Offline	Unmounts the file system, forcing unmount if necessary, and sets primary to secondary if necessary.
Monitor	Determines if the file system is mounted. Checks mount status using the `fsclustadm` command.
Clean	Generates a null operation for a cluster file system mount.
imf_init	Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for the agent. This function runs when the agent starts up.
imf_ getnotification	Gets notification about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification.
imf_register	Registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into steady state (online or offline).

Attribute definition for CFSMount agent

Table F-8 lists user-modifiable attributes of the CFSMount Agent resource type.

Table F-8 CFSMount Agent attributes

Attribute	Dimension	Description
MountPoint	string-scalar	Directory for the mount point.
BlockDevice	string-scalar	Block device for the mount point.

Table F-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description
NodeList	string-keylist	List of nodes on which to mount. If NodeList is NULL, the agent uses the service group system list.

Table F-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description
IMF	integer-association	

Table F-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description
		Resource-type level attribute that determines whether the CFSMount agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 0—Does not perform intelligent resource monitoring ■ 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources ■ 3—Performs intelligent resource monitoring for both online and for offline resources Default: 0 ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 1 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources

Table F-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description
		■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the oracle_imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3. See "Enabling and disabling intelligent resource monitoring" on page 428.

MountOpt
(optional)
	string-scalar	Options for the mount command. To create a valid MountOpt attribute string:
		■ Use the VxFS type-specific options only.
		■ Do not use the -o flag to specify the VxFS-specific options.
		■ Be aware the cluster option is not required.
		■ Specify options in comma-separated list:
		`ro`
		`ro,cluster`
		`blkclear,mincache=closesync`

Policy (optional)	string-scalar	List of nodes to assume the primaryship of the cluster file system if the primary fails. If set to NULL or if none of the hosts specified in the list is active when the primary fails, a node is randomly selected from the set of active nodes to assume primaryship.

CFSMount agent type definition

The `CFSTypes.cf` file includes the CFSMount agent type definition:

```
type CFSMount (
    static keylist RegList = { MountOpt, Policy, NodeList, ForceOff, SetPrimary }
    static keylist SupportedActions = { primary }
    static int FaultOnMonitorTimeouts = 1
    static int OnlineWaitLimit = 1
    static str ArgList[] = { MountPoint, BlockDevice, MountOpt, Primary, AMFMountType }
    str MountPoint
    str MountType
    str BlockDevice
    str MountOpt
    keylist NodeList
    keylist Policy
    temp str Primary
    str SetPrimary
    temp str RemountRes
    temp str AMFMountType
    str ForceOff
)
```

CFSMount agent sample configuration

Each Oracle service group requires a CFSMount resource type to be defined:

```
CFSMount ora_mount (
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol1"
        Primary = nebula;
        )
```

To see CFSMount defined in a more extensive example:

CFSfsckd agent

The CFSfsckd agent starts, stops, and monitors the `vxfsckd` process. The CFSfsckd agent executable is `/opt/VRTSvcs/bin/CFSfsckd/CFSfsckdAgent`. The type definition is in the `/etc/VRTSvcs/conf/config/CFSTypes.cf` file. The configuration is added to the `main.cf` file after running the `cfscluster config` command.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

Entry points for CFSfsckd agent

Table F-9 describes the CFSfsckd agent entry points.

Table F-9 CFSfsckd agent entry points

Entry Points	Description
Online	Starts the vxfsckd process.
Offline	Kills the vxfsckd process.
Monitor	Checks whether the vxfsckd process is running.
Clean	A null operation for a cluster file system mount.
imf_init	Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for the agent. This function runs when the agent starts up.
imf_ getnotification	Gets notification about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification.
imf_register	Registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into steady state (online or offline).

Attribute definition for CFSfsckd agent

Table F-10 lists user-modifiable attributes of the CFSfsckd Agent resource type.

Table F-10 CFSfsckd Agent attributes

Attribute	Dimension	Description
IMF	integer-association	

Table F-10 CFSfsckd Agent attributes *(continued)*

Attribute	Dimension	Description
		Resource-type level attribute that determines whether the CFSfsckd agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 0—Does not perform intelligent resource monitoring ■ 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources ■ 3—Performs intelligent resource monitoring for both online and for offline resources Default: 0 ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 1 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources

Table F-10 CFSfsckd Agent attributes *(continued)*

Attribute	Dimension	Description
		■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the oracle_imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3. See "Enabling and disabling intelligent resource monitoring" on page 428.

CFSfsckd agent type definition

The CFSfsckd type definition:

```
type CFSfsckd (
        static int RestartLimit = 1
        str ActivationMode{}
)
```

CFSfsckd agent sample configuration

This is a sample of CFSfsckd configuration:

```
CFSfsckd vxfsckd (
)
```

Appendix G

Troubleshooting information

This appendix includes the following topics:

Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

What to do if you see a licensing reminder

In this release, you can install without a license key. In order to comply with the End User License Agreement, you must either install a license key or make the host managed by a Management Server. If you do not comply with these terms within 60 days, the following warning messages result:

```
WARNING V-365-1-1 This host is not entitled to run Veritas Storage
Foundation/Veritas Cluster Server.As set forth in the End User
```

```
License Agreement (EULA) you must complete one of the two options
set forth below. To comply with this condition of the EULA and
stop logging of this message, you have <nn> days to either:
- make this host managed by a Management Server (see
  http://go.symantec.com/sfhakeyless for details and free download),
  or
- add a valid license key matching the functionality in use on this host
  using the command 'vxlicinst'
```

To comply with the terms of the EULA, and remove these messages, you must do one of the following within 60 days:

- Install a valid license key corresponding to the functionality in use on the host.
  See "Installing Veritas product license keys" on page 52.
  After you install the license key, you must validate the license key using the following command:

  ```
  # vxkeyless display
  ```

- Continue with keyless licensing by managing the server or cluster with a management server.
  For more information about keyless licensing, see the following URL:
  http://go.symantec.com/sfhakeyless

Troubleshooting an installation on AIX

Save a copy of `/var/adm/ras/errtmplt` and `/etc/trcfmt` files before you install the product. If the filesets fail to install due to the `template file is corrupted` error message, replace `/var/adm/ras/errtmplt` file and `/etc/trcfmt` file with the ones that you had saved, uninstall all the filesets installed.

See "Preparing to uninstall a SFCFS product" on page 357.

Then reinstall.

Storage Foundation Cluster File System installation issues

If you encounter any issues installing SFCFS, refer to the following paragraphs for typical problems and their solutions:

Incorrect permissions for root on remote system

The permissions are inappropriate. Make sure you have remote root access permission on each system to which you are installing.

```
Failed to setup rsh communication on 10.198.89.241:
'rsh 10.198.89.241 <command>' failed
Trying to setup ssh communication on 10.198.89.241.
Failed to setup ssh communication on 10.198.89.241:
Login denied

Failed to login to remote system(s) 10.198.89.241.
Please make sure the password(s) are correct and superuser(root)
can login to the remote system(s) with the password(s).
If you want to setup rsh on remote system(s), please make sure
rsh with command argument ('rsh <host> <command>') is not
denied by remote system(s).

Either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication

Would you like the installer to setup ssh/rsh communication
automatically between the nodes?
Superuser passwords for the systems will be asked. [y,n,q] (y) n

System verification did not complete successfully

The following errors were discovered on the systems:

The ssh permission denied on 10.198.89.241
rsh exited 1 on 10.198.89.241
either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication
```

Suggested solution: You need to set up the systems to allow remote access using `ssh` or `rsh`.

See "About configuring secure shell or remote shell communication modes before installing products" on page 411.

Note: Remove remote shell permissions after completing the SFCFS installation and configuration.

