

Veritas Storage Foundation™ and High Availability Installation Guide

HP-UX 11i v3

5.1 Service Pack 1



Veritas Storage Foundation™ and High Availability 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: 5.1SP1.0

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

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

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

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

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

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

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

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

Technical Support	4
Section 1 Installation overview and planning	19
Chapter 1 Introducing Storage Foundation and High Availability Solutions	21
About Veritas products	21
About Veritas Storage Foundation and Storage Foundation High Availability	21
About Veritas Cluster Server	22
About Veritas high availability agents	22
About Veritas Volume Replicator	22
About Veritas Storage Foundation Cluster File System	23
About Veritas Storage Foundation for Oracle® RAC by Symantec	23
About Veritas graphical user interfaces	23
Veritas Operations Manager	23
About Storage Foundation and High Availability features	24
About Symantec Product Authentication Service	24
About LLT and GAB	24
About configuring SFHA clusters for data integrity	25
About I/O fencing for SFHA in virtual machines that do not support SCSI-3 PR	26
About I/O fencing components	26
About global clusters	29
Chapter 2 Planning to install the Storage Foundation and High Availability products	31
About planning for SFHA installation	31
About installation and configuration methods	32
Downloading the Storage Foundation and High Availability software	32

Chapter 3	System requirements	35
	Release notes	35
	Hardware compatibility list (HCL)	36
	Veritas File System requirements	36
	Cluster environment requirements	36
	Supported HP-UX operating systems	37
	Disk space requirements	37
	Mandatory patch required for Oracle Bug 4130116	37
	Database requirements	38
	I/O fencing requirements	38
	Coordinator disk requirements for I/O fencing	38
	CP server requirements	39
	Non-SCSI3 I/O fencing requirements	42
	Number of nodes supported	42
Chapter 4	Licensing Veritas products	43
	About Veritas product licensing	43
	Setting or changing the product level for keyless licensing	44
	Installing Veritas product license keys	46
Section 2	Installation of Storage Foundation and High Availability products	47
Chapter 5	Preparing to install	49
	Installation preparation overview	49
	About configuring ssh or remsh using the Veritas installer	50
	Setting up shared storage	51
	Setting up shared storage: SCSI	51
	Checking and changing SCSI Initiator IDs	52
	Setting up shared storage: Fibre Channel	54
	Creating the /opt directory	55
	Prerequisites for IPv6 support	56
	Setting environment variables	56
	Mounting the product disc	57
	Assessing system preparedness	58
	Symantec Operations Readiness Tools	58
	Prechecking your systems using the Veritas installer	58

Chapter 6	Installing Storage Foundation and High Availability Solutions using the script-based installer	61
	About installing Veritas Storage Foundation on HP-UX	61
	Summary of Veritas Storage Foundation installation tasks	62
	About the Veritas installer	62
	Installing Storage Foundation using the installer	63
	Installing Storage Foundation and High Availability Solutions using the installer	66
Chapter 7	Installing Storage Foundation and High Availability Solutions using the Web-based installer	69
	About the Web-based installer	69
	Features not supported with Web-based installer	70
	Before using the Veritas Web-based installer	70
	Starting the Veritas Web-based installer	71
	Obtaining a security exception on Mozilla Firefox	71
	Performing a pre-installation check with the Veritas Web-based installer	72
	Installing SFHA with the Web-based installer	72
Section 3	Configuration of Storage Foundation and High Availability products	75
Chapter 8	Preparing to configure Storage Foundation and High Availability	77
	Preparing to configure the clusters in secure mode	77
	Installing the root broker for the security infrastructure	81
	Creating authentication broker accounts on root broker system	82
	Creating encrypted files for the security infrastructure	83
	Preparing the installation system for the security infrastructure	85
	About planning to configure I/O fencing	86
	Typical SFHA cluster configuration with server-based I/O fencing	89
	Recommended CP server configurations	90
	Setting up the CP server	93
	Planning your CP server setup	93
	Installing the CP server using the installer	94
	Configuring the CP server cluster in secure mode	95

	Setting up shared storage for the CP server database	96
	Configuring the CP server using the configuration utility	97
	Configuring the CP server manually	105
	Verifying the CP server configuration	107
Chapter 9	Configuring Storage Foundation	109
	Configuring Storage Foundation using the installer	109
	Configuring Storage Foundation manually	109
	Configuring Veritas Volume Manager	109
	Configuring Veritas File System	116
	Configuring your system after the installation	117
	Configuring the SFDB repository database after installation	117
Chapter 10	Configuring Storage Foundation and High Availability	119
	Configuring Storage Foundation and High Availability Solutions	119
	Required information for configuring Storage Foundation and High Availability Solutions	119
	Configuring Storage Foundation High Availability using the installer	120
	Configuring SFHA using the Web-based installer	140
	Configuring and starting Veritas Enterprise Administrator	146
Chapter 11	Configuring Storage Foundation High Availability for data integrity	149
	Setting up disk-based I/O fencing using installsfha	149
	Initializing disks as VxVM disks	149
	Checking shared disks for I/O fencing	150
	Configuring disk-based I/O fencing using installsfha	154
	Setting up disk-based I/O fencing manually	156
	Removing permissions for communication	157
	Identifying disks to use as coordinator disks	157
	Setting up coordinator disk groups	157
	Creating I/O fencing configuration files	158
	Modifying VCS configuration to use I/O fencing	159
	Verifying I/O fencing configuration	161
	Setting up server-based I/O fencing using installsfha	161
	Verifying the security configuration on the SFHA cluster to use CP server coordination point	162
	Configuring server-based I/O fencing using the installsfha	164
	Setting up non-SCSI3 server-based I/O fencing using installsfha	173

	Setting up server-based I/O fencing manually	173
	Preparing the CP servers manually for use by the SFHA cluster	173
	Configuring Coordination Point agent to monitor coordination points	177
	Verifying server-based I/O fencing configuration	179
	Setting up non-SCSI3 fencing in virtual environments manually	180
	Sample /etc/vxfenmode file for non-SCSI3 fencing	182
	Enabling or disabling the preferred fencing policy	184
Section 4	Upgrading Storage Foundation and High Availability products	187
Chapter 12	Preparing to upgrade	189
	About upgrading	189
	About the different ways that you can upgrade	190
	Supported upgrade paths	190
	About using the installer to upgrade when the root disk is encapsulated	192
	Tasks for upgrading the Storage Foundation for Databases (SFDB) tools	192
	Preparing to upgrade	192
	Preparing for an upgrade of Storage Foundation or Storage Foundation High Availability	193
	Creating backups	195
	Determining which 5.x release of Veritas File System and Veritas Volume Manager that you have installed	195
	Pre-upgrade tasks for migrating the SFDB repository database	197
	Preupgrade planning for Veritas Volume Replicator	197
	Preparing to upgrade VVR when VCS agents are configured	199
	Upgrading the array support	203
Chapter 13	Upgrading Storage Foundation or Storage Foundation and High Availability	205
	Upgrading Storage Foundation or Storage Foundation High Availability using the script-based installer	205
	Upgrading from Storage Foundation or Storage Foundation and High Availability 5.0_11iv3, 5.0.1, 5.0.1 RP1, or 5.0.1 RP2	206

	Upgrading from previous versions of Storage Foundation on HP-UX 11i v2	207
	Upgrading from Storage Foundation 3.5 on 11i v1 to Storage Foundation 5.1 SP1 on HP-UX 11i v3	209
	Upgrading from VxVM 5.0 on HP-UX 11i v3 to VxVM 5.1 SP1 using integrated VxVM 5.1 SP1 package for HP-UX 11i v3	210
	Upgrading from Storage Foundation High Availability from 5.0_11iv3, 5.0.1, or 5.0.1 RP1 on HP-UX 11i v3 to 5.1 SP1 on HP-UX 11i v3	210
	Upgrading from SFHA or SFORAHA 4.1, 4.1 MP1, 4.1 MP2, 5.0, 5.0 MP1, or 5.0 MP2 on HP-UX 11i v2 to SFHA 5.1 SP1 on HP-UX 11i v3	213
	Upgrading SFHA with the Veritas Web-based installer	217
	Upgrading the HP-UX operating system	218
	Upgrading Veritas Volume Replicator	219
	Upgrading VVR without disrupting replication	219
Chapter 14	Performing a phased upgrade	221
	About phased upgrade	221
	Prerequisites for a phased upgrade	221
	Planning for a phased upgrade	221
	Phased upgrade limitations	222
	Phased upgrade example	222
	Phased upgrade example overview	223
	Performing a phased upgrade	223
	Moving the service groups to the second subcluster	224
	Upgrading the operating system on the first subcluster	227
	Upgrading the first subcluster	227
	Preparing the second subcluster	229
	Activating the first subcluster	232
	Upgrading the operating system on the second subcluster	233
	Upgrading the second subcluster	233
	Finishing the phased upgrade	235
Chapter 15	Performing post-upgrade tasks	239
	Optional configuration steps	240
	Post upgrade tasks for migrating the SFDB repository database	240
	Migrating from a 5.0 repository database to 5.1 SP1	240
	Migrating from a 4.x repository database to 5.1 SP1	244
	Recovering VVR if automatic upgrade fails	247
	Post-upgrade tasks when VCS agents for VVR are configured	247

	Unfreezing the service groups	248
	Restoring the original configuration when VCS agents are configured	248
	Upgrading disk layout versions	250
	Upgrading the VxVM cluster protocol version	251
	Changing permissions for Storage Foundation for Databases	251
	Editing the snapplan after upgrading Veritas Storage Foundation for Oracle	252
	Migrating from /etc/vx/vxdba to /var/vx/vxdba for Oracle	253
	About upgrading disk layout versions	254
	Upgrading VxFS disk layout versions	254
	When to use vxfsconvert	255
	When to use vxupgrade	255
	Requirements for upgrading to disk layout Version 7	255
	Upgrading VxVM disk group versions	256
	Updating variables	256
	Setting the default disk group	256
	Configuring Powerfail Timeout after upgrade	257
	Converting from QuickLog to Multi-Volume support	258
	About enabling LDAP authentication for clusters that run in secure mode	259
	Enabling LDAP authentication for clusters that run in secure mode	261
	Verifying the Veritas Storage Foundation upgrade	267
Section 5	Verification of the installation or the upgrade	269
Chapter 16	Verifying the installation	271
	About using the postcheck option	271
	Performing a postcheck on a node	272
	Verifying that the products were installed	272
	Installation log files	273
	Using the installation log file	273
	Using the summary file	273
	Starting and stopping processes for the Veritas products	273
	Checking Veritas Volume Manager processes	274
	Checking Veritas File System installation	274
	Command installation verification	274
	Verifying the LLT, GAB, and VCS configuration files	274
	Verifying LLT, GAB, and cluster operation	275

	Verifying LLT	275
	Verifying the cluster	278
	Verifying the cluster nodes	278
Section 6	Adding and removing nodes	283
Chapter 17	Adding a node to a cluster	285
	About adding a node to a cluster	285
	Before adding a node to a cluster	286
	Meeting hardware and software requirements	286
	Setting up the hardware	286
	Preparing to add a node to a cluster	288
	Adding a node to a cluster	288
	Adding a node to a cluster using the SFHA installer	288
	Adding a node using the Web-based installer	292
	Adding the node to a cluster manually	293
	Configuring server-based fencing on the new node	299
	After adding the new node	301
	Updating the Storage Foundation for Databases (SFDB) repository after adding a node	302
Chapter 18	Removing a node from a cluster	303
	Removing a node from a cluster	303
	Verifying the status of nodes and service groups	304
	Deleting the departing node from SFHA configuration	305
	Modifying configuration files on each remaining node	308
	Removing the node configuration from the CP server	308
	Removing security credentials from the leaving node	309
	Unloading LLT and GAB and removing VCS on the departing node	310
Section 7	Uninstallation of Storage Foundation and High Availability products	311
Chapter 19	Uninstalling Storage Foundation and High Availability products	313
	Disabling VCS agents for VVR the agents on a system	313
	Removing the Replicated Data Set	314
	Uninstalling SFHA depots using the script-based installer	316
	Uninstalling SFHA with the Veritas Web-based installer	317

	Removing license files (Optional)	318
	Removing the CP server configuration using the removal script	319
	Removing the Storage Foundation for Databases (SFDB) repository after removing the product	322
	Stopping the AMF driver	323
Section 8	Installation reference	325
Appendix A	Installation scripts	327
	About installation scripts	327
	Installation script options	328
Appendix B	Response files	335
	About response files	335
	Installing Storage Foundation or Storage Foundation and High Availability using response files	336
	Configuring SFHA using response files	337
	Upgrading Storage Foundation or Storage Foundation and High Availability using response files	337
	Uninstalling Storage Foundation or Storage Foundation and High Availability using response files	338
	Syntax in the response file	338
	Response file variables to install, upgrade, or uninstall Storage Foundation or Storage Foundation and High Availability	339
	Response file variables to configure SFHA	342
	Sample response file for SFHA configuration	351
	Sample response file for SFHA install	351
	Sample response file for SF upgrade	352
	Sample response file for SFHA upgrade	352
Appendix C	Configuring I/O fencing using a response file	353
	Configuring I/O fencing using response files	353
	Response file variables to configure disk-based I/O fencing	354
	Sample response file for configuring disk-based I/O fencing	355
	Response file variables to configure server-based I/O fencing	356
	Sample response file for configuring server-based I/O fencing	358
	Sample response file for configuring non-SCSI3 server-based I/O fencing	359
	Response file variables to configure non-SCSI3 server-based I/O fencing	360

Appendix D	Configuration files	363
	About the LLT and GAB configuration files	363
	About the AMF configuration files	365
	About the VCS configuration files	366
	Sample main.cf file for VCS clusters	368
	Sample main.cf file for global clusters	370
	About I/O fencing configuration files	373
	Sample configuration files for CP server	375
	Sample main.cf file for CP server hosted on a single node that runs VCS	375
	Sample main.cf file for CP server hosted on a two-node SFHA cluster	378
Appendix E	Configuring the secure shell or the remote shell for communications	381
	About configuring secure shell or remote shell communication modes before installing products	381
	Configuring and enabling ssh	382
	Enabling remsh	386
Appendix F	Storage Foundation and High Availability components	387
	Storage Foundation and High Availability installation depots	387
	Veritas Cluster Server installation depots	389
	Veritas Storage Foundation obsolete and reorganized installation depots	390
Appendix G	Troubleshooting installation issues	393
	Restarting the installer after a failed connection	393
	What to do if you see a licensing reminder	393
	Incorrect permissions for root on remote system	394
	Resource temporarily unavailable	395
	Inaccessible system	396
	Upgrading Veritas Storage Foundation for Databases (SFDB) tools from 5.0MP2 to 5.1SP1 (2003131)	397
	Workaround	397
	Upgrading Veritas Storage Foundation for Databases (SFDB) tools from 5.0.x to 5.1SP1 (2184482)	397
	Workaround	398

Appendix H	Troubleshooting cluster installation	399
	Unmount failures	399
	Command failures	399
	Installer cannot create UUID for the cluster	400
	The vxfsentsthdw utility fails when SCSI TEST UNIT READY command fails	400
	Troubleshooting server-based I/O fencing	401
	Troubleshooting issues related to the CP server service group	401
	Checking the connectivity of CP server	402
	Troubleshooting server-based fencing on the SFHA cluster nodes	402
	Issues during fencing startup on SFHA cluster nodes set up for server-based fencing	403
	Issues during online migration of coordination points	405
	Troubleshooting server-based I/O fencing in mixed mode	406
	Checking keys on coordination points when vxfsen_mechanism value is set to cps	410
	After upgrading from 5.0.x and before migrating SFDB	411
Appendix I	Sample SFHA cluster setup diagrams for CP server-based I/O fencing	413
	Configuration diagrams for setting up server-based I/O fencing	413
	Two unique client clusters served by 3 CP servers	413
	Client cluster served by highly available CPS and 2 SCSI-3 disks	414
	Two node campus cluster served by remote CP server and 2 SCSI-3 disks	416
	Multiple client clusters served by highly available CP server and 2 SCSI-3 disks	418
Appendix J	Configuring LLT over UDP using IPv4	421
	Using the UDP layer for LLT	421
	When to use LLT over UDP	421
	Manually configuring LLT over UDP using IPv4	421
	Broadcast address in the /etc/llttab file	422
	The link command in the /etc/llttab file	423
	The set-addr command in the /etc/llttab file	424
	Selecting UDP ports	424
	Configuring the netmask for LLT	425
	Configuring the broadcast address for LLT	426

Sample configuration: direct-attached links	426
Sample configuration: links crossing IP routers	428
Index	431

Installation overview and planning

- [Chapter 1. Introducing Storage Foundation and High Availability Solutions](#)
- [Chapter 2. Planning to install the Storage Foundation and High Availability products](#)
- [Chapter 3. System requirements](#)
- [Chapter 4. Licensing Veritas products](#)

Introducing Storage Foundation and High Availability Solutions

This chapter includes the following topics:

- [About Veritas products](#)
- [About Veritas graphical user interfaces](#)
- [About Storage Foundation and High Availability features](#)

About Veritas products

The following products are available for this release.

About Veritas Storage Foundation and Storage Foundation High Availability

Veritas Storage Foundation by Symantec includes Veritas File System by Symantec (VxFS) and Veritas Volume Manager by Symantec (VxVM) with various feature levels.

Veritas File System is a high-performance, journaling file system that provides easy management and quick-recovery for applications. Veritas File System delivers scalable performance, continuous availability, increased I/O throughput, and structural integrity.

Veritas Volume Manager removes the physical limitations of disk storage. You can configure, share, manage, and optimize storage I/O performance online

without interrupting data availability. Veritas Volume Manager also provides easy-to-use, online storage management tools to reduce downtime.

You add high availability functionality to Storage Foundation HA by installing Veritas Cluster Server software.

VxFS and VxVM are a part of all Veritas Storage Foundation products. Do not install or update VxFS or VxVM as individual components.

Veritas Storage Foundation has the following products:

- Storage Foundation Standard
- Storage Foundation Standard HA
- Storage Foundation Enterprise
- Storage Foundation Enterprise HA

About Veritas Storage Foundation Basic

Storage Foundation Basic supports all Storage Foundation Standard features, but with deployment and technical support limitations.

About Veritas Cluster Server

Veritas Cluster Server by Symantec (VCS) is a clustering solution that provides the following benefits:

- Reduces application downtime
- Facilitates the consolidation and the failover of servers
- Manages a range of applications in heterogeneous environments

About Veritas high availability agents

Veritas agents provide high availability for specific resources and applications. Each agent manages resources of a particular type.

For example, the Oracle agent manages Oracle databases. Agents typically start, stop, and monitor resources and report state changes.

About Veritas Volume Replicator

Veritas Volume Replicator by Symantec is an optional, separately-licensable feature that is fully integrated with Veritas Volume Manager. This component replicates data to remote locations over any standard IP network to provide continuous data availability.

Volume Replicator is available with Veritas Storage Foundation Standard and Enterprise products.

About Veritas Storage Foundation Cluster File System

Veritas Storage Foundation Cluster File System by Symantec extends Veritas File System and Veritas Volume Manager to support shared data in a storage area network (SAN) environment. Using Storage Foundation Cluster File System, multiple servers can concurrently access shared storage and files transparently to applications.

Storage Foundation Cluster File System HA adds the failover functionality of Veritas Cluster Server. This functionality can protect everything from a single critical database instance to very large multiple-application clusters in networked environments. Veritas Storage Foundation Cluster File System also provides increased automation and intelligent management of availability and performance.

You can license Veritas Volume Replicator with this product.

About Veritas Storage Foundation for Oracle® RAC by Symantec

Veritas Storage Foundation for Oracle® RAC by Symantec is an integrated suite of Veritas storage management and high-availability software. The software is engineered to improve performance, availability, and manageability of Real Application Cluster (RAC) environments. Certified by Oracle Corporation, Veritas Storage Foundation for Oracle RAC delivers a flexible solution that makes it easy to deploy and manage RAC.

You can license Veritas Volume Replicator with this product.

About Veritas graphical user interfaces

The following are descriptions of Veritas GUIs.

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.

About Storage Foundation and High Availability features

The following describes different features in the Storage Foundation and High Availability product.

About Symantec Product Authentication Service

The Symantec Product Authentication Service protects communication channels among Symantec application clients and services through message integrity and confidentiality services.

About LLT and GAB

VCS uses two components, LLT and GAB, to share data over private networks among systems. These components provide the performance and reliability that VCS requires.

LLT (Low Latency Transport) provides fast, kernel-to-kernel communications, and monitors network connections.

GAB (Group Membership and Atomic Broadcast) provides the global message order that is required to maintain a synchronized state among the nodes. It monitors disk communications such as the VCS heartbeat utility.

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 SFHA clusters for data integrity

When a node fails, SFHA 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. SFHA 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 SFHA, you must configure I/O fencing in SFHA to ensure data integrity.

See [“About planning to configure I/O fencing”](#) on page 86.

About I/O fencing for SFHA 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, SFHA attempts to provide reasonable safety for the data disks. SFHA 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 installsfha”](#) on page 173.

See [“Setting up non-SCSI3 fencing in virtual environments manually”](#) on page 180.

About I/O fencing components

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

- Data disks—Store shared data
See [“About data disks”](#) on page 27.
- Coordination points—Act as a global lock during membership changes

See [“About coordination points”](#) on page 27.

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 disk groups. VxVM 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 SFHA configuration.

Dynamic Multi-pathing (DMP) allows coordinator disks to take advantage of the path failover and the dynamic adding and removal capabilities of DMP.

On cluster nodes with HP-UX 11i v3, you must use DMP devices or iSCSI devices for I/O fencing. The following changes in HP-UX 11i v3 require you to not use raw devices for I/O fencing:

■ Provides native multipathing support

■ Does not provide access to individual paths through the device file entries

The metanode interface that HP-UX provides does not meet the SCSI-3 PR requirements for the I/O fencing feature. You can configure coordinator disks to use Veritas Volume Manager Dynamic Multi-pathing (DMP) feature.

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 SFHA cluster nodes to perform the following tasks:

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

Multiple SFHA clusters running different operating systems can simultaneously access the CP server. TCP/IP based communication is used between the CP server and the SFHA 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 Cluster Server Administrator's Guide* for more details.

See [“Enabling or disabling the preferred fencing policy”](#) on page 184.

About global clusters

Global clusters provide the ability to fail over applications between geographically distributed clusters when disaster occurs. You require a separate license to configure global clusters. You must add this license during the installation. The installer only asks about configuring global clusters if you have used the global cluster license.

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

Planning to install the Storage Foundation and High Availability products

This chapter includes the following topics:

- [About planning for SFHA installation](#)
- [About installation and configuration methods](#)
- [Downloading the Storage Foundation and High Availability software](#)

About planning for SFHA 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: 5.1SP1.0.

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

Follow the preinstallation instructions if you are installing one of the Storage Foundation and High Availability products by Symantec.

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

- Veritas Storage Foundation Basic
- Veritas Storage Foundation (Standard and Enterprise Editions)
- Veritas Storage Foundation High Availability (HA) (Standard and Enterprise Editions)

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

About installation and configuration methods

You can install and configure SFHA with Veritas installation programs or with native operating system methods.

Use one of the following methods to install and configure SFHA:

- The Veritas product installer
The installer displays a menu that simplifies the selection of installation options.
- The product-specific installation scripts
The installation scripts provide a command-line interface to install a specific product. The product-specific scripts enable you to specify some additional command-line options. Otherwise, installing with the installation script is identical to specifying SFHA from the installer menu.
- The Web-based Veritas installer
The installer provides an interface to manage the installation from a remote site using a standard Web browser.
In this release, there are some limitations in the Web-based installer.
See [“About the Web-based installer”](#) on page 69.
- Silent installation with response files
You can use any of the above options to generate a response file. You can then customize the response file for another system. Run the product installation script with the response file to install silently on one or more other systems.
See [“About response files”](#) on page 335.

Downloading the Storage Foundation and High Availability software

One method of obtaining the Storage Foundation and High Availability 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 327.

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 37.

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

```
# df -b filesystem
```

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

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

System requirements

This chapter includes the following topics:

- [Release notes](#)
- [Hardware compatibility list \(HCL\)](#)
- [Veritas File System requirements](#)
- [Cluster environment requirements](#)
- [Supported HP-UX operating systems](#)
- [Disk space requirements](#)
- [Mandatory patch required for Oracle Bug 4130116](#)
- [Database requirements](#)
- [I/O fencing requirements](#)
- [Number of nodes supported](#)

Release notes

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

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

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

Hardware compatibility list (HCL)

The hardware compatibility list contains information about supported hardware and is updated regularly. Before installing or upgrading Storage Foundation and High Availability Solutions products, review the current compatibility list to confirm the compatibility of your hardware and software.

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

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

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

Veritas File System requirements

Complete the tasks in this section before installing Veritas File System.

Before installing Veritas File System, perform the following tasks:

- Review the *Veritas Storage Foundation Release Notes*.
- Ensure that the `/opt` directory exists and has write permissions for `root`.
- The Veritas File System does not support OmniStorage. Do not install VxFS without first retrieving any files archived using OmniStorage.
- Install all the latest required HP-UX patches.

Cluster environment requirements

If your configuration has a cluster, which is a set of hosts that share a set of disks, there are additional requirements.

To set up a cluster environment

- 1 If you plan to place the root disk group under VxVM control, decide into which disk group you want to configure it for each node in the cluster. The root disk group, usually aliased as `bootdg`, contains the volumes that are used to boot the system. VxVM sets `bootdg` to the appropriate disk group if it takes control of the root disk. Otherwise `bootdg` is set to `nodg`. To check the name of the disk group, enter the command:

```
# vxvg bootdg
```

- 2 Decide on the layout of shared disk groups. There may be one or more shared disk groups. Determine how many you wish to use.

- 3 If you plan to use Dirty Region Logging (DRL) with VxVM in a cluster, leave a small amount of space on the disk for these logs. The log size is proportional to the volume size and the number of nodes. Refer to the *Veritas Volume Manager Administrator's Guide* for more information on DRL.
- 4 Install the license that supports the clustering feature on every node in the cluster.

Supported HP-UX operating systems

This release of Veritas products can only be installed on a system running HP-UX B.11.31.1009, HP-UX 11i Version 3 September 2010 Operating Environments Update Release or later on the PA-RISC or Itanium platforms.

To verify the operating system version use the `swlist` command as follows:

```
# swlist | grep HPUX11i
HPUX11i-DC-OE      B.11.31.1009    HP-UX Data Center Operating Environment
```

JFS must be installed on your system prior to installing any Veritas software.

To verify that JFS is installed use the `swlist` command as follows:

```
# swlist -l product JFS
JFS                B.11.31        Base VxFS File System 4.1 for HP-UX
```

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
```

Mandatory patch required for Oracle Bug 4130116

If you are running Oracle versions 9.2.0.6 or 9.2.0.7, you must apply the Oracle patch for Oracle Bug 4130116. Contact Oracle to obtain this patch, and for details on how to apply it.

For more information, refer to the following TechNote:

<http://seer.entsupport.symantec.com/docs/333656.htm>

Database requirements

[Database requirements](#) identifies supported database and HP-UX combinations for Storage Foundation and High Availability.

Table 3-1 Supported database and HP-UX combinations

Oracle Release	HP-UX 11iv3 0903 OEUR or later
9.2	Yes
10.1	Yes
10.2	Yes
11gR1	Yes
11gR2	Yes

Oracle 11gR2 is supported in this release and following patches are mandatory for Oracle 11gR2 installation: PHSS_37042 PHSS_40546.

- PHCO_40381
- PHSS_37042
- PHSS_40546

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 38.
- CP servers
See [“CP server requirements”](#) on page 39.

If you have installed SFHA 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 42.

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 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

SFHA 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*.

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 3-2](#) lists additional requirements for hosting the CP server.

Table 3-2 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: <ul style="list-style-type: none"> ■ 550 MB in the /opt directory (additionally, the language pack requires another 15 MB) ■ 300 MB in /usr ■ 20 MB in /var
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 SFHA clusters (application clusters).

[Table 3-3](#) 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 3-3 CP server supported operating systems and versions

CP server	Operating system and version
CP server hosted on a VCS single-node cluster or on an SFHA cluster	<p>CP server supports any of the following operating systems:</p> <ul style="list-style-type: none"> ■ AIX 5.3 and 6.1 ■ HP-UX 11i v3 ■ Linux: <ul style="list-style-type: none"> ■ RHEL 5 ■ SLES 10 ■ SLES 11 ■ Solaris 9 and 10 <p>Review other details such as supported operating system levels and architecture for the supported operating systems.</p> <p>For other supported operating systems, see the <i>Veritas Cluster Server Installation Guide</i> or the <i>Veritas Storage Foundation High Availability Installation Guide</i> for that platform.</p>

Following are the CP server networking requirements and recommendations:

- Symantec recommends that network access from the application clusters to the CP servers should be made highly-available and redundant. The network connections require either a secure LAN or VPN.
- The CP server uses the TCP/IP protocol to connect to and communicate with the application clusters by these network paths. The CP server listens for messages from the application clusters using TCP port 14250. This is the default port that can be changed during a CP server configuration.
- 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 SFHA 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 Cluster Server Administrator's Guide*.

Non-SCSI3 I/O fencing requirements

Supported virtual environment for non-SCSI3 fencing:

- HP-UX Integrity Virtual Machines (IVM) Server 4.0 and 4.1

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:

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

Number of nodes supported

SFHA is capable of supporting cluster configurations with up to 64 nodes. Symantec has tested and qualified configurations of up to 32 nodes on IA-64 (Itanium) 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://www.symantec.com/docs/TECH144835>

Licensing Veritas products

This chapter includes the following topics:

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

About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

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

Within 60 days of choosing this option, you must install a valid license key corresponding to the license level entitled or continue with keyless licensing by managing the server or cluster with a management server. If you do not comply with the above terms, continuing to use the Veritas product is a violation of your end user license agreement, and results in warning messages. For more information about keyless licensing, see the following URL:
<http://go.symantec.com/sfhakeyless>

If you upgrade to this release from a prior release of the Veritas software, the product installer does not change the license keys that are already installed. The existing license keys may not activate new features in this release.

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
See “[Setting or changing the product level for keyless licensing](#)” on page 44.
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 46.
See the `vxlicinst (1m)` manual page.

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

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

Setting or changing the product level for keyless licensing

The keyless licensing method uses product levels to determine the Veritas products and functionality that are licensed. In order to use keyless licensing, you must set up a Management Server to manage your systems.

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

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

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

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

To set or change the product level

- 1 View the current setting for the product level.

```
# vxkeyless -v display
```

- 2 View the possible settings for the product level.

```
# vxkeyless displayall
```

- 3 Set the desired product level.

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

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

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

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

To clear the product license level

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

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

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

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

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

Installing Veritas product license keys

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

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

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

To install a new license

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