Resource temporarily unavailable

If the installation fails with the following error message on the console:

```
fork() failed: Resource temporarily unavailable
```

The value of maximum number of processes allowed per user may not be large enough. This kernel attribute is a tunable and can be changed on any node of the cluster.

To determine the current value of "Maximum number of PROCESSES allowed per user", enter:

```
# lsattr -H -E -l sys0 -a maxuproc
```

To see the default value of this tunable and its valid range of values, enter:

```
# odmget -q "attribute=maxuproc" PdAt
```

If necessary, you can change the value of the tunable using the smitty interface:

```
# smitty chgsys
```

You can also directly change the CuAt class using the following command:

```
# chdev -l sys0 -a maxuproc=600
```

Increasing the value of the parameter takes effect immediately; otherwise the change takes effect after a reboot.

See the `smitty` and `chdev` manual pages.

Inaccessible system

The system you specified is not accessible. This could be for a variety of reasons such as, the system name was entered incorrectly or the system is not available over the network.

```
 Verifying systems: 12% .....................................
 Estimated time remaining: 0:10 1 of 8
 Checking system communication ............................. Done
System verification did not complete successfully
The following errors were discovered on the systems:
cannot resolve hostname host1
Enter the AIX system names separated by spaces: q,? (host1)
```

Suggested solution: Verify that you entered the system name correctly; use the `ping`(1M) command to verify the accessibility of the host.

Storage Foundation Cluster File System problems

If there is a device failure or controller failure to a device, the file system may become disabled cluster-wide. To address the problem, unmount file system on all the nodes, then run a full `fsck`. When the file system check completes, mount all nodes again.

Unmount failures

The `umount` command can fail if a reference is being held by an NFS server. Unshare the mount point and try the unmount again.

Mount failures

Mounting a file system can fail for the following reasons:

- The file system is not using disk layout Version 6 or 7.
- The mount options do not match the options of already mounted nodes.
- A cluster file system is mounted by default with the `qio` option enabled if the node has a Quick I/O for Databases license installed, even if the `qio` mount option was not explicitly specified. If the Quick I/O license is not installed, a cluster file system is mounted without the `qio` option enabled. So if some nodes in the cluster have a Quick I/O license installed and others do not, a cluster mount can succeed on some nodes and fail on others due to different mount options. To avoid this situation, ensure that Quick I/O licensing is uniformly applied, or be careful to mount the cluster file system with the `qio/noqio` option appropriately specified on each node of the cluster.
  See the `mount`(1M) manual page.
- A shared CVM volume was not specified.
- The device is still mounted as a local file system somewhere on the cluster. Unmount the device.
- The `fsck` or `mkfs` command is being run on the same volume from another node, or the volume is mounted in non-cluster mode from another node.
- The `vxfsckd` daemon is not running. This typically happens only if the `CFSfsckd` agent was not started correctly.
- If `mount` fails with an error message:

  ```
  vxfs mount: device already mounted, ...
  ```

The device is in use by `mount`, `mkfs` or `fsck` on the same node. This error cannot be generated from another node in the cluster.

- If this error message displays:

  ```
  mount: slow
  ```

  The node may be in the process of joining the cluster.

- If you try to mount a file system that is already mounted without `-o cluster` option (that is, not in shared mode) on another cluster node,

  ```
  # mount -V vxfs /dev/vx/dsk/share/vol01 /vol01
  ```

  The following error message displays:

  ```
  vxfs mount: /dev/vx/dsk/share/vol01 is already mounted,
    /vol01 is busy, allowable number of mount points exceeded,
    or cluster reservation failed for the volume
  ```

Command failures

This section describes command failures.

- Manual pages not accessible with the `man` command. Set the MANPATH environment variable appropriately.
  See "Setting environment variables" on page 33.
- The `mount`, `fsck`, and `mkfs` utilities reserve a shared volume. They fail on volumes that are in use. Be careful when accessing shared volumes with other utilities such as `dd`, it is possible for these commands to destroy data on the disk.
- Running some commands, such as `vxupgrade -n 7 /vol02`, can generate the following error message:

  ```
  vxfs vxupgrade: ERROR: not primary in a cluster file system
  ```

  This means that you can run this command only on the primary, that is, the system that mounted this file system first.

Performance issues

Quick I/O File system performance is adversely affected if a cluster file system is mounted with the `qio` option enabled, but the file system is not used for Quick I/O files. Because `qio` is enabled by default, if you do not intend to use a shared file system for Quick I/O, explicitly specify the `noqio` option when mounting.

High availability issues

This section describes high availability issues.

Network partition and jeopardy

Network partition (or split brain) is a condition where a network failure can be misinterpreted as a failure of one or more nodes in a cluster. If one system in the cluster incorrectly assumes that another system failed, it may restart applications already running on the other system, thereby corrupting data. CFS tries to prevent this by having redundant heartbeat links.

At least one link must be active to maintain the integrity of the cluster. If all the links go down, after the last network link is broken, the node can no longer communicate with other nodes in the cluster. Thus the cluster is in one of two possible states. Either the last network link is broken (called a network partition condition), or the last network link is okay, but the node crashed, in which case it is not a network partition problem. It is not possible to identify whether it is the first or second state, so a kernel message is issued to indicate that a network partition may exist and there is a possibility of data corruption.

Jeopardy is a condition where a node in the cluster has a problem connecting to other nodes. In this situation, the link or disk heartbeat may be down, so a jeopardy warning may be displayed. Specifically, this message appears when a node has only one remaining link to the cluster and that link is a network link. This is considered a critical event because the node may lose its only remaining connection to the network.

Warning: Do not remove the communication links while shared storage is still connected.

Low memory

Under heavy loads, software that manages heartbeat communication links may not be able to allocate kernel memory. If this occurs, a node halts to avoid any chance of network partitioning. Reduce the load on the node if this happens frequently.

A similar situation may occur if the values in the `/etc/lltab` files on all cluster nodes are not correct or identical.

Appendix H

Troubleshooting cluster installation

This appendix includes the following topics:

Installer cannot create UUID for the cluster

The installer displays the following error message if the installer cannot find the uuidconfig.pl script before it configures the UUID for the cluster:

```
Couldn't find uuidconfig.pl for uuid configuration,
please create uuid manually before start vcs
```

You may see the error message during SFCFS configuration, upgrade, or when you add a node to the cluster using the installer.

Workaround: To start SFCFS, you must run the uuidconfig.pl script manually to configure the UUID on each cluster node.

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

The vxfentsthdw utility fails when SCSI TEST UNIT READY command fails

While running the vxfentsthdw utility, you may see a message that resembles as follows:

```
Issuing SCSI TEST UNIT READY to disk reserved by other node
FAILED.
Contact the storage provider to have the hardware configuration
fixed.
```

The disk array does not support returning success for a `SCSI TEST UNIT READY` command when another host has the disk reserved using SCSI-3 persistent reservations. This happens with the Hitachi Data Systems 99XX arrays if bit 186 of the system mode option is not enabled.

Troubleshooting server-based I/O fencing

All CP server operations and messages are logged in the `/var/VRTScps/log` directory in a detailed and easy to read format. The entries are sorted by date and time. The logs can be used for troubleshooting purposes or to review for any possible security issue on the system that hosts the CP server.

The following files contain logs and text files that may be useful in understanding and troubleshooting a CP server:

- `/var/VRTScps/log/cpserver_[ABC].log`
- `/var/VRTSat/vrtsat_broker.txt` (Security related)
- If the vxcpserv process fails on the CP server, then review the following diagnostic files:
  - `/var/VRTScps/diag/FFDC_CPS_`*`pid`*`_vxcpserv.log`
  - `/var/VRTScps/diag/stack_`*`pid`*`_vxcpserv.txt`

Note: If the vxcpserv process fails on the CP server, these files are present in addition to a core file. VCS restarts vxcpserv process automatically in such situations.

The file `/var/VRTSvcs/log/vxfen/vxfend_[ABC].log` contains logs and text files that may be useful in understanding and troubleshooting fencing-related issues on a SFCFS cluster (client cluster) node.

See "Troubleshooting issues related to the CP server service group" on page 463.

See "Checking the connectivity of CP server" on page 463.

See "Issues during fencing startup on SFCFS cluster nodes set up for server-based fencing" on page 464.

See "Issues during online migration of coordination points" on page 466.

See "Troubleshooting server-based I/O fencing in mixed mode" on page 467.

See "Checking keys on coordination points when vxfen_mechanism value is set to cps" on page 471.

Troubleshooting issues related to the CP server service group

If you cannot bring up the CPSSG service group after the CP server configuration, perform the following steps:

- Verify that the CPSSG service group and its resources are valid and properly configured in the VCS configuration.
- Check the VCS engine log (`/var/VRTSvcs/log/engine_[ABC].log`) to see if any of the CPSSG service group resources are FAULTED.
- Review the sample dependency graphs to make sure the required resources are configured correctly.

Checking the connectivity of CP server

You can test the connectivity of CP server using the `cpsadm` command.

You must have set the environment variables CPS_USERNAME and CPS_DOMAINTYPE to run the `cpsadm` command on the SFCFS cluster (client cluster) nodes.

To check the connectivity of CP server

- Run the following command to check whether a CP server is up and running at a process level:

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

  where *cp_server* is the virtual IP address or virtual hostname on which the CP server is listening.

Troubleshooting server-based fencing on the SFCFS cluster nodes

The file `/var/VRTSvcs/log/vxfen/vxfend_[ABC].log` contains logs and text files that may be useful in understanding and troubleshooting fencing-related issues on a SFCFS cluster (client cluster) node.

Issues during fencing startup on SFCFS cluster nodes set up for server-based fencing

Table H-1 Fencing startup issues on SFCFS cluster (client cluster) nodes

Issue	Description and resolution
`cpsadm` command on the SFCFS cluster gives connection error	If you receive a connection error message after issuing the `cpsadm` command on the SFCFS cluster, perform the following actions: ■ Ensure that the CP server is reachable from all the SFCFS cluster nodes. ■ Check that the SFCFS cluster nodes use the correct CP server virtual IP or virtual hostname and the correct port number. Check the /etc/vxfenmode file. ■ Ensure that the running CP server is using the same virtual IP/virtual hostname and port number.
Authorization failure	Authorization failure occurs when the CP server's nodes or users are not added in the CP server configuration. Therefore, fencing on the SFCFS cluster (client cluster) node is not allowed to access the CP server and register itself on the CP server. Fencing fails to come up if it fails to register with a majority of the coordination points. To resolve this issue, add the CP server node and user in the CP server configuration and restart fencing. See "Preparing the CP servers manually for use by the SFCFS cluster" on page 167.

Table H-1 Fencing startup issues on SFCFS cluster (client cluster) nodes *(continued)*

Issue	Description and resolution
Authentication failure	If you had configured secure communication between the CP server and the SFCFS cluster (client cluster) nodes, authentication failure can occur due to the following causes: ■ Symantec Product Authentication Services (AT) is not properly configured on the CP server and/or the SFCFS cluster. ■ The CP server and the SFCFS cluster nodes use the same root broker but the certificate hash of the root broker is not same on the SFCFS cluster and the CP server. Run the following command on both the CP server and the SFCFS cluster to see the certificate hash: `# cpsat showalltrustedcreds` ■ The CP server and the SFCFS cluster nodes use different root brokers, and trust is not established between the authentication brokers: ■ The hostname of the SFCFS cluster nodes is not the same hostname used when configuring AT. The hostname of the SFCFS cluster nodes must be set to the hostname used when configuring AT. You can view the fully qualified hostname registered with AT using the `cpsat showcred` command. After entering this command, the hostname appears in the User Name field. ■ The CP server and SFCFS cluster do not have the same security setting. In order to configure secure communication, both the CP server and the SFCFS cluster must have same security setting. In order to have the same security setting, the security parameter must have same value in the `/etc/vxcps.conf` file on CP server and in the `/etc/vxfenmode` file on the SFCFS cluster (client cluster) nodes.

Table H-1 Fencing startup issues on SFCFS cluster (client cluster) nodes *(continued)*

Issue	Description and resolution
Preexisting split-brain	Assume the following situations to understand preexisting split-brain in server-based fencing: ■ There are three CP servers acting as coordination points. One of the three CP servers then becomes inaccessible. While in this state, also one client node leaves the cluster. When the inaccessible CP server restarts, it has a stale registration from the node which left the SFCFS cluster. In this case, no new nodes can join the cluster. Each node that attempts to join the cluster gets a list of registrations from the CP server. One CP server includes an extra registration (of the node which left earlier). This makes the joiner node conclude that there exists a preexisting split-brain between the joiner node and the node which is represented by the stale registration. ■ All the client nodes have crashed simultaneously, due to which fencing keys are not cleared from the CP servers. Consequently, when the nodes restart, the vxfen configuration fails reporting preexisting split brain. These situations are similar to that of preexisting split-brain with coordinator disks, where the problem is solved by the administrator running the `vxfenclearpre` command. A similar solution is required in server-based fencing using the `cpsadm` command. Run the `cpsadm` command to clear a registration on a CP server: `# cpsadm -s cp_server -a unreg_node -c cluster_name -n nodeid` where *cp_server* is the virtual IP address or virtual hostname on which the CP server is listening, *cluster_name* is the VCS name for the SFCFS cluster, and *nodeid* specifies the node id of SFCFS cluster node. Ensure that fencing is not already running on a node before clearing its registration on the CP server. After removing all stale registrations, the joiner node will be able to join the cluster.

Issues during online migration of coordination points

During online migration of coordination points using the vxfenswap utility, the operation is automatically rolled back if a failure is encountered during validation of coordination points from all the cluster nodes.

Validation failure of the new set of coordination points can occur in the following circumstances:

■ The `/etc/vxfenmode` file is not updated on all the SFCFS cluster nodes, because new coordination points on the node were being picked up from an old `/etc/vxfenmode` file.

- The coordination points listed in the `/etc/vxfenmode` file on the different SFCFS cluster nodes are not the same. If different coordination points are listed in the /etc/vxfenmode file on the cluster nodes, then the operation fails due to failure during the coordination point snapshot check.
- There is no network connectivity from one or more SFCFS cluster nodes to the CP server(s).
- Cluster, nodes, or users for the SFCFS cluster nodes have not been added on the new CP servers, thereby causing authorization failure.

Vxfen service group activity after issuing the vxfenswap command

After issuing the `vxfenswap` command, the Coordination Point agent reads the details of coordination points from the `vxfenconfig -l` output and starts monitoring the registrations on them.

During vxfenswap, when the vxfenmode file is being changed by the user, the Coordination Point agent does not move to FAULTED state but continues monitoring the old set of coordination points.

As long as the changes to vxfenmode file are not committed or the new set of coordination points are not re-elected in `vxfenconfig -l` output, the Coordination Point agent continues monitoring the old set of coordination points it read from `vxfenconfig -l` output in every monitor cycle.

The status of the Coordination Point agent (either ONLINE or FAULTED) depends upon the accessibility of the coordination points, the registrations on these coordination points, and the fault tolerance value.

When the changes to vxfenmode file are committed and reflected in the `vxfenconfig -l` output, then the Coordination Point agent reads the new set of coordination points and proceeds to monitor them in its new monitor cycle.

Troubleshooting server-based I/O fencing in mixed mode

Use the following procedure to troubleshoot a mixed I/O fencing configuration (configuration which uses both coordinator disks and CP server for I/O fencing).