```
# cd /opt/VRTS/bin  
  
# ./vxlicinst -k xxxx-xxxx-xxxx-xxxx-xxxx-xxx
```

Installation of Storage Foundation and High Availability products

- [Chapter 5. Preparing to install](#)
- [Chapter 6. Installing Storage Foundation and High Availability Solutions using the script-based installer](#)
- [Chapter 7. Installing Storage Foundation and High Availability Solutions using the Web-based installer](#)

Preparing to install

This chapter includes the following topics:

- [Installation preparation overview](#)
- [About configuring ssh or remsh using the Veritas installer](#)
- [Setting up shared storage](#)
- [Creating the /opt directory](#)
- [Prerequisites for IPv6 support](#)
- [Setting environment variables](#)
- [Mounting the product disc](#)
- [Assessing system preparedness](#)

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 43.
Download the software, or insert the product DVD.	See “Downloading the Storage Foundation and High Availability software” on page 32. See “Mounting the product disc” on page 57.
Set environment variables.	See “Setting environment variables” on page 56.

Table 5-1 Installation overview (*continued*)

Installation task	Section
Create the /opt directory, if it does not exist.	See “Creating the /opt directory” on page 55.
Configure the secure shell (ssh) on all nodes.	See “About configuring secure shell or remote shell communication modes before installing products” on page 381.
Verify that hardware, software, and operating system requirements are met.	See “Supported HP-UX operating systems” on page 37. See “Release notes” on page 35.
Check that sufficient disk space is available.	See “Disk space requirements” on page 37.
Use the installer to install the products.	See “About the Veritas installer” on page 62.

About configuring ssh or remsh using the Veritas installer

The installer can configure passwordless secure shell (ssh) or remote shell (remsh) communications among systems. The installer uses the ssh or remsh 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. Note that for security reasons, the installation program neither stores nor caches these passwords. The ssh or remsh 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 remsh configuration from the systems.

See [“Installation script options”](#) on page 328.

In most installation, configuration, upgrade (where necessary), and uninstallation scenarios, the installer can configure ssh or remsh on the target systems. In the following scenarios, you need to set up ssh or remsh 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 381.

Setting up shared storage

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

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

See “[About planning to configure I/O fencing](#)” on page 86.

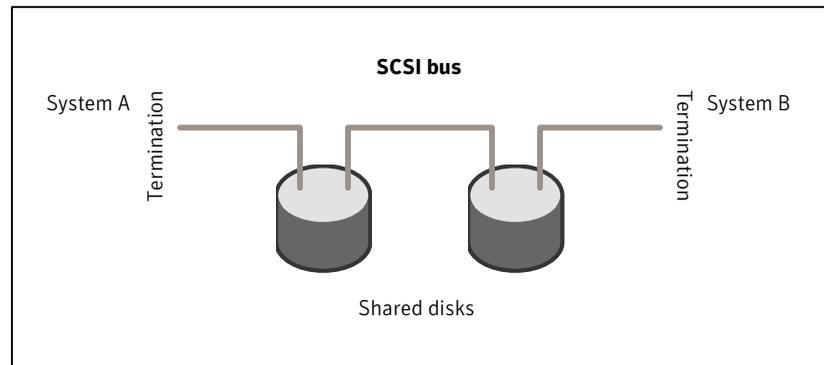
See also the *Veritas Cluster Server Administrator's Guide* for a description of I/O fencing.

Setting up shared storage: SCSI

Perform the following steps to set up shared storage.

[Figure 5-1](#) shows how to cable systems for shared storage.

Figure 5-1 Cabling the shared storage



To set up shared storage

- 1 Shut down the systems in the cluster.
- 2 Install the required SCSI host bus adapters and set up the external shared SCSI storage devices.
- 3 Cable the external shared storage devices. With cables connected to shared storage between two systems, you must terminate the two ends of the SCSI bus on the systems, as shown in the figure.

For more than two systems, disable SCSI termination on the systems that are not positioned at the ends of the SCSI chain.

Checking and changing SCSI Initiator IDs

The SCSI Initiator IDs for the host bus adapters (HBAs) on each of the systems that access the shared storage must be unique. So, you may have to change the HBA SCSI ID on one or more systems if these IDs are the same. Typically, the host bus adapters (HBAs) for the SCSI devices are shipped with a default SCSI ID of 7. Use the following procedure to check SCSI IDs and change them if necessary.

To check and change SCSI initiator IDs

- 1 For systems with PA architecture, turn on the power of the first system. During the boot process, the system delays for ten seconds, giving you the opportunity to stop the boot process and enter the boot menu:

To discontinue, press any key within 10 seconds.

Press any key. The boot process discontinues.

Boot terminated.

- 2 When you see the boot Main Menu, display the Information Menu by entering:

Main Menu: enter command or menu > **in**

- 3 From the Information Menu, enter "io" at the prompt for I/O interface information:

Information Menu: Enter command > **io**

The output shows information about the I/O interfaces and resembles:

Path	Bus	Slot	Vendor	Device	Id	Id
Description		(dec)	#	#		
-----		----	---	-----	-----	-----
.						
.						
SCSI bus cntlr		0/3/0/0	24	10	0x1000	0xf
.						

- 4 Return to the Main Menu:

Information Menu: Enter command > **main**

- 5 Go the Service Menu:

Main Menu: enter command or menu > **ser**

6 Display the host bus adapter's SCSI ID:

Service Menu: enter command or menu > **scsi**

The output displays information about the SCSI devices:

Path (dec)	Initiator ID	SCSI Rate	Auto Term
0/3/0/0	7	Fast	Unknown

The output in this example shows the SCSI ID is 7, the preset default for the HBA as shipped.

- If you choose, you can leave the ID set at 7 and return to the Main Menu:

Service Menu: enter command or menu > **main**

- You can change the SCSI ID for the HBA. For example, to change the SCSI ID from 7 to 6, you would enter:

Service Menu: Enter command > **SCSI init 0/3/0/0 6**
FAST

- To verify the change, enter "SCSI" at the prompt:

Service Menu: Enter command > **SCSI**

Path (dec)	Initiator ID	SCSI Rate	Auto Term
0/3/0/0	6	Fast	Unknown

7 Return to the Main Menu:

Service Menu: enter command or menu > **main**

8 At the Main Menu, enter the command to boot the system. Answer "n" when you are prompted to interact with IPL:

Menu: Enter command or menu > **boot**
 Interact with IPL (Y, N, or Cancel)?> **n**

Booting...

Setting up shared storage: Fibre Channel

Perform the following steps to set up Fibre Channel.

To set up Fibre Channel shared storage

- 1** Shut down the cluster systems that must share the devices.
- 2** Install the required Fibre Channel host bus adapters on each system.
- 3** Cable the shared devices.

- 4 Reboot each system.
- 5 Verify that each system can see all shared devices. Use the command:

```
# ioscan -fnC disk
```

Where "disk" is the class of devices to be shared. For example, from a system galaxy type:

```
galaxy# ioscan -fnC disk
Class I H/W Path Driver S/W State H/W Type Description
=====
.
.
disk 4 0/4/0/0.1.16.255.13.4.0 sdisk CLAIMED DEVICE
SEAGATE ST318304 CLAR18
/dev/dsk/c4t4d0 /dev/rdisk/c4t4d0
disk 5 0/4/0/0.1.16.255.13.5.0 sdisk CLAIMED DEVICE
SEAGATE ST318304 CLAR18
/dev/dsk/c4t5d0 /dev/rdisk/c4t5d0
.
.
```

And on another system, nebula, enter:

```
nebula# ioscan -fnC disk
Class I H/W Path Driver S/W State H/W Type Description
=====
.
.
disk 4 0/4/0/0.1.16.255.13.4.0 sdisk CLAIMED DEVICE
SEAGATE ST318304 CLAR18
/dev/dsk/c4t4d0 /dev/rdisk/c4t4d0
disk 5 0/4/0/0.1.16.255.13.5.0 sdisk CLAIMED DEVICE
SEAGATE ST318304 CLAR18
/dev/dsk/c4t5d0 /dev/rdisk/c4t5d0
.
.
```

Creating the /opt directory

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

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

Prerequisites for IPv6 support

Before you use IPv6, perform the following procedure.

To prepare to use IPv6

- 1 Ensure that `remsh` or `ssh` communications work.
- 2 Ensure that the IPv6 IP is up on the targeted system.
- 3 Ensure that `rpcd` is running with the IPv6 protocol (`ncacn_ipv6_tcp`).

The following steps are an example:

- Find and kill the `rpcd` daemon.

```
# ps -aef|grep rpcd|grep -v grep
root 2430      1  0 14:21:48 ?           0:00 /opt/dce/sbin/rpcd
# kill 2430
```

- Run `rpcd` with the IPv6 protocol as parameter.

```
# /opt/dce/sbin/rpcd ncacn_ipv6_tc
# echo $?
0
```

- 4 The `swlist`, `swagentd`, `swremove`, and `swreg` commands must be working with the IPv6 protocol. You must specify `"rpc_binding_info=ncacn_ipv6_tcp"` in the file `/var/adm/sw/defaults`.

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, SFHA commands are in `/opt/VRTS/bin`. SFHA 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
```

Mounting the product disc

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

To mount the product disc

- 1 Log in as superuser on a system where you want to install SFHA.
The system from which you install SFHA need not be part of the cluster. The systems must be in the same subnet.
- 2 Insert the product disc in the appropriate drive on your local system.
- 3 Determine the block device file for the DVD drive:

```
# ioscan -fnC disk
```

Make a note of the device file as it applies to your system.

- 4 Create a directory in which to mount the software disc and mount the disc using the appropriate drive name. For example:

```
# mkdir -p /dvdrom
# mount /dev/rdsk/c0t0d0 /dvdrom
```

- 5 Verify that the disc is mounted:

```
# mount
```

Assessing system preparedness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Storage Foundation 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 58.

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 Storage Foundation 5.1 SP1.

See [“Prechecking your systems using the Veritas installer”](#) on page 58.

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.

Installing Storage Foundation and High Availability Solutions using the script-based installer

This chapter includes the following topics:

- [About installing Veritas Storage Foundation on HP-UX](#)
- [Summary of Veritas Storage Foundation installation tasks](#)
- [About the Veritas installer](#)
- [Installing Storage Foundation using the installer](#)
- [Installing Storage Foundation and High Availability Solutions using the installer](#)

About installing Veritas Storage Foundation on HP-UX

This release of Veritas Storage Foundation requires HP-UX B.11.31.1009, HP-UX 11i Version 3 September 2010 Operating Environments Update Release or later. If you are not running this release of HP-UX, upgrade HP-UX on your system before you install the new Veritas software.

For an initial installation on a new system, you can use one of the installation procedures described in this section. If you have an existing installation of Storage Foundation that you are upgrading, you must perform an upgrade to move to the 5.1 SP1 versions of the Veritas products.

Summary of Veritas Storage Foundation installation tasks

Installation of Veritas Storage Foundation products consists of the following tasks:

- Obtain a license key, if required.
- If the operating system is not at the required OS fusion level, upgrade the operating system to the latest release.
The operating system is bundled with Veritas Volume Manager and Veritas File System. If the Veritas Volume Manager or Veritas File System is in use, follow the steps in the upgrade chapter to upgrade the Storage Foundation and the operating system.
- If patches for the operating system are required, install the patches before upgrading the product.
- Mount the disk.
- Install the 5.1 SP1 Veritas Storage Foundation product.
Start the installer and select 'I' for install, or run the appropriate installation script.
- Reboot the system.

```
# /usr/sbin/shutdown -r now
```
- Configure the Veritas software.
Start the installer and select 'C' for configure, or run the appropriate installation script with the `-configure` option.

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 327.

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 328.

Installing Storage Foundation using the installer

The Veritas product installer is the recommended method to license and install Storage Foundation.

This sample procedure is based on the installation of Storage Foundation on a single system.

To install Storage Foundation

- 1 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 381.
- 2 Load and mount the software disc. If you downloaded the software, navigate to the top level of the download directory and skip the next step.
[See “Mounting the product disc”](#) on page 57.
- 3 Move to the top-level directory on the disc.
- 4 From this directory, type the following command to install on the local system:

```
# ./installer
```

Use this command to install on remote systems if secure shell or remote shell communication modes are configured.
- 5 Enter `1` to install and press Return.
- 6 When the list of available products is displayed, select Storage Foundation, enter the corresponding number, and press Return.

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

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

- 8 Select from one of the following installation options:

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

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") where you want to install the software. Enter the system name or names and then press Return.

```
Enter the platform system names separated by spaces:
[q,?] host1
```

Where *platform* indicates the operating system.

- 10 After the system checks complete, the installer displays a list of the depots to be installed. Press Return to continue with the installation.
- 11 The installer can configure remote shell or secure shell communications for you among systems, however each system needs to have remote shell or secure shell servers installed. You also need to provide the superuser passwords for the systems. Note that for security reasons, the installation program neither stores nor caches these passwords.
- 12 The installer may prompt for previous Veritas Volume Manager configurations.

- 13** Choose the licensing method. Answer the licensing questions and follow the prompts.

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.

Note: If you are install Storage Foundation Basic, choose the first option to install the required license keys.

See “[About Veritas product licensing](#)” on page 43.

- 14** You are prompted to enter the Standard or Enterprise product mode.

- 1) SF Standard
- 2) SF Enterprise
- b) Back to previous menu

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

- 15** At the prompt, specify whether you want to send your installation information to Symantec.

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

- 16** The installation and configuration complete automatically. The product processes are started.

Check the log file, if needed, to confirm the installation and configuration.

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

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

Installing Storage Foundation and High Availability Solutions using the installer

The following sample procedure is based on the installation of a Storage Foundation Enterprise High Availability (SF/HA) cluster with two nodes: "host1" and "host2."

To install Storage Foundation and High Availability 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 381.

- 2 Load and mount the software disc. If you downloaded the software, navigate to the top level of the download directory and skip the next step.

See [“Mounting the product disc”](#) on page 57.

- 3 Move to the top-level directory on the disc.
- 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 or remote shell utilities are configured:

```
# ./installer
```

- 5 Enter **I** to install and press Return.
- 6 When the list of available products is displayed, select Storage Foundation High Availability, enter the corresponding number, and press Return.
- 7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA).

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

- 8 Select from one of the following install options:
 - Minimal depots: installs only the basic functionality for the selected product.
 - Recommended depots: installs the full feature set without optional depots.
 - All depots: installs all available depots.

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

For example, you should see output similar to the following:

- 1) Install minimal Storage Foundation HA depots -
694 MB required
- 2) Install recommended Storage Foundation HA depots -
1132 MB required
- 3) Install all Storage Foundation HA depots -
1132 MB required
- 4) Display depots to be installed for each option

Select the depots to be installed on all systems?

[1-4,q,?] (2) 2

- 9 You are prompted to enter the system names (in the following example, "host1" and "host2") where you want to install the software. Enter the system name or names and then press Return.

Enter the *platform* system names separated by spaces: [q,?] **host1 host2**

Where *platform* indicates the operating system.

- 10 The installer can configure remote shell or secure shell communications for you among systems, however each system needs to have secure shell or remote shell servers installed. You also need to provide the superuser passwords for the systems. Note that for security reasons, the installation program neither stores nor caches these passwords.
- 11 After the system checks complete, the installer displays a list of the depots that will be installed. Press Enter to continue with the installation.
- 12 Choose the licensing method. Answer the licensing questions and follow the prompts.

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.

See [“About Veritas product licensing”](#) on page 43.

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

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

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

- 15** If you are going to use the Global Cluster Option, enter **y** at the following prompt:

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

- 16** Review the output. You may need to reboot some systems before you can proceed. When you are ready to reboot the systems, run the following command for each system that the installer recommends:

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

- 17** You need to configure Veritas Storage Foundation High Availability before you can start it. When you are ready to configure, run the following command:

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

- 18** 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-****
```

Installing Storage Foundation and High Availability Solutions using the Web-based installer

This chapter includes the following topics:

- [About the Web-based installer](#)
- [Features not supported with Web-based installer](#)
- [Before using the Veritas Web-based installer](#)
- [Starting the Veritas Web-based installer](#)
- [Obtaining a security exception on Mozilla Firefox](#)
- [Performing a pre-installation check with the Veritas Web-based installer](#)
- [Installing SFHA with the Web-based installer](#)

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 `xprt1wid` 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/xprt1wid.conf`.

See [“Before using the Veritas Web-based installer”](#) on page 70.

See [“Starting the Veritas Web-based installer”](#) on page 71.

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 7-1 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 Storage Foundation 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 7-1 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: <ul style="list-style-type: none"> ■ Internet Explorer 6, 7, and 8 ■ Firefox 3.x

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 71.
- 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, click **Next**. The installer prompts you to begin the installation. Click **Yes** to install on the selected system. Click **No** to install later.
- 7 Click **Finish**. The installer prompts you for another task.

Installing SFHA with the Web-based installer

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

To install SFHA using the Web-based installer

- 1 Perform preliminary steps. See [“Performing a pre-installation check with the Veritas Web-based installer”](#) on page 72.
- 2 Start the Web-based installer.
See [“Starting the Veritas Web-based installer”](#) on page 71.
- 3 Select **Install a Product** from the **Task** drop-down list.

- 4 Select **SFHA** from the Product drop-down list, and click **Next**.
- 5 On the License agreement page, read the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.
- 6 Choose minimal, recommended, or all depots. Click **Next**.
- 7 Indicate the systems where you want to install. Separate multiple system names with spaces. Click **Validate**.
- 8 If you have not yet configured a communication mode among systems, you have the option to let the installer configure ssh or remsh. If you choose to allow this configuration, select the communication mode and provide the superuser passwords for the systems.
- 9 After the validation completes successfully, click **Next** to install SFHA on the selected system.
- 10 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 install Standard or Enterprise mode.
- 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**.

- 11** For Storage Foundation, click **Next** to complete the configuration and start the product processes.

Note that you are prompted to configure only if the product is not yet configured.

If you select **n**, you can exit the installer. You must configure the product before you can use SFHA.

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.

- 12** 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**.

Configuration of Storage Foundation and High Availability products

- [Chapter 8. Preparing to configure Storage Foundation and High Availability](#)
- [Chapter 9. Configuring Storage Foundation](#)
- [Chapter 10. Configuring Storage Foundation and High Availability](#)
- [Chapter 11. Configuring Storage Foundation High Availability for data integrity](#)

Preparing to configure Storage Foundation and High Availability

This chapter includes the following topics:

- [Preparing to configure the clusters in secure mode](#)
- [About planning to configure I/O fencing](#)
- [Setting up the CP server](#)

Preparing to configure the clusters in secure mode

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

In a cluster that is online, if you want to enable or disable AT using the `installsfha -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 81.

- 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 82.

- 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 remsh 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 remsh 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 remsh or ssh passwordless login.

[Figure 8-1](#) depicts the flow of configuring SFHA cluster in secure mode.

Figure 8-1 Workflow to configure SFHA cluster in secure mode

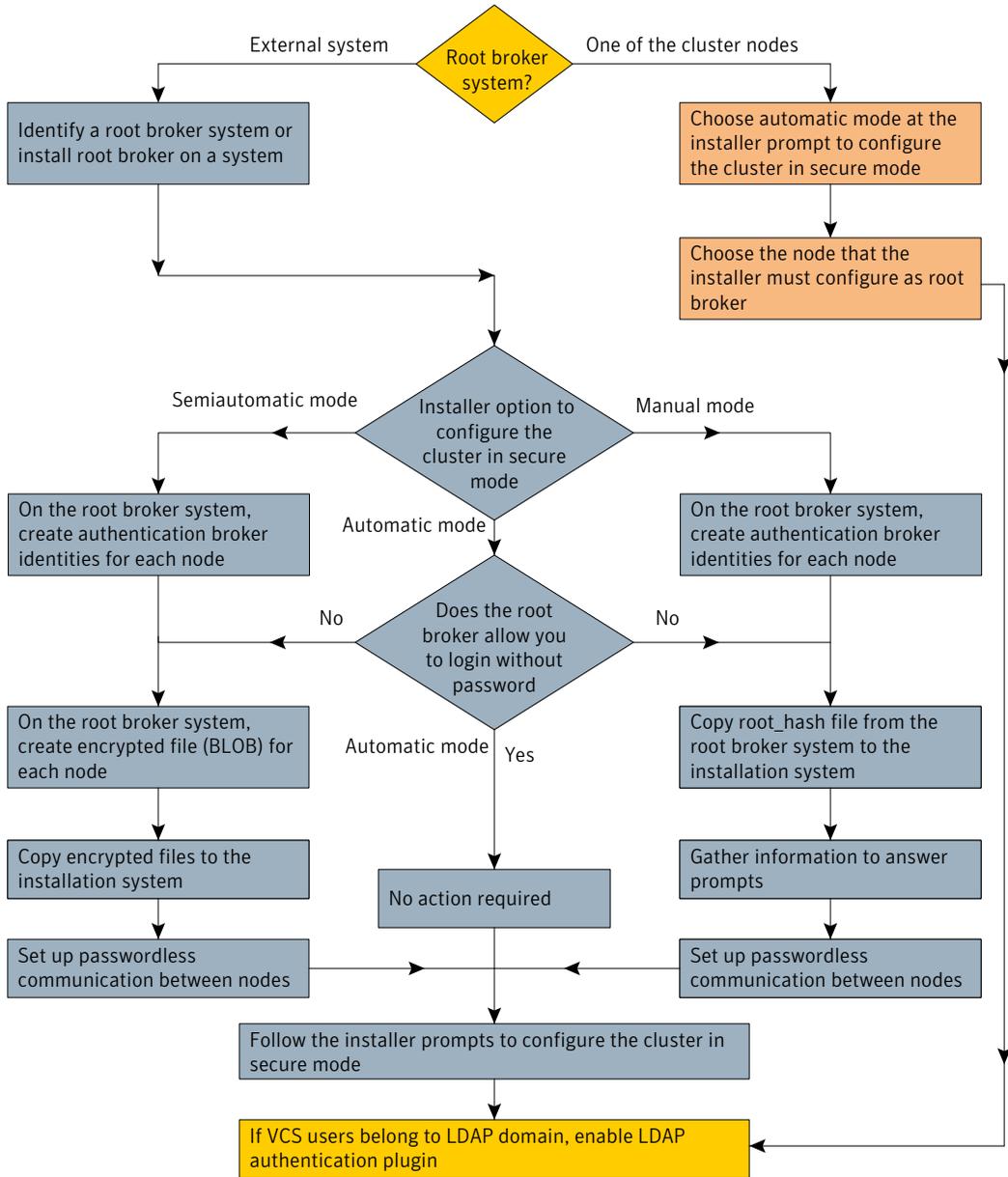


Table 8-1 lists the preparatory tasks in the order which the AT and VCS administrators must perform. These preparatory tasks apply only when you use an external root broker system for the cluster.

Table 8-1 Preparatory tasks to configure a cluster in secure mode (with an external root broker)

Tasks	Who performs this task
<p>Decide one of the following configuration modes to set up a cluster in secure mode:</p> <ul style="list-style-type: none"> ■ Automatic mode ■ Semi-automatic mode ■ Manual mode 	VCS administrator
<p>Install the root broker on a stable system in the enterprise.</p> <p>See “Installing the root broker for the security infrastructure” on page 81.</p>	AT administrator
<p>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.</p> <p>See “Creating authentication broker accounts on root broker system” on page 82.</p> <p>The AT administrator requires the following information from the VCS administrator:</p> <ul style="list-style-type: none"> ■ Node names that are designated to serve as authentication brokers ■ Password for each authentication broker 	AT administrator
<p>To use the semi-automatic mode, create the encrypted files (BLOB files) for each node and provide the files to the VCS administrator.</p> <p>See “Creating encrypted files for the security infrastructure” on page 83.</p> <p>The AT administrator requires the following additional information from the VCS administrator:</p> <ul style="list-style-type: none"> ■ Administrator password for each authentication broker Typically, the password is the same for all nodes. 	AT administrator
<p>To use the manual mode, provide the root_hash file (/opt/VRTSat/bin/root_hash) from the root broker system to the VCS administrator.</p>	AT administrator
<p>Copy the files that are required to configure a cluster in secure mode to the system from where you plan to install and configure SFHA.</p> <p>See “Preparing the installation system for the security infrastructure” on page 85.</p>	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 SFHA. 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 depots are already on the system.

The installer lists the depots 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 SFHA.

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	<p>The value for the authentication broker identity, which you provided to create authentication broker principal on the root broker system.</p> <p>This is the value for the <code>--prplname</code> option of the <code>addprpl</code> command.</p> <p>See “Creating authentication broker accounts on root broker system” on page 82.</p>
password	<p>The value for the authentication broker password, which you provided to create authentication broker principal on the root broker system.</p> <p>This is the value for the <code>--password</code> option of the <code>addprpl</code> command.</p> <p>See “Creating authentication broker accounts on root broker system” on page 82.</p>

- 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.symanteceexample.com
hash=758a33dbd6fae751630058ace3dedb54e562fe98
securitylevel=high

[configab]
identity=galaxy
password=password
root_domain=root@venus.symanteceexample.com
root_broker=venus.symanteceexample.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 SFHA configuration, choose the configuration option 1 when the installsfha 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 SFHA configuration, choose the configuration option 2 when the installsfha 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 SFHA configuration, choose the configuration option 3 when the installsfha prompts.

About planning to configure I/O fencing

After you configure SFHA 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 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 SFHA 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 88.

[Figure 8-2](#) illustrates a high-level flowchart to configure I/O fencing for the SFHA cluster.

Figure 8-2 Workflow to configure I/O fencing

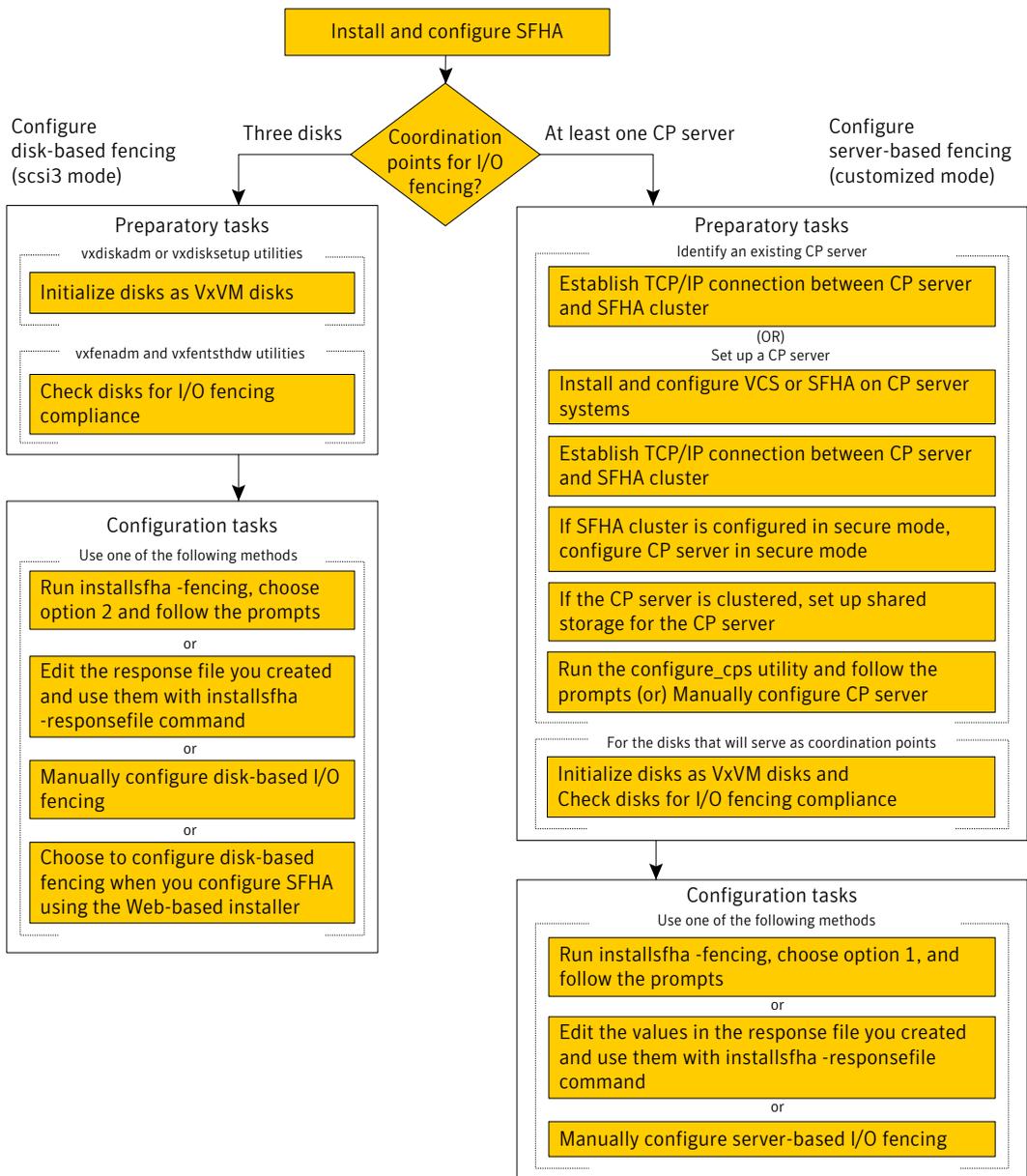
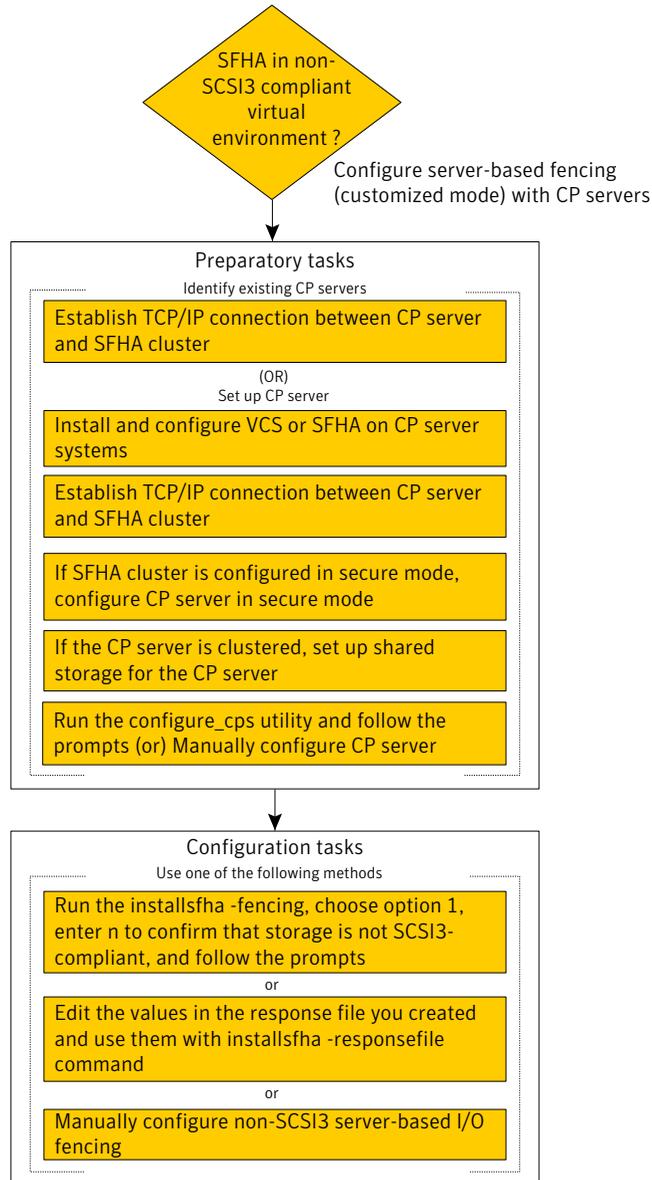


Figure 8-3 illustrates a high-level flowchart to configure non-SCSI3 server-based I/O fencing for the SFHA cluster in virtual environments that do not support SCSI-3 PR.

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



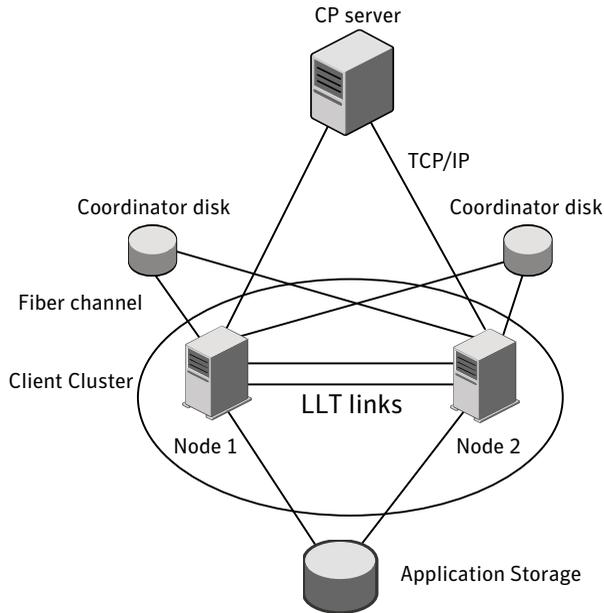
After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:

Using the installsfha	See “Setting up disk-based I/O fencing using installsfha” on page 149. See “Setting up server-based I/O fencing using installsfha” on page 161. See “Setting up non-SCSI3 server-based I/O fencing using installsfha” on page 173.
Using the Web-based installer	See “Configuring SFHA using the Web-based installer” on page 140. Note: The Web-based installer supports only the disk-based fencing configuration.
Using response files	See “Response file variables to configure disk-based I/O fencing” on page 354. See “Response file variables to configure server-based I/O fencing” on page 356. See “Response file variables to configure server-based I/O fencing” on page 356. See “Configuring I/O fencing using response files” on page 353.
Manually editing configuration files	See “Setting up disk-based I/O fencing manually” on page 156. See “Setting up server-based I/O fencing manually” on page 173. See “Setting up non-SCSI3 fencing in virtual environments manually” on page 180.

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

[Figure 8-4](#) displays a configuration using a SFHA cluster (with two nodes), a single CP server, and two coordinator disks. The nodes within the SFHA cluster are connected to and communicate with each other using LLT links.

Figure 8-4 CP server, SFHA 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 91.
- 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 92.
- 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 92.

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

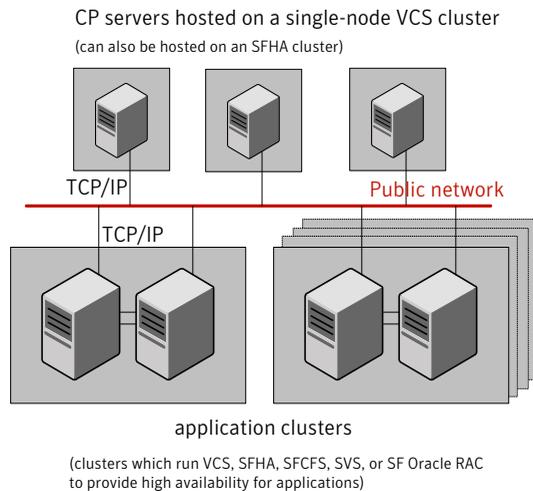


Figure 8-6 displays a configuration using a single CP server that is connected to multiple application clusters with each application cluster also using two coordinator disks.

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

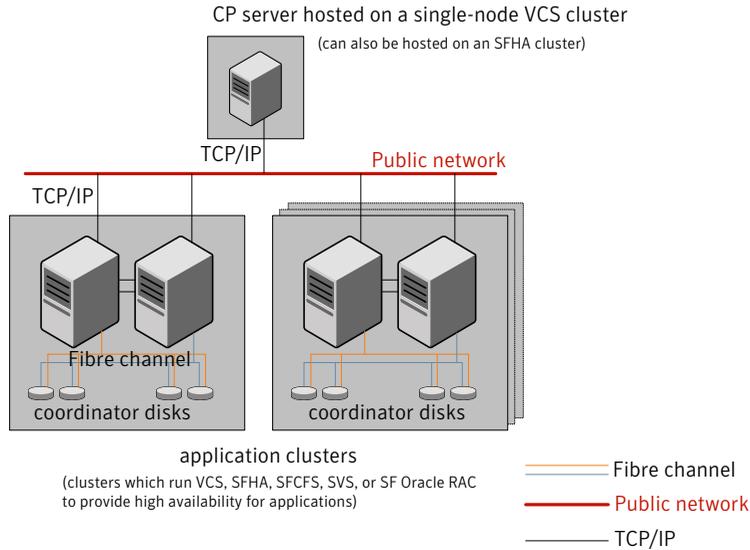
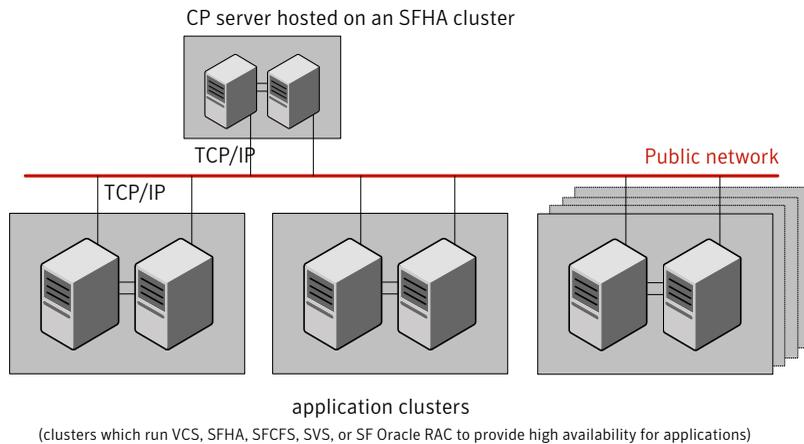


Figure 8-7 displays a configuration using a single CP server that is connected to multiple application clusters.

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



See "Configuration diagrams for setting up server-based I/O fencing" on page 413.

Setting up the CP server

[Table 8-2](#) lists the tasks to set up the CP server for server-based I/O fencing.

Table 8-2 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 93.
Install the CP server	See “Installing the CP server using the installer” on page 94.
Configure the CP server cluster in secure mode	See “Configuring the CP server cluster in secure mode” on page 95.
Set up shared storage for the CP server database	See “Setting up shared storage for the CP server database” on page 96.
Configure the CP server	See “Configuring the CP server using the configuration utility” on page 97. See “Configuring the CP server manually” on page 105.
Verify the CP server configuration	See “Verifying the CP server configuration” on page 107.

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 SFHA 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 (SFHA 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 39.
- 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 depots for installation. The VRTScps depot is installed only if you select to install all depots.
- 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 SFHA 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 97.

See “[Configuring the CP server manually](#)” on page 105.

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 depots for installation. The VRTScps depot is installed only if you select to install all depots.
- During configuration, set up the cluster in secure mode if you want secure communication between the CP server and the SFHA cluster (application cluster).
 See “[Preparing to configure the clusters in secure mode](#)” on page 77.
- During configuration, configure disk-based fencing (scsi3 mode).

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 SFHA 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:

```
# installsfha -security
```

See “[Preparing to configure the clusters in secure mode](#)” on page 77.

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/rdisk/cps_dg/cps_volume
```

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

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

```
Solaris # mkfs -F vxfs /dev/vx/rdisk/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 depot.

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 97.

For CP servers on an SFHA cluster: See [“To configure the CP server on an SFHA cluster”](#) on page 101.

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

- 1 Verify that the VRTScps depot 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 SFHA 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: lan0
```

- 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 lan0 on  
system mycps1? [y/n] : y  
Enter a valid IP address to configure NetworkHosts for NIC lan0 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 Cluster Server Administrator's Guide*.

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

See “[Sample configuration files for CP server](#)” on page 375.

To configure the CP server on an SFHA cluster

- 1** Verify that the VRTScps depot is installed on each node.
- 2** Make sure that you have configured passwordless ssh or remsh 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 remsh 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 SFHA 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 : lan0
```

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 lan0 on  
system mycps1? [y/n] : y  
Enter a valid IP address to configure NetworkHosts for NIC lan0 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 Cluster Server Administrator's Guide*.

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

See [“Sample configuration files for CP server”](#) on page 375.

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:

See “[Sample configuration files for CP server](#)” on page 375.

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

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

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

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

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

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

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

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

- 5 Start VCS on all the cluster nodes.

```
# hstart
```

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

```
# hagrps -state CPSSG
```

Output similar to the following appears:

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

Verifying the CP server configuration

Perform the following steps to verify the CP server configuration.

To verify the CP server configuration

- 1 Verify that the following configuration files are updated with the information you provided during the CP server configuration process:
 - `/etc/vxcps.conf` (CP server configuration file)
 - `/etc/VRTSvcs/conf/config/main.cf` (VCS configuration file)
 - `/etc/VRTSvcs/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.

Configuring Storage Foundation

This chapter includes the following topics:

- [Configuring Storage Foundation using the installer](#)
- [Configuring Storage Foundation manually](#)
- [Configuring your system after the installation](#)
- [Configuring the SFDB repository database after installation](#)

Configuring Storage Foundation using the installer

Storage Foundation does not require configuration. You need to start it.

To start Storage Foundation

- ◆ Run the installer command with the start option.

```
# ./installer -start
```

Configuring Storage Foundation manually

You can manually configure different components for Storage Foundation.

Configuring Veritas Volume Manager

Use the following procedures to configure Veritas Volume Manager. If you have installed and configured VxVM using the product installer, you do not need to complete the procedures in this section.

For information on setting up VxVM disk groups and volumes after installation, see "Configuring Veritas Volume Manager" in the *Veritas Volume Manager Administrator's Guide*.

Converting to a VxVM root disk

It is possible to select VxVM as a choice for your root disk when performing a new installation using Ignite-UX. Alternatively, you can use the following procedure to achieve VxVM rootability by cloning your LVM root disk using the `vxcp_lvmroot` command.

To convert to a VxVM root disk

- 1 Select the disk to be used as your new VxVM root disk. It is recommended that this disk is internal to the main computer cabinet. If this is currently an LVM disk, then it must be removed from LVM control as follows:
 - Use the `lvremove` command to remove any LVM volumes that are using the disk.
 - Use the `vgreduce` command to remove the disk from any LVM volume groups to which it belongs.
 - Use the `pvremove` command to erase the LVM disk headers

If the disk to be removed is the last disk in the volume group, use the `vgremove` command to remove the volume group, and then use `pvremove` to erase the LVM disk headers.

If the disk is not currently in use by any volume or volume group, but has been initialized by `pvcreate`, you must still use the `pvremove` command to remove LVM disk headers.

If you want to mirror the root disk across multiple disks, make sure that all the disks are free from LVM control.

- 2 While booted on the newly upgraded LVM root disk, invoke the `vxcp_lvmroot` command to clone the LVM root disk to the disk(s) you have designated to be the new VxVM root disks. In the following example, `c1t0d0` is used for the target VxVM root disk:

```
# /etc/vx/bin/vxcp_lvmroot -v c1t0d0
```

To additionally create a mirror of the root disk on `c2t0d0`:

```
# /etc/vx/bin/vxcp_lvmroot -v -m c2t0d0 c1t0d0
```

Use of the `-v` (verbose) option is highly recommended. The cloning of the root disk is a lengthy operation, and this option gives a time-stamped progress indication as each volume is copied, and other major events.

- 3 Use the `setboot (1M)` command to save the hardware path of the new VxVM root disk in the system NVRAM. The disk hardware paths can be found using this command:

```
# ioscan -kfnC disk
```

- 4 Reboot from the new VxVM root disk. If you created a mirrored root disk, then there is nothing more to do. The LVM root disk safely co-exists with your VxVM root disk, and provides a backup boot target.
- 5 If desired, you can convert the original LVM root disk into a mirror of your VxVM root disk by using the following commands:

```
# /etc/vx/bin/vxdestroy_lvmroot -v c2t0d0  
# /etc/vx/bin/vxrootmir -v c2t0d0
```

Once this operation is complete, the system is running on a completely mirrored VxVM root disk.

- 6 If later required, you can use the `vxres_lvmroot` command to restore the LVM root disk.

Starting and enabling the configuration daemon

The VxVM configuration daemon (`vxconfigd`) maintains VxVM disk and disk group configurations. The `vxconfigd` communicates configuration changes to the kernel and modifies configuration information stored on disk.

Startup scripts usually invoke `vxconfigd` at system boot time. The `vxconfigd` daemon must be running for VxVM to operate properly.

The following procedures describe how to check that `vxconfigd` is started, whether it is enabled or disabled, how to start it manually, or how to enable it as required.

To determine whether `vxconfigd` is enabled, use the following command:

```
# vxctl mode
```

The following message indicates that the `vxconfigd` daemon is running and enabled:

```
mode: enabled
```

This message indicates that `vxconfigd` is not running:

```
mode: not-running
```

This message indicates that `vxconfigd` is running, but not enabled:

```
mode: disabled
```

To start the `vxconfigd` daemon, enter the following command:

```
# vxconfigd
```

To enable the volume daemon, enter the following command:

```
# vxctl enable
```

Once started, `vxconfigd` automatically becomes a background process.

By default, `vxconfigd` writes error messages to the console. However, you can configure it to write errors to a log file. For more information, see the `vxconfigd(1M)` and `vxctl(1M)` manual pages.

Starting the volume I/O daemon

The volume I/O daemon (`vxiod`) provides extended I/O operations without blocking calling processes. Several `vxiod` daemons are usually started at system boot time after initial installation, and they should be running at all times. The procedure below describes how to verify that the `vxiod` daemons are running, and how to start them if necessary.

To verify that `vxiod` daemons are running, enter the following command:

```
# vxiod
```

The `vxiod` daemon is a kernel thread and is not visible using the `ps` command.

If, for example, 16 `vxiod` daemons are running, the following message displays:

```
16 volume I/O daemons running
```

where 16 is the number of `vxiod` daemons currently running. If no `vxiod` daemons are currently running, start some by entering this command:

```
# vxiod set no_of_daemons
```

where the number of daemons ranges from 1 to 16. Symantec recommends that at least one `vxiod` daemon should be run for each CPU in the system.

For more information, see the `vxiod(1M)` manual page.

Enabling optional cluster support in VxVM

This release includes an optional cluster feature that enables VxVM to be used in a cluster environment. The cluster functionality in VxVM allows multiple hosts to simultaneously access and manage a set of disks under VxVM control. A cluster is a set of hosts sharing a set of disks; each host is referred to as a node in the cluster.

The VxVM cluster feature requires a license, which can be obtained from your Customer Support channel.

To enable the cluster functionality in VxVM

- 1 Obtain a license for the VxVM cluster feature.
- 2 Install the software packages onto each system (node) to be included in the cluster.
- 3 Create the configuration files required to form a cluster.
- 4 Start the cluster services.
- 5 Configure shared disks.

See the *Veritas Volume Manager Administrator's Guide*.

Converting existing VxVM disk groups to shared disk groups

Use this procedure if you are upgrading from VxVM 3.x to VxVM 5.1 SP1 (or Storage Foundation 3.x to a Storage Foundation product at the 5.1 SP1 level) and you want to convert existing disk groups to shared disk groups.

If you want to convert existing private disk groups to shared disk groups, use the following procedure. Use these steps if you are moving from a single node to a cluster, or if you are already in a cluster and have existing private disk groups.

To convert existing disk groups to shared disk groups

- 1 Ensure that all systems that are running are part of the same cluster.
- 2 Start the cluster on all of the nodes on which you are converting the disk groups.
- 3 Configure the disk groups using the following procedure.

To list all disk groups, use the following command:

```
# vxdg list
```

To deport disk groups to be shared, use the following command:

```
# vxdg deport disk_group_name
```

To import disk groups to be shared, use the following command on the master node:

```
# vxdg -s import disk_group_name
```

This procedure marks the disks in the shared disk groups as shared and stamps them with the ID of the cluster, enabling other nodes to recognize the shared disks.

If dirty region logs exist, ensure they are active. If not, replace them with larger ones.

To display the shared flag for all the shared disk groups, use the following command:

```
# vxdg list
```

The disk groups are now ready to be shared.

- 4 If the cluster is only running with one node, bring up the other cluster nodes. Enter the `vxdg list` command on each node to display the shared disk groups. This command displays the same list of shared disk groups displayed earlier.

Configuring shared disks

This section describes how to configure shared disks. If you are installing VxVM for the first time or adding disks to an existing cluster, you need to configure new shared disks. If you are upgrading VxVM, verify that your shared disks still exist.

The shared disks should be configured from one node only. Since the VxVM software cannot tell whether a disk is shared or not, you must specify which are the shared disks.

Make sure that the shared disks are not being accessed from another node while you are performing the configuration. If you start the cluster on the node where you perform the configuration only, you can prevent disk accesses from other nodes because the quorum control reserves the disks for the single node.

Verifying existing shared disks

If you are upgrading from a previous release of VxVM, verify that your shared disk groups still exist.

To verify that your shared disk groups exist

- 1 Start the cluster on all nodes.
- 2 Enter the following command on all nodes:

```
# vxdg -s list
```

This displays the existing shared disk groups.

Upgrading in a clustered environment with FastResync set

Upgrading in a clustered environment with FastResync set requires additional steps.

This procedure applies to the following upgrade scenarios:

- Upgrading from VxVM 3.5 to VxVM 5.1 SP1
- Upgrading from VxVM 3.5 Maintenance Pack 4 to VxVM 5.1 SP1

If there are volumes in the shared disk groups with FastResync set (`fastresync=on`), before beginning the upgrade procedure, reattach each snapshot to its data volume, using this procedure:

To upgrade in a clustered environment when FastResync is set

- 1 You should run this procedure from the master node; to find out if you are on the master node, enter the command:

```
# vxdctl -c mode
```

- 2 On the master node, list which disk groups are shared by entering:

```
# vxdg -s list
```

- 3 Using the diskgroup names displayed by the previous command, list the disk groups that have volumes on which FastResync is set:

```
# vxprint -g diskgroup -F "%name" -e "_fastresync"
```

4 Reattach each snapshot:

```
# vxassist -g diskgroup -o nofmr snapback snapshot_volume
```

5 If you are upgrading from VxVM 3.5 Maintenance Patch 3 or from VxVM 3.2 Maintenance Patch 5, set FastResync to off for each volume:

```
# vxvol -g diskgroup set fastresync=off volume
```

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/fstab
```

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

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

vxtunefs command permissions and Cached Quick I/O

By default, you must have superuser (`root`) privileges to use the `/opt/VRTS/bin/vxtunefs` command. The `vxtunefs` command is a tool that lets you change caching policies to enable Cached Quick I/O and change other file system options. Database administrators can be granted permission to change default file system behavior in order to enable and disable Cached Quick I/O. The system administrator must change the `vxtunefs` executable permissions as follows:

```
# chown root:dba /opt/VRTS/bin/vxtunefs  
# chmod 4550 /opt/VRTS/bin/vxtunefs
```

Setting the permissions for `/opt/VRTS/bin/vxtunefs` to 4550 allows all users in the `dba` group to use the `vxtunefs` command to modify caching behavior for Quick I/O files.

For more information, see the *Veritas File System Administrator's Guide*.

Configuring your system after the installation

Use the following procedure to configure your system after installation.

To configure your system after the software upgrade

- 1 Reinstall the mount points in the `/etc/fstab` file that you recorded in the preparation steps.
- 2 Reboot the upgraded systems.
- 3 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

Optional configuration steps

Perform the following optional configuration steps:

- If you want to use Storage Foundation and High Availability for which you do not currently have an appropriate license installed, obtain the license and run the `vxlicinst` command to add it to your system.
 - Stop the cluster, restore the VCS configuration files to the `/etc/VRTSvcs/conf/config` directory, and restart the cluster.
 - To create root volumes that are under VxVM control after installation, use the `vxcp_lvmroot` command.
See [“Converting to a VxVM root disk”](#) on page 110.
See the *Veritas Volume Manager Administrator’s Guide*.
 - To upgrade VxFS Disk Layout versions and VxVM Disk Group versions, follow the upgrade instructions.
See [“Upgrading VxFS disk layout versions”](#) on page 254.
See [“Upgrading VxVM disk group versions”](#) on page 256.
- 4 After you complete the installation procedure, proceed to initializing (where required), setting up, and using Veritas Storage Foundation.

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 SFHA and Oracle. For SFDB repository set up procedures:

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

Configuring Storage Foundation and High Availability

This chapter includes the following topics:

- [Configuring Storage Foundation and High Availability Solutions](#)

Configuring Storage Foundation and High Availability Solutions

After installation, you must configure the product. To do this, run the Veritas product installer or the appropriate installation script using the `-configure` option.

Use the following procedures to configure Storage Foundation High Availability and clusters using the installer.

Required information for configuring Storage Foundation and High Availability Solutions

To configure Storage Foundation High Availability, the following information is required:

See also the *Veritas Cluster Server Installation Guide*.

- A unique Cluster name
- A unique Cluster ID number between 0-65535
- Two or more NIC cards per system used for heartbeat links

One or more heartbeat links are configured as private links and one heartbeat link may be configured as a low priority link.

You can configure Storage Foundation High Availability to use Symantec Security Services.

Running SFHA in Secure Mode guarantees that all inter-system communication is encrypted and that users are verified with security credentials. When running in Secure Mode, NIS and system usernames and passwords are used to verify identity. SFHA usernames and passwords are no longer used when a cluster is running in Secure Mode.

Before configuring a cluster to operate using Symantec Security Services, another system must already have Symantec Security Services installed and be operating as a Root Broker.

See the *Veritas Cluster Server Installation Guide* for more information on configuring a secure cluster.

The following information is required to configure SMTP notification:

- The domain-based hostname of the SMTP server
- The email address of each SMTP recipient
- A minimum severity level of messages to be sent to each recipient

The following information is required to configure SNMP notification:

- System names of SNMP consoles to receive VCS trap messages
- SNMP trap daemon port numbers for each console
- A minimum severity level of messages to be sent to each console

Configuring Storage Foundation High Availability using the installer

Storage Foundation HA configuration requires configuring the HA (VCS) cluster. Perform the following tasks to configure the cluster.

Overview of tasks to configure SFHA using the script-based installer

[Table 10-1](#) lists the tasks that are involved in configuring SFHA using the script-based installer.

Table 10-1 Tasks to configure SFHA using the script-based installer

Task	Reference
Start the software configuration	See “Starting the software configuration” on page 121.
Specify the systems where you want to configure SFHA	See “Specifying systems for configuration” on page 122.
Configure the basic cluster	See “Configuring the cluster name and ID” on page 123. See “Configuring private heartbeat links” on page 123.
Configure virtual IP address of the cluster (optional)	See “Configuring the virtual IP of the cluster” on page 126.
Configure the cluster in secure mode (optional)	See “Configuring the cluster in secure mode” on page 128.
Add VCS users (required if you did not configure the cluster in secure mode)	See “Adding VCS users” on page 132.
Configure SMTP email notification (optional)	See “Configuring SMTP email notification” on page 132.
Configure SNMP email notification (optional)	See “Configuring SNMP trap notification” on page 134.
Configure global clusters (optional) Note: You must have enabled Global Cluster Option when you installed SFHA.	See “Configuring global clusters” on page 136.
Complete the software configuration	See “Completing the VCS configuration” on page 137.

Starting the software configuration

You can configure SFHA using the Veritas product installer or the `installsfha`.

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

To configure SFHA 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 SFHA using the installsfha program

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

```
# /opt/VRTS/install/installsfha -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 SFHA. 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 SFHA.

```
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 SFHA is installed
 - Exits if Storage Foundation 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 86.

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 421.

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 lan5.)

```
Enter the NIC for the first private heartbeat link on galaxy:
[b,q,?] lan0
lan0 has an IP address configured on it. It could be a
public NIC on galaxy.
Are you sure you want to use lan0 for the first private
heartbeat link? [y,n,q,b,?] (n) y
Would you like to configure a second private heartbeat link?
[y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat link on galaxy:
[b,q,?] lan1
lan1 has an IP address configured on it. It could be a
public NIC on galaxy.
Are you sure you want to use lan1 for the second private
heartbeat link? [y,n,q,b,?] (n) y
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: lan5
```

```
Enter the NIC for Virtual IP of the Cluster to use on galaxy:
```

```
[b,q,?] (lan5)
```

- 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 *lan5* 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: *lan5*
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: lan5  
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 77.

To configure the cluster in secure mode

- 1 Choose whether to configure SFHA 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 132.

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 134.

- 3 Provide information to configure SMTP notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on galaxy: lan5
Enter the NIC for the VCS Notifier to use on galaxy:
[b,q,?] (lan5)
Is lan5 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: lan5
```

```
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
```

If you skip this option and if you had installed a valid HA/DR license, the installer presents you with an option to configure this cluster as global cluster. If you did not install an HA/DR license, the installer proceeds to configure SFHA based on the configuration details you provided.

See “[Configuring global clusters](#)” on page 136.

3 Provide information to configure SNMP trap notification.

Provide the following information:

■ **Enter the NIC information.**

```
Active NIC devices discovered on galaxy: lan5
Enter the NIC for the VCS Notifier to use on galaxy:
[b,q,?] (lan5)
Is lan5 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: lan5
```

```
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. If not, the installer proceeds to configure SFHA based on the configuration details you provided. You can also run the gcoconfig utility in each cluster later to update the VCS configuration file for 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 Cluster Server Administrator's Guide* for instructions to set up SFHA 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: lan5
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: lan5
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 SFHA 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 SFHA and its related processes.

If you chose to configure the cluster in secure mode, the installer then does the following before it starts SFHA 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 SFHA 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 SFHA 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 SFHA 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 SFHA using response files” on page 337.

Verifying and updating licenses on the system

After you install SFHA, 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 139.

See [“Updating product licenses using vxlicinst”](#) on page 139.

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.

```
License Key           = xxx-xxx-xxx-xxx-xxx
Product Name         = Storage Foundation and High Availability
Serial Number        = xxxxxx
License Type         = PERMANENT
OEM ID               = xxxxxx

Features :=
Platform            = HP-UX
Version             = 5.1 SP1
Tier                = 0
Reserved            = 0
Mode                = VCS
```

Updating product licenses using `vxlicinst`

You can use the `vxlicinst` command to add the SFHA license key on each node. If you have SFHA already installed and configured and you use a demo license, you can replace the demo license.

See [“Replacing a SFHA demo license with a permanent license”](#) on page 140.

To update product licenses

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

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

Replacing a SFHA demo license with a permanent license

When a SFHA 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 SFHA on all nodes in the cluster:

```
# hstop -all -force
```

This command does not shut down any running applications.

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

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

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

```
# vxlicrep
```

- 5 Start SFHA on each node:

```
# hstart
```

Configuring SFHA using the Web-based installer

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

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

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

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

You can click **Quit** to quit the Web-installer at any time during the configuration process.

To configure SFHA on a cluster

- 1 Start the Web-based installer.

See “[Starting the Veritas Web-based installer](#)” on page 71.

- 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 and High Availability

Click **Next**.

- 3 On the Select Systems page, enter the system names where you want to configure SFHA, 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 `installsfha -fencing` command or manually configure.

- 5 On the Set Cluster Name/ID page, specify the following information for the cluster.

Cluster Name	Enter a unique cluster name.
Cluster ID	Enter a unique cluster ID.
LLT Type	Select an LLT type from the list. You can choose to configure LLT over UDP or over Ethernet. If you choose Auto detect over Ethernet , the installer auto-detects the LLT links over Ethernet. Verify the links and click Yes in the Confirmation dialog box. Skip to step 7. If you click No, you must manually enter the details to configure LLT over Ethernet.
Number of Heartbeats	Choose the number of heartbeat links you want to configure.
Low Priority Heartbeat NIC	Select the check box if you want to configure a low priority link. The installer configures one heartbeat link as low priority link.
Unique Heartbeat NICs per system	For LLT over Ethernet, select the check box if you do not want to use the same NIC details to configure private heartbeat links on other systems. For LLT over UDP, this check box is selected by default.

Click **Next**.

- 6 On the Set Cluster Heartbeat page, select the heartbeat link details for the LLT type you chose on the Set Cluster Name/ID page.

For **LLT over Ethernet**: Do the following:

- If you are using the same NICs on all the systems, select the NIC for each private heartbeat link.
- If you had selected **Unique Heartbeat NICs per system** on the Set Cluster Name/ID page, provide the NIC details for each system.

For **LLT over UDP**: Select the NIC, Port, and IP address for each private heartbeat link. You must provide these details for each system.

Click **Next**.

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

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

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

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

Do not configure security services Choose this option if you do not want to enable security. The installer takes you to the next page to configure optional features of SFHA.

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. Enter the value for the networkhosts. 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 Cluster Server Administrator's Guide* for instructions to set up SFHA 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. Enter the value for the networkhosts. You can use an IPv4 or an IPv6 address.

Click **Next**.

- 10 On the Stop Processes page, click **Next** after the installer stops all the processes successfully.
- 11 On the Start Processes page, click **Next** after the installer performs the configuration based on the details you provided and starts all the processes successfully.

If you did not choose to configure I/O fencing in step 4, then skip to step 14. Go to step 12 to configure fencing.

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

- Configure disk based fencing** Choose the **Configure disk based fencing** option.
- Select a Disk Group** Select the **Create a new disk group** option or select one of the disk groups from the list.
 - If you selected one of the disk groups that is listed, the default fencing mechanism for the disk group is dmp. Go to step 14.
 - If you selected the **Create a new disk group** option, make sure you have SCSI-3 PR enabled disks, and click **Yes** in the confirmation dialog box. Click **Next**. Go to step 13.

- 13 On the Create New DG page, specify the following information:

- New Disk Group Name** Enter a name for the new coordinator disk group you want to create.
- Select Disks** Select at least three disks to create the coordinator disk group.
If you want to select more than three disks, make sure to select an odd number of disks.
- Fencing Mechanism** The default fencing mechanism for the disk group is dmp.

- 14 Click **Next** to complete the process of configuring SFHA.

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 and starting Veritas Enterprise Administrator

Before using the Veritas Enterprise Administrator server or client, start them both.

Optional configuration can also be completed at this time.

Activating, getting status, starting, and stopping the VEA server

After installing the VEA packages, the VEA server may need to be stopped and restarted. The VEA service is automatically started when you reboot your system.

To activate and start the VEA server

- 1 Activate the VEA server.

```
# /opt/VRTSob/bin/vxsvcctrl activate
```

- 2 Check the state of the VEA server.

```
# /opt/VRTSob/bin/vxsvcctrl status
```

- 3 Start the VEA server.

```
# /opt/VRTSob/bin/vxsvcctrl start
```

- 4 Stop the VEA server.

```
# /opt/VRTSob/bin/vxsvcctrl stop
```

You can also stop the VEA server manually by killing the `vxsvc` process.

The VEA server is automatically started on a reboot.

Starting the VEA client on Windows or HP-UX

Only users with appropriate privileges can run VEA. VEA can administer the local machine or a remote machine. However, VxVM and the VEA server must be installed on the machine to be administered. The VxVM `vxconfigd` daemon and the VEA server must be running on the machine to be administered.

After installing VxVM and VEA and starting the server, start the VEA client in one of the following ways.

HP-UX operating system

To administer the HP-UX machine, use the following command:

```
# /opt/VRTSob/bin/vea
```

Windows operating system

To administer a remote HP-UX machine from a Windows machine, select Start > Programs > Veritas > Veritas Enterprise Administrator.

Modifying optional connection access on HP-UX

To allow users other than root to access VEA, set up a group called `vrtsadm` in `/etc/group`, and add the users to this group. For example, adding the following entry:

```
vrtsadm::600:root,ed
```

will allow the two users, root and ed, to access VEA.

To specify a group other than `vrtsadm`, you should add the group to `/etc/group`, modify the Security key and restart the VEA server daemon, as in the following example.

To modify connection access

- 1 Add a new group:

```
# groupadd -g gid veagrp
```

- 2 Edit `/etc/group` to add users to the group.

- 3 Modify the Security key in the registry:

```
# /opt/VRTSob/bin/vxregctl /etc/vx/isis/Registry setvalue \  
Software/Veritas/VxSvc/Current/Version/Security AccessGroups \  
REG_SZ veagrp
```

- 4 Restart the VEA server.

```
# /opt/VRTS/bin/vxsvcctl restart
```


Configuring Storage Foundation High Availability for data integrity

This chapter includes the following topics:

- [Setting up disk-based I/O fencing using installsfha](#)
- [Setting up disk-based I/O fencing manually](#)
- [Setting up server-based I/O fencing using installsfha](#)
- [Setting up non-SCSI3 server-based I/O fencing using installsfha](#)
- [Setting up server-based I/O fencing manually](#)
- [Setting up non-SCSI3 fencing in virtual environments manually](#)
- [Enabling or disabling the preferred fencing policy](#)

Setting up disk-based I/O fencing using installsfha

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

Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

To initialize disks as VxVM disks

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

```
# ioscan -nfc disk
# insf -e
```

Warning: The HP-UX man page for the `insf` command instructs you to run the command in single-user mode only. You can run `insf -e` in multiuser mode only when no other user accesses any of the device files. This command can change the mode, owner, or group of an existing special (device) file, or unlink and recreate a file. The special files that are currently open may be left in an indeterminate state.

- 2 To initialize the disks as VxVM disks, use one of the following methods:
 - Use the interactive `vxdiskadm` utility to initialize the disks as VxVM disks. For more information see the *Veritas Volume Manager Administrator's Guide*.
 - Use the `vxdisksetup` command to initialize a disk as a VxVM disk.

```
vxdisksetup -i device_name
```

The example specifies the CDS format:

```
# vxdisksetup -i c2t13d0
```

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

Checking shared disks for I/O fencing

Make sure that the shared storage you set up while preparing to configure SFHA meets the I/O fencing requirements. You can test the shared disks using the `vxfststhdw` utility. The two nodes must have `ssh` (default) or `remsh` communication. To confirm whether a disk (or LUN) supports SCSI-3 persistent reservations, two nodes must simultaneously have access to the same disks. Because a shared disk is likely to have a different name on each node, check the serial number to verify the identity of the disk. Use the `vxfenadm` command with the `-i` option. This command option verifies that the same serial number for the LUN is returned on all paths to the LUN.

Make sure to test the disks that serve as coordinator disks.

The `vxfcntlsthdw` 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 Cluster Server 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 151.
- Verifying that nodes have access to the same disk
See [“Verifying that the nodes have access to the same disk”](#) on page 151.
- Testing the shared disks for SCSI-3
See [“Testing the disks using vxfcntlsthdw utility”](#) on page 152.

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.

```
# vxddladm listsupport all
```

- 3 Scan all disk drives and their attributes, update the VxVM device list, and reconfigure DMP with the new devices. Type:

```
# vxdisk scandisks
```

See the Veritas Volume Manager documentation for details on how to add and configure disks.

Verifying that the nodes have access to the same disk

Before you test the disks that you plan to use as shared data storage or as coordinator disks using the `vxfcntlsthdw` utility, you must verify that the systems see the same disk.

To verify that the nodes have access to the same disk

- 1 Verify the connection of the shared storage for data to two of the nodes on which you installed SFHA.
- 2 Ensure that both nodes are connected to the same disk during the testing. Use the `vxfenadm` command to verify the disk serial number.

```
vxfenadm -i diskpath
```

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

For example, an EMC disk is accessible by the `/dev/rdisk/c1t1d0` path on node A and the `/dev/rdisk/c2t1d0` path on node B.

From node A, enter:

```
vxfenadm -i /dev/rdisk/c1t1d0
```

```
Vendor id : EMC  
Product id : SYMMETRIX  
Revision : 5567  
Serial Number : 42031000a
```

The same serial number information should appear when you enter the equivalent command on node B using the `/dev/rdisk/c2t1d0` path.

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

```
# vxfenadm -i /dev/rdisk/c3t1d2
```

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

Testing the disks using `vxfentsthdw` utility

This procedure uses the `/dev/rdisk/c1t1d0` 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/rdisk/ctl1d0 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 Cluster Server Administrator's Guide*.

To test the disks using vxfcntl utility

- 1 Make sure system-to-system communication functions properly.
- 2 From one node, start the utility.

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

```
# vxfcntl [-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.
 If the serial numbers of the disks are not identical, then the test terminates.
- 5 Review the output as the utility performs the checks and report its activities.

- 6 If a disk is ready for I/O fencing on each node, the utility reports success for each node. For example, the utility displays the following message for the node galaxy.

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

```
ALL tests on the disk /dev/rdisk/clt1d0 have PASSED  
The disk is now ready to be configured for I/O Fencing on node galaxy
```

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

Configuring disk-based I/O fencing using installsfha

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

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

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

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

The installsfha 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 SFHA 5.1 SP1 is configured properly.

- 3 Review the I/O fencing configuration options that the program presents. Type **2** to configure disk-based I/O fencing.