This procedure uses the following commands to obtain I/O fencing information:

- To obtain I/O fencing cluster information on the coordinator disks, run the following command on one of the cluster nodes:

```
# vxfenadm -s diskname
```

Any keys other than the valid keys used by the cluster nodes that appear in the command output are spurious keys.

- To obtain I/O fencing cluster information on the CP server, run the following command on one of the cluster nodes:

  ```
  # cpsadm -s cp_server -a list_membership -c cluster_name
  ```

  where *cp server* is the virtual IP address or virtual hostname on which the CP server is listening, and *cluster name* is the VCS name for the SFCFS cluster.
  Nodes which are not in GAB membership, but registered with CP server indicate a pre-existing network partition.
  Note that when running this command on the SFCFS cluster nodes, you need to first export the CPS_USERNAME and CPS_DOMAINTYPE variables.
  The CPS_USERNAME value is the user name which is added for this node on the CP server.

- To obtain the user name, run the following command on the CP server:

  ```
  # cpsadm -s cp_server -a list_users
  ```

  where *cp server* is the virtual IP address or virtual hostname on which the CP server is listening.
  The CPS_DOMAINTYPE value is vx.
  The following are export variable command examples:

```
# export CPS_USERNAME=_HA_VCS_test-system@HA_SERVICES@test-system.symantec.com
```

```
# export CPS_DOMAINTYPE=vx
```

Once a pre-existing network partition is detected using the above commands, all spurious keys on the coordinator disks or CP server must be removed by the administrator.

To troubleshoot server-based I/O fencing configuration in mixed mode

1 Review the current I/O fencing configuration by accessing and viewing the information in the vxfenmode file.

Enter the following command on one of the SFCFS cluster nodes:

```
# cat /etc/vxfenmode

vxfen_mode=customized
vxfen_mechanism=cps
scsi3_disk_policy=dmp
security=0
cps1=[10.140.94.101]:14250
vxfendg=vxfencoorddg
```

2 Review the I/O fencing cluster information.

Enter the `vxfenadm -d` command on one of the cluster nodes:

```
# vxfenadm -d

I/O Fencing Cluster Information:
================================

 Fencing Protocol Version: 201
 Fencing Mode: Customized
 Fencing Mechanism: cps
 Cluster Members:

        * 0 (galaxy)
          1 (nebula)

 RFSM State Information:
        node   0 in state  8 (running)
        node   1 in state  8 (running)
```

3 Review the SCSI registration keys for the coordinator disks used in the I/O fencing configuration.

The variables *disk_7* and *disk_8* in the following commands represent the disk names in your setup.

Enter the `vxfenadm -s` command on each of the SFCFS cluster nodes.

```
# vxfenadm -s /dev/vx/rdmp/disk_7
```

```
Device Name: /dev/vx/rdmp/disk_7
Total Number Of Keys: 2
key[0]:
         [Numeric Format]:  86,70,66,69,65,68,48,48
         [Character Format]: VFBEAD00
         [Node Format]: Cluster ID: 57069 Node ID: 0   Node Name: galaxy
key[1]:
         [Numeric Format]:  86,70,66,69,65,68,48,49
         [Character Format]: VFBEAD01
*        [Node Format]: Cluster ID: 57069 Node ID: 1   Node Name: nebula
```

Run the command on the other node:

```
# vxfenadm -s /dev/vx/rdmp/disk_8
```

```
Device Name: /dev/vx/rdmp/disk_8
Total Number Of Keys: 2
key[0]:
         [Numeric Format]:  86,70,66,69,65,68,48,48
         [Character Format]: VFBEAD00
         [Node Format]: Cluster ID: 57069 Node ID: 0   Node Name: galaxy
key[1]:
         [Numeric Format]:  86,70,66,69,65,68,48,49
         [Character Format]: VFBEAD01
*        [Node Format]: Cluster ID: 57069 Node ID: 1   Node Name: nebula
```

4 Review the CP server information about the cluster nodes. On the CP server, run the `cpsadm list nodes` command to review a list of nodes in the cluster.

```
# cpsadm -s cp_server -a list_nodes
```

where *cp server* is the virtual IP address or virtual hostname on which the CP server is listening.

5 Review the CP server list membership. On the CP server, run the following command to review the list membership.

```
# cpsadm -s cp_server -a list_membership -c cluster_name
```

where *cp_server* is the virtual IP address or virtual hostname on which the CP server is listening, and *cluster_name* is the VCS name for the SFCFS cluster.

For example:

```
# cpsadm -s 10.140.94.101 -a list_membership -c gl-ss2

List of registered nodes: 0 1
```

Checking keys on coordination points when vxfen_mechanism value is set to cps

When I/O fencing is configured in customized mode and the vxfen_mechanism value is set to cps, the recommended way of reading keys from the coordination points (coordinator disks and CP servers) is as follows:

- For coordinator disks, the disks can be put in a file and then information about them supplied to the `vxfenadm` command.
  For example:

  ```
  # vxfenadm -s all -f file_name
  ```

- For CP servers, the `cpsadm` command can be used to obtain the membership of the SFCFS cluster.
  For example:

  ```
  # cpsadm -s cp_server -a list_membership -c cluster_name
  ```

where *cp_server* is the virtual IP address or virtual hostname on which CP server is configured, and *cluster_name* is the VCS name for the SFCFS cluster.

Appendix I

Sample SFCFS cluster setup diagrams for CP server-based I/O fencing

This appendix includes the following topics:

Configuration diagrams for setting up server-based I/O fencing

The following CP server configuration diagrams can be used as guides when setting up CP server within your configuration:

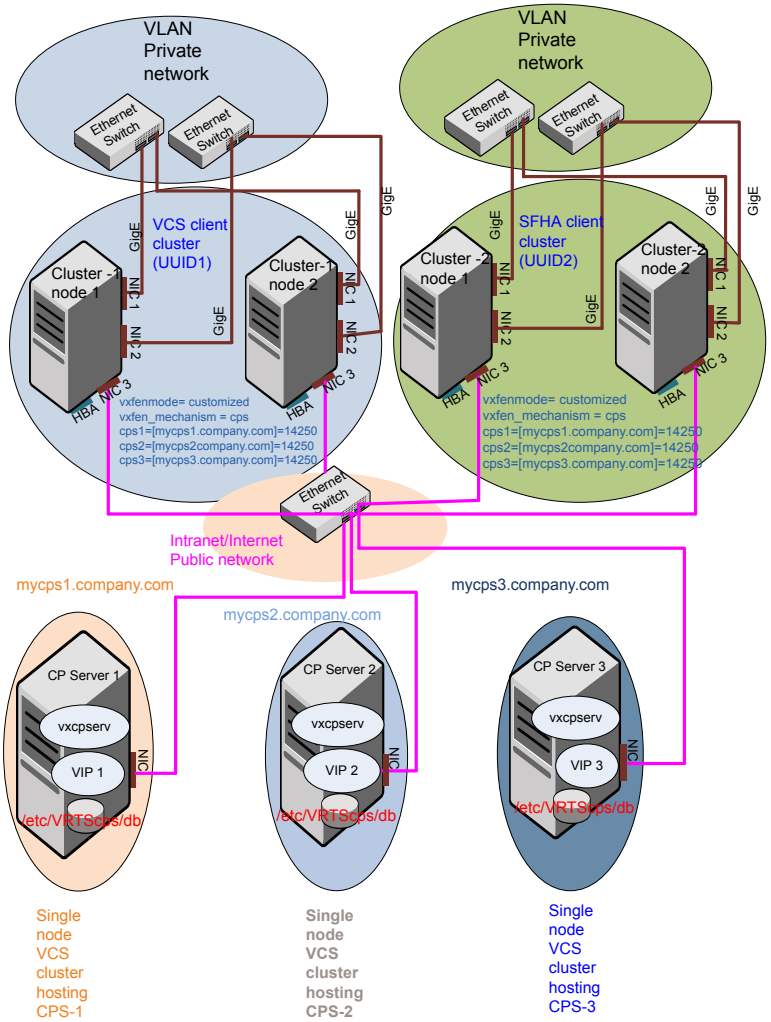
- Two unique client clusters that are served by 3 CP servers:
  See Figure I-1 on page 474.
- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:
- Two node campus cluster that is served be remote CP server and 2 SCSI-3 disks:
- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:

Two unique client clusters served by 3 CP servers

Figure I-1 displays a configuration where two unique client clusters are being served by 3 CP servers (coordination points). Each client cluster has its own unique user ID (UUID1 and UUID2).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

Figure I-1 Two unique client clusters served by 3 CP servers



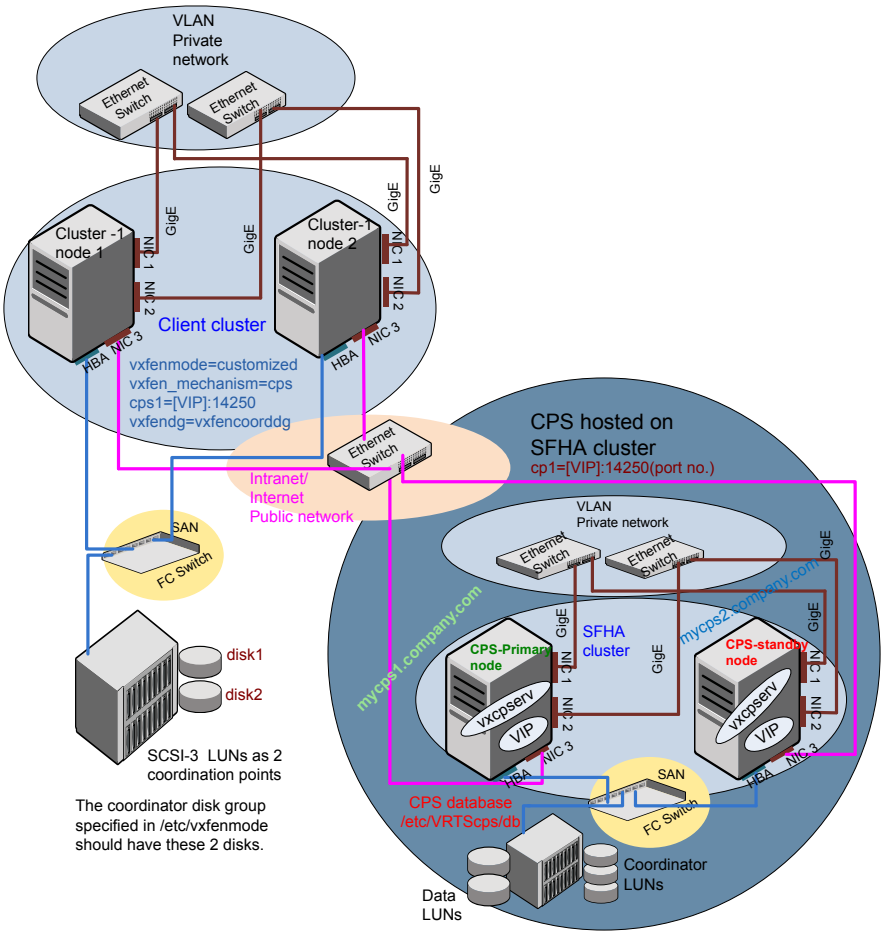
Client cluster served by highly available CPS and 2 SCSI-3 disks

Figure I-2 displays a configuration where a client cluster is served by one highly available CP server and 2 local SCSI-3 LUNs (disks).

In the `vxfenmode` file on the client nodes, `vxfenmode` is set to customized with vxfen mechanism set to `cps`.

The two SCSI-3 disks are part of the disk group vxfencoorddg. The third coordination point is a CP server hosted on an SFHA cluster, with its own shared database and coordinator disks.

Figure I-2 Client cluster served by highly available CP server and 2 SCSI-3 disks



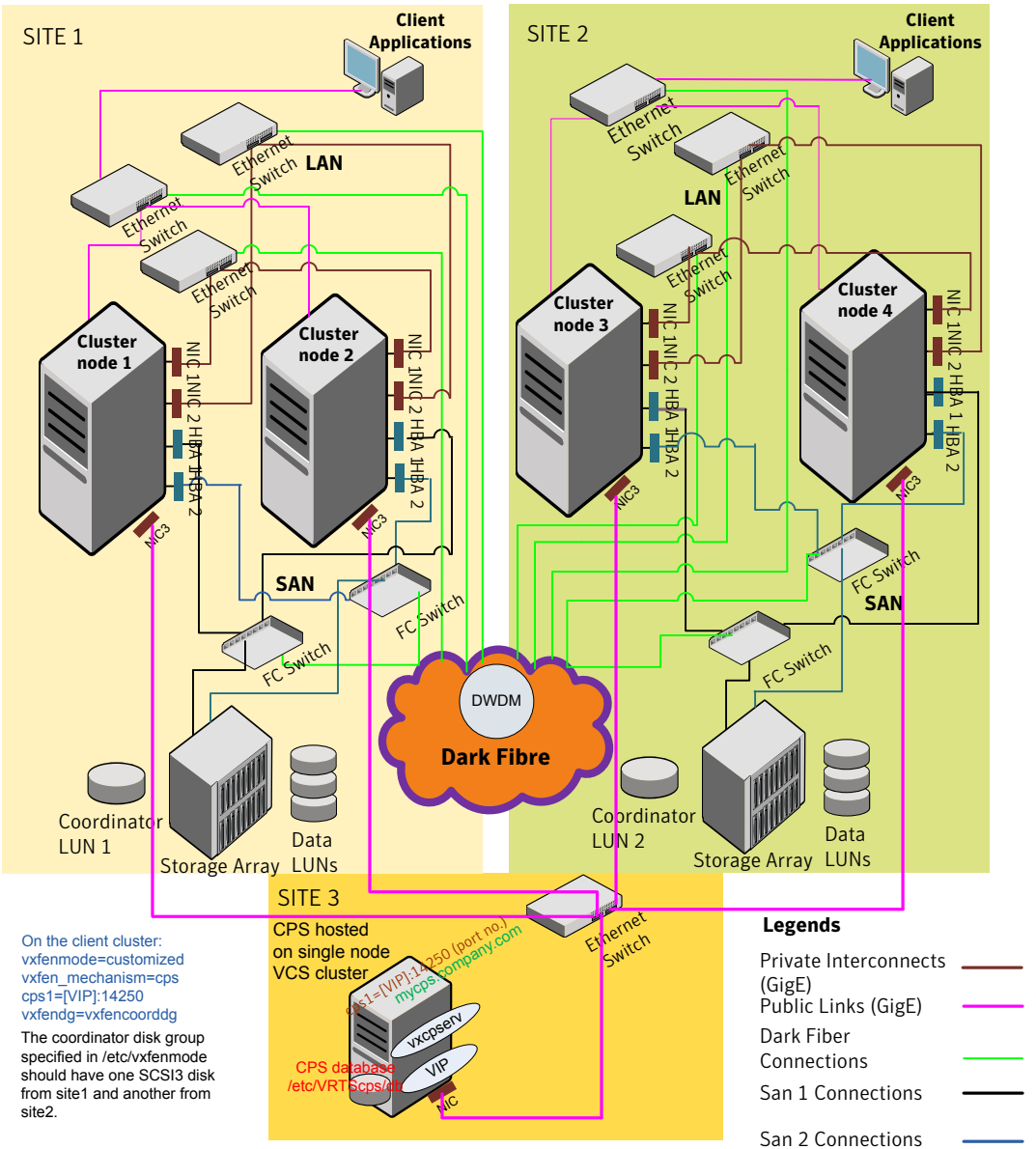
Two node campus cluster served by remote CP server and 2 SCSI-3 disks

Figure I-3 displays a configuration where a two node campus cluster is being served by one remote CP server and 2 local SCSI-3 LUN (disks).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

The two SCSI-3 disks (one from each site) are part of disk group vxfencoorddg. The third coordination point is a CP server on a single node VCS cluster.

Figure I-3 Two node campus cluster served by remote CP server and 2 SCSI-3



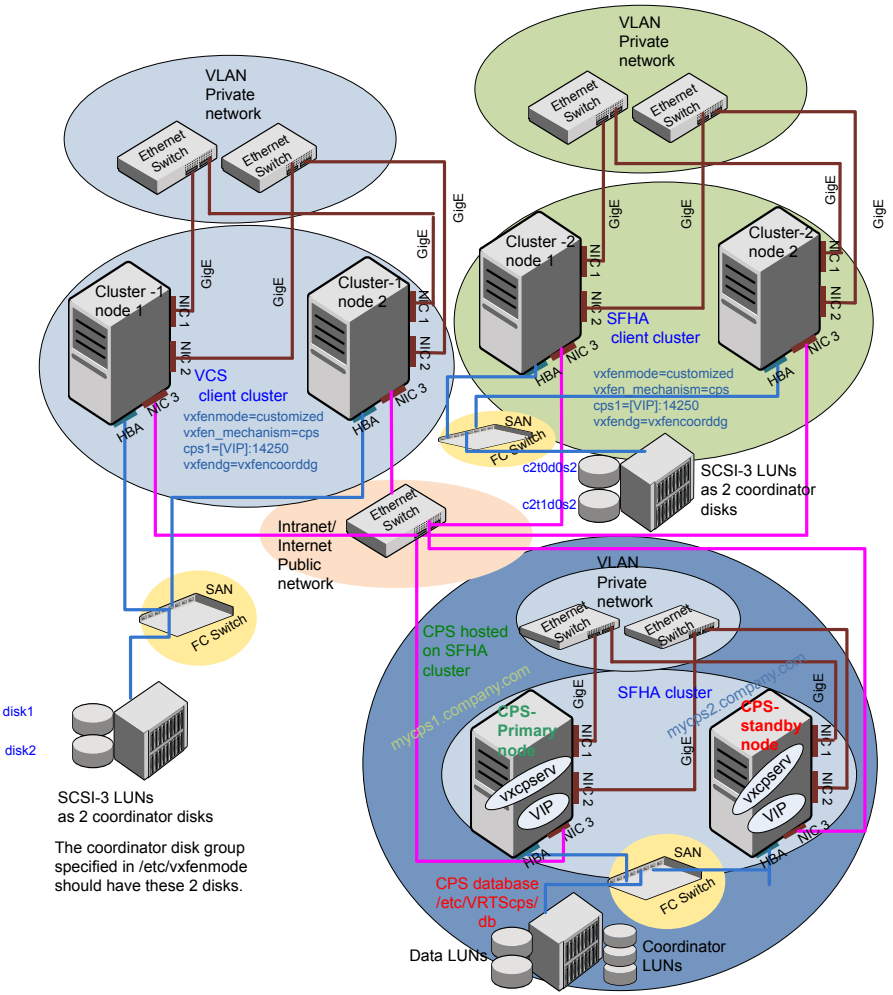
Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

Figure I-4 displays a configuration where multiple client clusters are being served by one highly available CP server and 2 local SCSI-3 LUNS (disks).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

The two SCSI-3 disks are are part of the disk group vxfencoorddg. The third coordination point is a CP server, hosted on an SFHA cluster, with its own shared database and coordinator disks.

Figure I-4 Multiple client clusters served by highly available CP server and 2 SCSI-3 disks



Appendix J

Changing NFS server major numbers for VxVM volumes

This appendix includes the following topics:

Changing NFS server major numbers for VxVM volumes

In a VCS cluster, block devices providing NFS service must have the same major and minor numbers on each cluster node. Major numbers identify required device drivers (such as AIX partition or VxVM volume). Minor numbers identify the specific devices themselves. NFS also uses major and minor numbers to identify the exported file system. Major and minor numbers must be verified to ensure that the NFS identity for the file system is the same when exported from each node.

Use the `haremajor` command to determine and reassign the major number that a system uses for shared VxVM volume block devices. For Veritas Volume Manager, the major number is set to the `vxio` driver number. To be highly available, each NFS server in a VCS cluster must have the same `vxio` driver number, or major number.

To list the major number currently in use on a system

- Use the command:

```
# haremajor -v
55
```

Run this command on each cluster node. If major numbers are not the same on each node, you must change them on the nodes so that they are identical.

To list the available major numbers for a system

- Use the command:

```
# haremajor -a
54,56..58,60,62..
```

The output shows the numbers that are not in use on the system where the command is issued.

To reset the major number on a system

- You can reset the major number to an available number on a system. For example, to set the major number to 75 type:

```
# haremajor -s 75
```

Appendix K

Configuring LLT over UDP using IPv6

This appendix includes the following topics:

Using the UDP layer of IPv6 for LLT

Veritas Storage Foundation Cluster File System 5.1 SP1 provides the option of using LLT over the UDP (User Datagram Protocol) layer for clusters using wide-area networks and routers. UDP makes LLT packets routable and thus able to span longer distances more economically.

When to use LLT over UDP

Use LLT over UDP in the following situations:

- LLT must be used over WANs
- When hardware, such as blade servers, do not support LLT over Ethernet

Manually configuring LLT over UDP using IPv6

The following checklist is to configure LLT over UDP:

- For UDP6, the multicast address is set to "-".
- Make sure that each NIC has an IPv6 address that is configured before configuring LLT.

- Make sure the IPv6 addresses in the /etc/llttab files are consistent with the IPv6 addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port.
  See "Selecting UDP ports" on page 485.
- For the links that cross an IP router, disable multicast features and specify the IPv6 address of each link manually in the /etc/llttab file.
  See "Sample configuration: links crossing IP routers" on page 487.

The link command in the /etc/llttab file

Review the link command information in this section for the /etc/llttab file. See the following information for sample configurations:

- See "Sample configuration: direct-attached links" on page 486.
- See "Sample configuration: links crossing IP routers" on page 487.

Note that some of the fields in Table K-1 differ from the command for standard LLT links.

Table K-1 describes the fields of the link command that are shown in the /etc/llttab file examples.

Table K-1 Field description for link command in /etc/llttab

Field	Description
tag-name	A unique string that is used as a tag by LLT; for example link1, link2,....
device	The device path of the UDP protocol; for example /dev/xti/udp6.
node-range	Nodes using the link. "-" indicates all cluster nodes are to be configured for this link.
link-type	Type of link; must be "udp6" for LLT over UDP.
udp-port	Unique UDP port in the range of 49152-65535 for the link. See "Selecting UDP ports" on page 485.
MTU	"-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the `lltstat -l` command to display the current value.
IPv6 address	IPv6 address of the link on the local node.
mcast-address	"-" is the default for clusters spanning routers.

The set-addr command in the /etc/llttab file

The `set-addr` command in the /etc/llttab file is required when the multicast feature of LLT is disabled, such as when LLT must cross IP routers.

See "Sample configuration: links crossing IP routers" on page 487.

Table K-2 describes the fields of the set-addr command.

Table K-2 Field description for set-addr command in /etc/llttab

Field	Description
node-id	The ID of the cluster node; for example, 0.
link tag-name	The string that LLT uses to identify the link; for example link1, link2,....
address	IPv6 address assigned to the link for the peer node.

Selecting UDP ports

When you select a UDP port, select an available 16-bit integer from the range that follows:

- Use available ports in the private range 49152 to 65535
- Do not use the following ports:
  - Ports from the range of well-known ports, 0 to 1023
  - Ports from the range of registered ports, 1024 to 49151

To check which ports are defined as defaults for a node, examine the file /etc/services. You should also use the `netstat` command to list the UDP ports currently in use. For example:

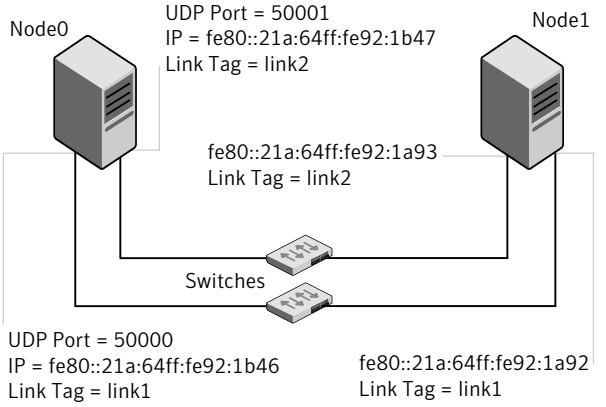
```
# netstat -a | more
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address   Foreign Address    (state)
tcp        0      0  *.32778         *.*                LISTEN
tcp        0      0  *.32781         *.*                LISTEN
udp4       0      0  *.daytime       *.*
udp4       0      0  *.time          *.*
udp4       0      0  *.sunrpc        *.*
udp        0      0  *.snmp          *.*
```

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the /etc/services file, its associated name is displayed rather than the port number in the output.

Sample configuration: direct-attached links

Figure K-1 depicts a typical configuration of direct-attached links employing LLT over UDP.

Figure K-1 A typical configuration of direct-attached links that use LLT over UDP



The configuration that the /etc/lltttab file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT uses IPv6 multicast requests for peer node address discovery. So the addresses of peer nodes do not need to be specified in the /etc/lltttab file using the `set-addr` command. Use the `ifconfig -a` command to verify that the IPv6 address is set correctly.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address mcast-address
link link1 /dev/xti/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -
link link1 /dev/xti/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -
```

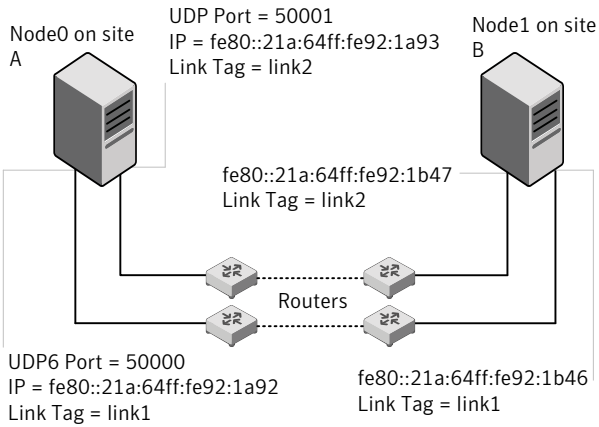
The file for Node 1 resembles:

```
set-node Node1
set-cluster 1
# configure Links
# link tag-name device node-range  link-type udp port MTU \
IP-address mcast-address
link link1 /dev/xti/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/xti/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -
```

Sample configuration: links crossing IP routers

Figure K-2 depicts a typical configuration of links crossing an IP router employing LLT over UDP. The illustration shows two nodes of a four-node cluster.

Figure K-2 A typical configuration of links crossing an IP router



The configuration that the following `/etc/lltab` file represents for Node 1 has links crossing IP routers. Notice that IPv6 addresses are shown for each link on each peer node. In this configuration multicasts are disabled.

```
set-node Node1
set-cluster 1

link link1 /dev/xti/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/xti/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 0 link1 fe80::21a:64ff:fe92:1b46
set-addr 0 link2 fe80::21a:64ff:fe92:1b47
```

```
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb     0
set-arp         0
```

The `/etc/llttab` file on Node 0 resembles:

```
set-node Node0
set-cluster 1

link link1 /dev/xti/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -
link link2 /dev/xti/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 1 link1 fe80::21a:64ff:fe92:1a92
set-addr 1 link2 fe80::21a:64ff:fe92:1a93
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb     0
set-arp         0
```

Appendix L

Configuring LLT over UDP using IPv4

This appendix includes the following topics:

Using the UDP layer for LLT

Veritas Storage Foundation Cluster File System 5.1 SP1 provides the option of using LLT over the UDP (User Datagram Protocol) layer for clusters using wide-area networks and routers. UDP makes LLT packets routable and thus able to span longer distances more economically.

When to use LLT over UDP

Use LLT over UDP in the following situations:

- LLT must be used over WANs
- When hardware, such as blade servers, do not support LLT over Ethernet

LLT over UDP is slower than LLT over Ethernet. Use LLT over UDP only when the hardware configuration makes it necessary.

Manually configuring LLT over UDP using IPv4

The following checklist is to configure LLT over UDP:

- Make sure that the LLT private links are on different physical networks.

If the LLT private links are not on different physical networks, then make sure that the links are on separate subnets. Set the broadcast address in `/etc/lltab` explicitly depending on the subnet for each link.
See "Broadcast address in the /etc/lltab file" on page 490.

- Make sure that each NIC has an IP address that is configured before configuring LLT.
- Make sure the IP addresses in the `/etc/lltab` files are consistent with the IP addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port.
See "Selecting UDP ports" on page 492.
- Set the broadcast address correctly for direct-attached (non-routed) links.
See "Sample configuration: direct-attached links" on page 494.
- For the links that cross an IP router, disable broadcast features and specify the IP address of each link manually in the `/etc/lltab` file.
See "Sample configuration: links crossing IP routers" on page 495.

Broadcast address in the /etc/lltab file

The broadcast address is set explicitly for each link in the following example.

- Display the content of the `/etc/lltab` file on the first node galaxy:

```
galaxy # cat /etc/lltab

set-node galaxy
set-cluster 1
link link1 /dev/xti/udp - udp 50000  -  192.168.9.1 192.168.9.255
link link2 /dev/xti/udp - udp 50001  -  192.168.10.1 192.168.10.255
```

Verify the subnet mask using the `ifconfig` command to ensure that the two links are on separate subnets.

- Display the content of the /etc/llttab file on the second node nebula:

```
nebula # cat /etc/lltab

set-node nebula
set-cluster 1
link link1 /dev/xti/udp - udp 50000  -  192.168.9.2 192.168.9.255
link link2 /dev/xti/udp - udp 50001  -  192.168.10.2 192.168.10.255
```

Verify the subnet mask using the `ifconfig` command to ensure that the two links are on separate subnets.

The link command in the /etc/lltab file

Review the link command information in this section for the `/etc/lltab` file. See the following information for sample configurations:

- See "Sample configuration: direct-attached links" on page 494.
- See "Sample configuration: links crossing IP routers" on page 495.

Table L-1 describes the fields of the link command that are shown in the `/etc/lltab` file examples. Note that some of the fields differ from the command for standard LLT links.

Table L-1 Field description for link command in /etc/lltab

Field	Description
tag-name	A unique string that is used as a tag by LLT; for example link1, link2,....
device	The device path of the UDP protocol; for example `/dev/xti/udp`.
node-range	Nodes using the link. "-" indicates all cluster nodes are to be configured for this link.
link-type	Type of link; must be "udp" for LLT over UDP.
udp-port	Unique UDP port in the range of 49152-65535 for the link. See "Selecting UDP ports" on page 492.
MTU	"-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the `lltstat -l` command to display the current value.
IP address	IP address of the link on the local node.
bcast-address	■ For clusters with enabled broadcasts, specify the value of the subnet broadcast address. ■ "-" is the default for clusters spanning routers.

The set-addr command in the /etc/lltab file

The `set-addr` command in the `/etc/lltab` file is required when the broadcast feature of LLT is disabled, such as when LLT must cross IP routers.

See "Sample configuration: links crossing IP routers" on page 495.

Table L-2 describes the fields of the set-addr command.

Table L-2 Field description for set-addr command in /etc/lltab

Field	Description
node-id	The ID of the cluster node; for example, 0.
link tag-name	The string that LLT uses to identify the link; for example link1, link2,....
address	IP address assigned to the link for the peer node.

Selecting UDP ports

When you select a UDP port, select an available 16-bit integer from the range that follows:

- Use available ports in the private range 49152 to 65535
- Do not use the following ports:
  - Ports from the range of well-known ports, 0 to 1023
  - Ports from the range of registered ports, 1024 to 49151

To check which ports are defined as defaults for a node, examine the file `/etc/services`. You should also use the `netstat` command to list the UDP ports currently in use. For example:

```
# netstat -a | more
UDP
   Local Address         Remote Address     State
--------------------  --------------------  ------
      *.*                                  Unbound
      *.32771                              Idle
      *.32776                              Idle
      *.32777                              Idle
      *.name                               Idle
      *.biff                               Idle
      *.talk                               Idle
      *.32779                              Idle
      .
      .
      .
      *.55098                               Idle
      *.syslog                              Idle
      *.58702                               Idle
      *.*                                   Unbound
```

```
# netstat -a |head -2;netstat -a | grep udp
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address Foreign Address (state)
udp4       0      0  *.daytime     *.*
udp4       0      0  *.time        *.*
udp4       0      0  *.sunrpc      *.*
udp4       0      0  *.snmp        *.*
udp4       0      0  *.syslog      *.*
```

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the `/etc/services` file, its associated name is displayed rather than the port number in the output.

Configuring the netmask for LLT

For nodes on different subnets, set the netmask so that the nodes can access the subnets in use. Run the following command and answer the prompt to set the netmask:

```
# ifconfig interface_name netmask netmask
```

For example:

- For the first network interface on the node galaxy:

  ```
  IP address=192.168.9.1, Broadcast address=192.168.9.255,
  Netmask=255.255.255.0
  ```

  For the first network interface on the node nebula:

  ```
  IP address=192.168.9.2, Broadcast address=192.168.9.255,
  Netmask=255.255.255.0
  ```

- For the second network interface on the node galaxy:

  ```
  IP address=192.168.10.1, Broadcast address=192.168.10.255,
  Netmask=255.255.255.0
  ```

  For the second network interface on the node nebula:

  ```
  IP address=192.168.10.2, Broadcast address=192.168.10.255,
  Netmask=255.255.255.0
  ```

Configuring the broadcast address for LLT

For nodes on different subnets, set the broadcast address in `/etc/lltab` depending on the subnet that the links are on.

An example of a typical `/etc/lltab` file when nodes are on different subnets. Note the explicitly set broadcast address for each link.

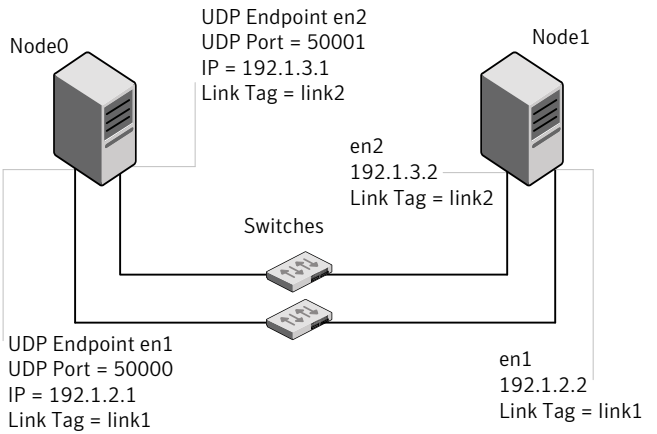
```
# cat /etc/lltab
set-node nodexyz
set-cluster 100

link link1 /dev/xti/udp - udp 50000 - 192.168.30.1
192.168.30.255
link link2 /dev/xti/udp - udp 50001 - 192.168.31.1
192.168.31.255
```

Sample configuration: direct-attached links

Figure L-1 depicts a typical configuration of direct-attached links employing LLT over UDP.

Figure L-1 A typical configuration of direct-attached links that use LLT over UDP



The configuration that the `/etc/lltab` file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT broadcasts requests peer nodes to discover their addresses. So the addresses of peer nodes do not need to be specified in the `/etc/lltab` file using the `set-addr`

command. For direct attached links, you do need to set the broadcast address of the links in the `/etc/lltab` file. Verify that the IP addresses and broadcast addresses are set correctly by using the `ifconfig -a` command.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/xti/udp - udp 50000 - 192.1.2.1 192.1.2.255
link link2 /dev/xti/udp - udp 50001 - 192.1.3.1 192.1.3.255
```

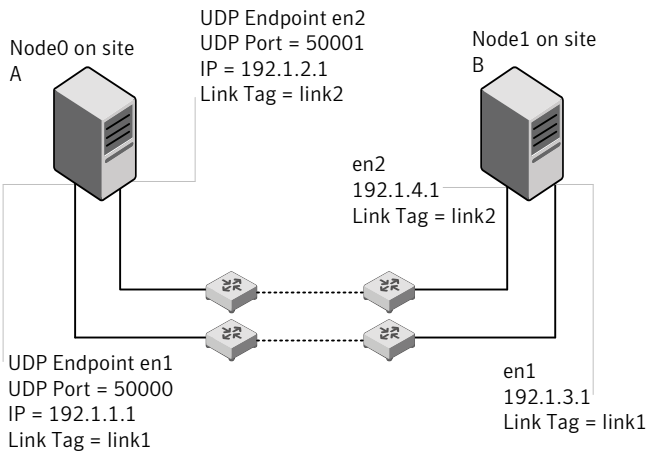
The file for Node 1 resembles:

```
set-node Node1
set-cluster 1
# configure Links
# link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/xti/udp - udp 50000 - 192.1.2.2 192.1.2.255
link link2 /dev/xti/udp - udp 50001 - 192.1.3.2 192.1.3.255
```

Sample configuration: links crossing IP routers

Figure L-2 depicts a typical configuration of links crossing an IP router employing LLT over UDP. The illustration shows two nodes of a four-node cluster.

Figure L-2 A typical configuration of links crossing an IP router



The configuration that the following `/etc/llttab` file represents for Node 1 has links crossing IP routers. Notice that IP addresses are shown for each link on each peer node. In this configuration broadcasts are disabled. Hence, the broadcast address does not need to be set in the `link` command of the `/etc/llttab` file.

```
set-node Node1
set-cluster 1
link link1 /dev/xti/udp - udp 50000 - 192.1.3.1 -
link link2 /dev/xti/udp - udp 50001 - 192.1.4.1 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr        0 link1 192.1.1.1
set-addr        0 link2 192.1.2.1
set-addr        2 link1 192.1.5.2
set-addr        2 link2 192.1.6.2
set-addr        3 link1 192.1.7.3
set-addr        3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb     0
set-arp         0
```

The `/etc/llttab` file on Node 0 resembles:

```
set-node Node0
set-cluster 1

link link1 /dev/xti/udp - udp 50000 - 192.1.1.1 -
link link2 /dev/xti/udp - udp 50001 - 192.1.2.1 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr        1 link1 192.1.3.1
set-addr        1 link2 192.1.4.1
set-addr        2 link1 192.1.5.2
set-addr        2 link2 192.1.6.2
set-addr        3 link1 192.1.7.3
set-addr        3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb     0
set-arp         0
```

Index

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W