```
Select the fencing mechanism to be configured in this  
Application Cluster [1-3,b,q] 2
```

- 4 Review the output as the configuration program checks whether VxVM is already started and is running.

- If the check fails, configure and enable VxVM before you repeat this procedure.
 - If the check passes, then the program prompts you for the coordinator disk group information.
- 5 Choose whether to use an existing disk group or create a new disk group to configure as the coordinator disk group.
- The program lists the available disk group names and provides an option to create a new disk group. Perform one of the following:
- To use an existing disk group, enter the number corresponding to the disk group at the prompt.
 The program verifies whether the disk group you chose has an odd number of disks and that the disk group has a minimum of three disks.
 - To create a new disk group, perform the following steps:
 - Enter the number corresponding to the **Create a new disk group** option.
 The program lists the available disks that are in the CDS disk format in the cluster and asks you to choose an odd number of disks with at least three disks to be used as coordinator disks.
 Symantec recommends that you use three disks as coordination points for disk-based I/O fencing.
 - Enter the numbers corresponding to the disks that you want to use as coordinator disks.
 - Enter the disk group name.
- 6 Verify that the coordinator disks you chose meet the I/O fencing requirements.
 You must verify that the disks are SCSI-3 PR compatible using the `vxfcntlshdw` utility and then return to this configuration program.
 See [“Checking shared disks for I/O fencing”](#) on page 150.
- 7 After you confirm the requirements, the program creates the coordinator disk group with the information you provided.
 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
- 8 Verify and confirm the I/O fencing configuration information that the installer summarizes.
- 9 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 SFHA is cleanly configured to use the I/O fencing feature.
- 10 Review the output as the configuration program displays the location of the log files, the summary files, and the response files.
- 11 Configure the Coordination Point agent to monitor the coordinator disks.
 See [“Configuring Coordination Point agent to monitor coordination points”](#) on page 177.

Setting up disk-based I/O fencing manually

[Table 11-1](#) lists the tasks that are involved in setting up I/O fencing.

Table 11-1 Tasks to set up I/O fencing manually

Task	Reference
Initializing disks as VxVM disks	See “Initializing disks as VxVM disks” on page 149.
Identifying disks to use as coordinator disks	See “Identifying disks to use as coordinator disks” on page 157.
Checking shared disks for I/O fencing	See “Checking shared disks for I/O fencing” on page 150.
Setting up coordinator disk groups	See “Setting up coordinator disk groups” on page 157.
Creating I/O fencing configuration files	See “Creating I/O fencing configuration files” on page 158.
Modifying SFHA configuration to use I/O fencing	See “Modifying VCS configuration to use I/O fencing” on page 159.
Configuring Coordination Point agent to monitor coordination points	See “Configuring Coordination Point agent to monitor coordination points” on page 177.

Table 11-1 Tasks to set up I/O fencing manually (*continued*)

Task	Reference
Verifying I/O fencing configuration	See “Verifying I/O fencing configuration” on page 161.

Removing permissions for communication

Make sure you completed the installation of SFHA and the verification of disk support for I/O fencing. If you used `remsh`, remove the temporary `remsh` access permissions that you set for the nodes and restore the connections to the public network.

If the nodes use `ssh` for secure communications, and you temporarily removed the connections to the public network, restore the connections.

Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See [“Initializing disks as VxVM disks”](#) on page 149.

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 150.

Setting up coordinator disk groups

From one node, create a disk group named `vxencoorddg`. This group must contain three disks or LUNs. You must also set the coordinator attribute for the coordinator disk group. VxVM uses this attribute to prevent the reassignment of coordinator disks to other disk groups.

Note that if you create a coordinator disk group as a regular disk group, you can turn on the coordinator attribute in Volume Manager.

Refer to the *Veritas 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 `c1t1d0`, `c2t1d0`, and `c3t1d0`.

To create the `vxfencoorddg` disk group

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

```
# vxdg init vxfencoorddg c1t1d0 c2t1d0 c3t1d0
```

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

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

- 3 Deport the coordinator disk group:

```
# vxdg deport vxfencoorddg
```

- 4 Import the disk group with the `-t` option to avoid automatically importing it when the nodes restart:

```
# vxdg -t import vxfencoorddg
```

- 5 Deport the disk group. Deporting the disk group prevents the coordinator disks from serving other purposes:

```
# vxdg deport vxfencoorddg
```

Creating I/O fencing configuration files

After you set up the coordinator disk group, you must do the following to configure I/O fencing:

- Create the I/O fencing configuration file `/etc/vxfendg`
- Update the I/O fencing configuration file `/etc/vxfenmode`

To update the I/O fencing files and start I/O fencing

- 1 On each nodes, type:

```
# echo "vxencoorddg" > /etc/vxfendg
```

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

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

- 2 Update the /etc/vxfenmode file to specify to use the SCSI-3 dmp disk policy. On all cluster nodes, type:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /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/rc.config.d/vxfenconf
```

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.

```
# /sbin/init.d/vxfen 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.

```
# /sbin/init.d/vxfen 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 installsfha

If SFHA 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 SFHA cluster to use CP server coordination point”](#) on page 162.

See [“Configuring server-based I/O fencing using the installsfha”](#) on page 164.

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

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

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

- 1** Run the following command:

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

The following is an example of the command output:

```
Domain(s) Found 1

*****

Domain Name HA_SERVICES@galaxy.symantec.com

Expiry Interval 0

*****
```

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

```
HA_SERVICES@hostname.domainname
```

or

```
HA_SERVICES@hostname
```

3 There should not be duplicate entries for HA_SERVICES domain.

The following is an example of an incorrect configuration:

```
showdomains

Domain(s) Found :          3

*****

Domain Name:      HA_SERVICES@galaxy.symantec.com

Domain Type:     vx

*****

Domain Name:      broker@galaxy.symantec.com

Domain Type:     vx

*****

Domain Name:      HA_SERVICES@galaxy

Domain Type:     vx

*****
```

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

Configuring server-based I/O fencing using the installsfha

You can configure server-based I/O fencing for the SFHA cluster using the installsfha.

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 86.

See [“Recommended CP server configurations”](#) on page 90.

This section covers the following example procedures:

Mix of CP servers and coordinator disks	See “To configure server-based fencing for the SFHA cluster (one CP server and two coordinator disks)” on page 165.
Single CP server	See “To configure server-based fencing for the SFHA cluster (single CP server)” on page 170.

To configure server-based fencing for the SFHA cluster (one CP server and two coordinator disks)

- Depending on the server-based configuration model in your setup, make sure of the following:
 - CP servers are configured and are reachable from the SFHA cluster. The SFHA cluster is also referred to as the application cluster or the client cluster.
See [“Setting up the CP server”](#) on page 93.
 - The coordination disks are verified for SCSI3-PR compliance.
See [“Checking shared disks for I/O fencing”](#) on page 150.

- Start the `installsfha` with `-fencing` option.

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

The `installsfha` 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.

- 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 SFHA 5.1 SP1 is configured properly.
- 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
```

- 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 SFHA (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) c1t1d0
- 2) c2t1d0
- 3) c3t1d0

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. c1t1d0
  2. c2t1d0
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 SFHA (application cluster) node.

- 10** If the CP server is configured for security, the installer sets up secure communication between the CP server and the SFHA (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 SFHA (application cluster) nodes have already established trust with an AT root broker.
- If the SFHA (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 SFHA (application cluster) nodes
 - Port number where the authentication broker for the SFHA (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 373.

- 13** Configure the CP agent on the SFHA (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 SFHA cluster (single CP server)

- 1 Make sure that the CP server is configured and is reachable from the SFHA cluster. The SFHA cluster is also referred to as the application cluster or the client cluster.

See “[Setting up the CP server](#)” on page 93.

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

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

The `installsfha` 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 SFHA 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 SFHA (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 SFHA (application cluster) nodes have already established trust with an AT root broker.
 - If the SFHA (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 SFHA (application cluster) nodes
 - Port number where the authentication broker for the SFHA (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 373.

12 Configure the CP agent on the SFHA (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 installsfha

If SFHA 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 SFHA cluster to use CP server coordination point”](#) on page 162.

Setting up server-based I/O fencing manually

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

Table 11-2 Tasks to set up server-based I/O fencing manually

Action	Description
Preparing the CP servers for use by the SFHA cluster	See “Preparing the CP servers manually for use by the SFHA cluster” on page 173.
Modifying I/O fencing configuration files to configure server-based I/O fencing	
Modifying SFHA configuration to use I/O fencing	See “Modifying VCS configuration to use I/O fencing” on page 159.
Configuring Coordination Point agent to monitor coordination points	See “Configuring Coordination Point agent to monitor coordination points” on page 177.
Verifying the server-based I/O fencing configuration	See “Verifying server-based I/O fencing configuration” on page 179.

Preparing the CP servers manually for use by the SFHA cluster

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

Table 11-3 displays the sample values used in this procedure.

Table 11-3 Sample values in procedure

CP server configuration component	Sample name
CP server	mycps1.symantecexample.com
Node #1 - SFHA cluster	galaxy
Node #2 - SFHA cluster	nebula
Cluster name	clus1
Cluster UUID	{f0735332-1dd1-11b2}

To manually configure CP servers for use by the SFHA cluster

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

For example, issue the following commands on one of the SFHA 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 SFHA 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 Cluster Server Administrator's Guide*.

3 Add the SFHA cluster and nodes to each CP server.

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

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

```
Cluster clus1 added successfully
```

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

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

```
Node 0 (galaxy) successfully added
```

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

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

```
Node 1 (nebula) successfully added
```

4 If security is to be enabled, check whether the `_HA_VCS_users` are created in the CP server.

If the output below does not show the users, then add them as described in the next step.

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

```
Username/Domain Type Cluster Name / UUID Role  
  
_HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com/vx  
clus1/{f0735332-1dd1-11b2} Operator  
  
_HA_VCS_nebula@HA_SERVICES@nebula.symantec.com/vx  
clus1/{f0735332-1dd1-11b2} Operator
```

If security is to be disabled, then add the user name "cpsclient@hostname" to the server instead of the `_HA_VCS_users` (for example, cpsclient@galaxy).

The CP server can only run in either secure mode or non-secure mode, both connections are not accepted at the same time.

5 Add the users to the CP server.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuring 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 SFHA 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
# hagr -add vxfen
# hagr -modify vxfen SystemList galaxy 0 nebula 1
# hagr -modify vxfen AutoFailOver 0
# hagr -modify vxfen Parallel 1
# hagr -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 SFHA 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 Cluster Server 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 173.

- 2 Make sure that the SFHA 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/vxenviro`n file as follows:

```
data_disk_fencing=off
```

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

```
# /usr/sbin/kctune 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:

```
/sbin/init.d/vcs stop
```

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

```
/sbin/init.d/vxfen stop
```

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

```
# /sbin/init.d/vxfen start  
# /sbin/init.d/vcs 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 with
# the coordination disks. This field is required only if customized
# coordinator disks are being used.
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
# scsi3_disk_policy=dmp

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

#
# Seconds for which vxfsend process wait for a customized fencing
# script to complete. Only used with vxfsen_mode=customized
vxfsen_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 28.

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:

```
# hagr -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
```

Upgrading Storage Foundation and High Availability products

- [Chapter 12. Preparing to upgrade](#)
- [Chapter 13. Upgrading Storage Foundation or Storage Foundation and High Availability](#)
- [Chapter 14. Performing a phased upgrade](#)
- [Chapter 15. Performing post-upgrade tasks](#)

Preparing to upgrade

This chapter includes the following topics:

- [About upgrading](#)
- [About the different ways that you can upgrade](#)
- [Supported upgrade paths](#)
- [About using the installer to upgrade when the root disk is encapsulated](#)
- [Tasks for upgrading the Storage Foundation for Databases \(SFDB\) tools](#)
- [Preparing to upgrade](#)

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 190.

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

See [“Supported upgrade paths”](#) on page 190.

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 12-1 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
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

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 12-2 HP-UX upgrades using the script- or Web-based installer

Veritas software versions	11.11	11.23	11.31
3.5 (SF/SFCFS)	Upgrade OS to 11.23, upgrade OS to 11.31, then upgrade directly to 5.1SP1 using the installer script (SFCFS requires additional manual changes as mentioned in IG)	N/A	N/A
3.5 (VCS/DBEDs/VVR/SFRAC)	Upgrade OS to 11.23, upgrade to 4.1, upgrade OS to 11.31, then upgrade directly to 5.1SP1 using the installer script	N/A	N/A
3.5_11iv2	N/A	Upgrade to 4.1, upgrade OS to 11.31, then upgrade directly to 5.1SP1 using the installer script	N/A
4.1 4.1 MP1 4.1 MP2 5.0 5.0 MP1 5.0 MP2	N/A	Upgrade OS to 11.31, then upgrade directly to 5.1SP1 using the installer script	N/A
5.0_11iv3 5.0.1 5.0.1 RP1	N/A	N/A	Upgrade directly to 5.1SP1 using the installer script

About using the installer to upgrade when the root disk is encapsulated

When you use the installer to upgrade from a previous version of SFHA and the system where you plan to upgrade has an encapsulated root disk, you may have to unencapsulate it.

Table 12-3 Upgrading using installer when the root disk is encapsulated

Starting version	Ending version	Action required
4.x or 4.x MPx	5.1 SP1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
5.0 or 5.0 MPx or 5.0.1 or 5.0.1 RPx	5.1 SP1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.

Tasks for upgrading the Storage Foundation for Databases (SFDB) tools

Tasks for upgrading SFDB tools to version 5.1 SP1:

- Preparing to migrate the repository database before upgrading from 5.0.x or earlier to 5.1 SP1
See [“Pre-upgrade tasks for migrating the SFDB repository database”](#) on page 197.
- Migrating the repository database after upgrading from 5.0.x or earlier to 5.1 SP1
See [“Post upgrade tasks for migrating the SFDB repository database”](#) on page 240.

Caution: If you are running Oracle version 11.1.0.6 and upgrading a Storage Foundation product to 5.1 SP1, upgrade the Oracle binaries and database to version 11.1.0.7 before moving to SP1.

Preparing to upgrade

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

Preparing for an upgrade of Storage Foundation or Storage Foundation High Availability

Ensure that you have made backups of all data that you want to preserve. In particular, you will need the information in files such as `/etc/fstab`. You should also run the `vxlicrep`, `vxdisk list`, and `vxprint -ht` commands, and record the output from these. You may need this information to reconfigure your system after the upgrade.

If you are upgrading an HA cluster, follow the guidelines given in the *Veritas Cluster Server (VCS) Installation Guide* for information on preserving your VCS configuration across the upgrade procedure. In particular, you should take care to make backups of configuration files, such as `main.cf` and `types.cf`, in the `/etc/VRTSvcs/conf/config` directory. Additional configuration files, such as `OracleTypes.cf`, may also be present in this directory if you have installed any VCS agents. You should also back up these files.

To prepare for the Veritas software upgrade

- 1 Log in as superuser.
- 2 Perform any necessary preinstallation checks and configuration.
See [“About planning for SFHA installation”](#) on page 31.
- 3 Use the `vxlicrep` command to make a record of the currently installed Veritas licenses. Print the output or save it on a different system.
- 4 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes.
- 5 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
```

- 6 Use the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# df -F vxfs
```

- 7 Unmount all Storage Checkpoints and non-system VxFS file systems:

```
# umount /checkpoint_name
# umount /filesystem
```

- 8 Verify that all file systems have been cleanly unmounted:

```
# echo "8192B.p S" | fsdb -F vxfs filesystem | grep clean
flags 0 mod 0 clean clean_value
```

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

- 9 (Optional) If a file system is not clean, enter the following commands for that file system:

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

This should complete any extended operations that were outstanding on the file system and unmount the file system cleanly.

There may be a pending large fileset clone removal extended operation if the `umount` command fails with the following error:

```
file system device busy
```

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

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

- 10 (Optional) If an extended operation is pending, 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.
- 11 (Optional) Repeat step 7 to verify that the unclean file system is now clean.
- 12 Stop all the volumes by entering the following command for each disk group:

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

To verify that no volumes remain open, use the following command:

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

- 13 Comment out the non-system local VxFS mount points from the `/etc/fstab`. Make a record of the mount points for VxFS file systems and VxVM volumes that are defined in the `/etc/fstab` file. You will need to uncomment these entries in the `/etc/fstab` file on the upgraded system.
- 14 If Veritas Volume Replicator (VVR) is configured, do the following steps in the order shown:
 - Verify that all of the Primary RLINKs are up to date:

```
# vxrlink -g diskgroup status rlink_name
```
 - Detach the RLINKs.
 - Disassociate the SRL.

Creating backups

Save relevant system information before the upgrade.

To create backups

- 1 Log in as superuser.
- 2 Before the upgrade, ensure that you have made backups of all data that you want to preserve.
- 3 Copy the `fstab` file to `fstab.orig`:

```
# cp /etc/fstab /etc/fstab.orig
```
- 4 Run the `vxlicrep`, `vxdisk list`, and `vxprint -ht` commands and record the output. Use this information to reconfigure your system after the upgrade.
- 5 If you are installing the high availability version of the Veritas Storage Foundation 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.

Determining which 5.x release of Veritas File System and Veritas Volume Manager that you have installed

If you are upgrading to this release and have a previously-installed release of Veritas File System (VxFS) and Veritas Volume Manager (VxVM), you must determine which release you have installed. Determining which 5.x release that you have installed can be difficult due to the binary path names being the same

for both releases. Use the following procedures to determine which release you have installed.

To determine which release of VxFS that you have installed

- ◆ To determine which release of VxFS that you have installed, enter the following command:

```
# swlist -l product VRTSvxfs
```

If you have the 5.0 release installed, the command output includes the following information:

```
VRTSvxfs          5.0.31.0          VERITAS File System
```

If you have the 5.0.1 release installed, the command output includes the following information:

```
VRTSvxfs          5.0.31.5          VERITAS File System
```

If you have the 5.1 SP1 release installed, the command output includes the following information:

```
VRTSvxfs          5.1.100.000      VERITAS File System
```

To determine which release of VxVM that you have installed

- ◆ To determine which release of VxVM that you have installed, enter the following command:

```
# swlist -l product VRTSvxvm
```

If you have the 5.0 release installed, the command output includes the following information:

```
VRTSvxvm          5.0.31.1          Veritas Volume Manager by Symantec
```

If you have the 5.0.1 release installed, the command output includes the following information:

```
VRTSvxvm          5.0.31.5          Veritas Volume Manager by Symantec
```

If you have the 5.1 SP1 release installed, the command output includes the following information:

```
VRTSvxvm          5.1.100.000      Veritas Volume Manager by Symantec
```

Pre-upgrade tasks for migrating the SFDB repository database

If you plan to continue using checkpoints or SmartTier for Oracle policies you created with a 5.0x or earlier version of Storage Foundation for Oracle, you must prepare to migrate the SFDB repository database to 5.1 SP1 before upgrading to Storage Foundation or Storage Foundation for Oracle RAC 5.1 SP1.

If you are upgrading from 5.1 to 5.1 SP1, no upgrade steps are required for the SFDB tools.

Note: The Sfua_Base repository resource group will be removed from the main.cf file. It is not required as a separate service group for SFHA 5.1 SP1.

Perform the following before upgrading SFHA.

To prepare to migrate the repository database

- ◆ Resynchronize all existing snapshots before upgrading. As Oracle user, enter:

```
$ /opt/VRTS/bin/dbed_vmsnap -S $ORACLE_SID \  
-f SNAPPLAN -o resync
```

Warning: The Database Flashsnap clone database will not be able to be carried over after upgrading. You must create a new Database Flashsnap clone database after upgrading to 5.1 SP1.

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).

VVR supports replicating data between VVR 5.1 SP1 and VVR 5.0.1 or later.

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

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in [Table 12-4](#), 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 12-4 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
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.
 - OFFLINE all application service groups that do not contain RVG resources. Do not OFFLINE the service groups containing RVG resources.
 - If the application resources are part of the same service group as an RVG resource, then OFFLINE only the application resources. In other words, ensure that the RVG resource remains ONLINE so that the private disk groups containing these RVG objects do not get deported.

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

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

```
# haconf -makerw
```

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

```
# hagrps -list
```

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

```
# hagrps -freeze group_name -persistent
```

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 201.

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.

Upgrading the array support

The Storage Foundation 5.1 SP1 release includes all array support in a single depot, VRTSaslapm. The array support depot includes the array support previously included in the VRTSvxvm depot. The array support depot 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 depot 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 through updates to the VRTSaslapm package.

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

Upgrading Storage Foundation or Storage Foundation and High Availability

This chapter includes the following topics:

- [Upgrading Storage Foundation or Storage Foundation High Availability using the script-based installer](#)
- [Upgrading SFHA with the Veritas Web-based installer](#)
- [Upgrading the HP-UX operating system](#)
- [Upgrading Veritas Volume Replicator](#)

Upgrading Storage Foundation or Storage Foundation High Availability using the script-based installer

You can use the script-based installer to upgrade Storage Foundation or Storage Foundation High Availability.

Upgrading from Storage Foundation or Storage Foundation and High Availability 5.0_11iv3, 5.0.1, 5.0.1 RP1, or 5.0.1 RP2

This procedure describes upgrading from Storage Foundation or Storage Foundation and High Availability 5.0_11iv3, 5.0.1, or 5.0.1 RP1 on HP-UX 11i v3 to 5.1 SP1 on HP-UX 11i v3.

After successful completion of the upgrade, disk groups that you created in previous versions are accessible.

To upgrade from Storage Foundation or Storage Foundation and High Availability on HP-UX 11i v3

- 1 Perform the necessary pre-upgrade tasks such as resynchronizing existing database snapshots.
- 2 Upgrade the HP-UX operating system to the latest available HP-UX 11i v3 fusion release.
- 3 If patches to HP-UX 11i v3 are required, apply the patches before upgrading the product.
- 4 Install Storage Foundation 5.1 SP1 for HP-UX 11i v3 using the installer script.

```
# ./installer
```

- 5 Enter **G** to upgrade and press **Return**.
- 6 You are prompted to enter the system names on which the software is to be installed. Enter the system name or names and then press Return.

Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.

- 7 You are prompted to agree with the End User License Agreement. Enter **y** and press Return.

```
Do you agree with the terms of the End User License Agreement as specified
in the storage_foundation/EULA/en/EULA_SF_Ux_5.1SP1.pdf file present on
media? [y,n,q,?] y
```

- 8** The installer lists the packages that will be installed or updated. You are prompted to confirm that you are ready to stop SF processes.

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

If you select **y**, the installer stops the product processes and makes some configuration updates before upgrading.

- 9** The installer uninstalls and reinstalls the listed packages.
- 10** Uncomment the entries in the `/etc/fstab` file which were commented as part of the pre-upgrade steps.
- 11** Reboot all the nodes.

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

- 12** Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctl status
```

- 13** If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctl start
```

Upgrading from previous versions of Storage Foundation on HP-UX 11i v2

Use this procedure to upgrade Storage Foundation from a previous version on HP-UX 11i v2. You can upgrade to Storage Foundation 5.1 SP1 from Storage Foundation 4.1, 4.1 MP1, 4.1 MP2, 5.0. 5.0 MP1, or 5.0 MP2 on HP-UX 11i v2.

After successful completion of the upgrade, any disk groups that were created in Storage Foundation 4.1, 4.1 MP1, 4.1 MP2, 5.0. 5.0 MP1, or 5.0 MP2 are accessible by Storage Foundation 5.1 SP1.

Note: If you are upgrading from Storage Foundation for Oracle:

See [“Tasks for upgrading the Storage Foundation for Databases \(SFDB\) tools”](#) on page 192.

To upgrade from Storage Foundation or Storage Foundation for Oracle on HP-UX 11i v2

- 1** Perform the necessary preupgrade tasks such as resynchronizing existing database snapshots.

- 2 If you have any external Array Policy Modules (APMs) installed, uninstall the APMs. The following warning message displays during the OS upgrade and also when you issue an administrative command for HP-UX kernel modules after the upgrade, until SF 5.0 on HP-UX 11i v3 is installed:

```
WARNING: The file '/usr/conf/mod/dmpXXX.1' does not
contain valid kernel code. It will be ignored.
```

This message can be ignored and does not affect the functionality of SF.

- 3 Upgrade the HP-UX operating system to the latest available HP-UX 11i v3 fusion release.

See “[Upgrading the HP-UX operating system](#)” on page 218.

- 4 If patches to HP-UX 11i v3 are required, apply the patches before upgrading the product.
- 5 Install Storage Foundation 5.1 SP1 for HP-UX 11i v3 using the installer script.

```
# ./installer
```

- 6 Enter **G** to upgrade and press **Return**.
- 7 You are prompted to enter the system names on which the software is to be installed. Enter the system name or names and then press Return.

Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.

- 8 You are prompted to agree with the End User License Agreement. Enter **y** and press Return.

```
Do you agree with the terms of the End User License Agreement as specified
in the storage_foundation/EULA/en/EULA_SF_Ux_5.1SP1.pdf file present on
media? [y,n,q,?] y
```

- 9 The installer lists the packages that will be installed or updated. You are prompted to confirm that you are ready to stop SF processes.

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

If you select **y**, the installer stops the product processes and makes some configuration updates before upgrading.

- 10 The installer uninstalls and reinstalls the listed packages.

11 Reboot all the nodes.

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

12 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

13 If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

Upgrading from Storage Foundation 3.5 on 11i v1 to Storage Foundation 5.1 SP1 on HP-UX 11i v3

This procedure describes upgrading Storage Foundation 3.5 on HP-UX 11i v1 to Storage Foundation 5.1 SP1 on HP-UX 11i v3. Upgrading from HP-UX 11i v1 requires an intermediate upgrade to HP-UX 11i v2 for Storage Foundation and Storage Foundation Clustered File System.

Veritas Volume Manager 3.5 and Veritas Volume Manager 5.1 SP1 both support disk group version 90. Therefore, any disk groups with version 90 are accessible by Storage Foundation 5.1 SP1 after the upgrade. However, certain features in Storage Foundation 5.1 SP1 may require the latest disk group version. Therefore, we recommend upgrading the disk group.

To upgrade from Storage Foundation 3.5 on HP-UX 11i v1 to Storage Foundation 5.1 SP1 on HP-UX 11i v3

- 1 Stop activity to all Storage Foundation volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.
- 2 Upgrade from HP-UX 11i v1 to HP-UX 11i v2 using practices recommended by HP. HP-UX 11i v2 includes VxVM 4.1 by default. All disk groups created using Storage Foundation 3.5 on HP-UX 11i v1 would be accessible.
- 3 Upgrade from HP-UX 11i v2 to the latest available HP-UX 11i v3 fusion release, using practices recommended by HP. The HP-UX 11i v3 fusion release includes VxVM 5.0 by default.
- 4 If patches to HP-UX 11i v3 are required, apply the patches before upgrading the product.
- 5 Install Storage Foundation 5.1 SP1 for HP-UX 11i v3.

- 6 Start Storage Foundation 5.1 SP1 HP-UX 11i v3 using the `installsf -start` option.

Upgrading from VxVM 5.0 on HP-UX 11i v3 to VxVM 5.1 SP1 using integrated VxVM 5.1 SP1 package for HP-UX 11i v3

You can upgrade from VxVM 5.0 on HP-UX 11i v3 to VxVM 5.1 SP1 on HP-UX 11i v3. Use the integrated VxVM 5.1 SP1 package for HP-UX 11i v3 from the ignite depot.

To upgrade using the integrated VxVM 5.1 SP1 package from the ignite depot

- 1 Use HP recommended steps to integrate VxVM 5.1 SP1 package with the latest 11i v3 fusion.
- 2 Stop activity to all Storage Foundation volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.
- 3 Upgrade the HP-UX 11i v3 operating system to the latest fusion using the integrated VxVM 5.1 SP1 package. This process installs VxVM 5.1 SP1 package with the operating system. All disk groups that were created using VxVM 5.0 11i v3 are accessible.

Upgrading from Storage Foundation High Availability from 5.0_11iv3, 5.0.1, or 5.0.1 RP1 on HP-UX 11i v3 to 5.1 SP1 on HP-UX 11i v3

If your systems are already running Storage Foundation High Availability 5.0_11iv3, 5.0.1, or 5.0.1 RP1 on HP-UX 11i v3, this section describes how to upgrade to Veritas Storage Foundation High Availability 5.1 SP1. The operating system must be at a supported level for this upgrade.

This procedure describes upgrading from Storage Foundation High Availability 5.0_11iv3, 5.0.1, or 5.0.1 RP1 on HP-UX 11i v3 to Storage Foundation High Availability 5.1 SP1 on HP-UX 11i v3.

After successful completion of the upgrade, any disk groups that were created in Storage Foundation High Availability 5.0 are accessible by Storage Foundation High Availability 5.1 SP1.

Note: If you are upgrading from Storage Foundation for Oracle:

See [“Tasks for upgrading the Storage Foundation for Databases \(SFDB\) tools”](#) on page 192.

To upgrade from SFHA or SFORA HA 5.0 on 11.31 to 5.1 SP1 on 11.31

- 1 Stop activity to all SFHA volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

- 2 Offline all the VCS service groups.

```
# hagr -offline servicegroup -sys node_name
```

- 3 Stop VCS if it is already running. On any node, run the following command:

```
# /opt/VRTS/bin/hastop -all
```

- 4 If fencing is configured with VCS, you must disable fencing before proceeding to upgrade.

To disable fencing, perform the following steps:

- 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

- On each node, edit the `/etc/vxfenmode` file to configure vxfen in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

- Stop I/O fencing on each node:

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

# /sbin/vxfenconfig -U
```

- 5 Upgrade the HP-UX operating system to the latest available HP-UX 11i v3 fusion release.
- 6 If patches to HP-UX 11i v3 are required, apply the patches before upgrading the product.
- 7 Install Storage Foundation High Availability 5.1 SP1 for HP-UX 11i v3 using the installer script.

```
# ./installer
```

- 8 Enter **G** to upgrade and press **Return**.

- 9** You are prompted to enter the system names on which the software is to be installed. Enter the system name or names and then press Return.

Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.

- 10** You are prompted to agree with the End User License Agreement. Enter **y** and press Return.

```
Do you agree with the terms of the End User License Agreement
as specified in the storage_foundation_high_availability/
EULA/lang/EULA_SFHA_Ux_5.1SP1.pdf file present on media?
[y,n,q,?] y
```

- 11** The installer lists the packages that will be installed or updated. You are prompted to confirm that you are ready to stop SFHA processes.

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

If you select **y**, the installer stops the product processes and makes some configuration updates before upgrading.

- 12** The installer uninstalls and reinstalls the listed packages.
- 13** Enable I/O fencing if required. Follow the below steps to enable the fencing.

- Execute the following steps on all the nodes:

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

- Set the clusterwide attribute "UseFence" to use SCSI3. Add the following line to the `/etc/VRTSvcs/conf/config/main.cf` file:

```
UseFence=SCSI3
```

- Verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file by running the following commands:

```
# cd /etc/VRTSvcs/conf/config
```

```
# /opt/VRTS/bin/hacf -verify .
```

- 14** Reboot all the nodes.

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

- 15 Start Storage Foundation High Availability 5.1 SP1 for HP-UX 11i v3 using the following command:

```
# ./ installsfha -start
```

- 16 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

- 17 If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

- 18 Disk groups that were created using VxVM 5.0 can be imported after upgrading to VxVM 5.1.100. However, we recommend upgrading the VxVM disk groups to the latest version.

See [“Upgrading VxVM disk group versions”](#) on page 256.

Upgrading from SFHA or SFORAHA 4.1, 4.1 MP1, 4.1 MP2, 5.0. 5.0 MP1, or 5.0 MP2 on HP-UX 11i v2 to SFHA 5.1 SP1 on HP-UX 11i v3

If your systems are already running Storage Foundation High Availability 4.1, 4.1 MP1, 4.1 MP2, 5.0. 5.0 MP1, or 5.0 MP2 on HP-UX 11i v2, you must upgrade the operating system to HP-UX 11i v3. Then upgrade Storage Foundation High Availability to Storage Foundation High Availability 5.1 SP1.

- Prepare to upgrade Veritas products
- Prepare to upgrade SFHA or SFORAHA on HP-UX 11iv2 to HP-UX 11iv3
See [“Preparing to upgrade SFHA or SFORAHA on HP-UX 11i v2 to HP-UX 11i v3”](#) on page 213.
- Upgrade HP-UX
See [“Upgrading the HP-UX operating system”](#) on page 218.
- Upgrade SFHA
See [“Upgrading SFHA on HP-UX 11i v2 to 5.1 SP1”](#) on page 215.

Preparing to upgrade SFHA or SFORAHA on HP-UX 11i v2 to HP-UX 11i v3

Perform the following steps before you upgrade SFHA or SFORAHA on HP-UX 11i v2 to SFHA on HP-UX 11i v3.

To prepare for upgrading SFHA or SFORAHA on HP-UX 11i v2 to HP-UX 11iv3

- 1 Perform the necessary pre-upgrade steps before upgrading the product stack to SFHA 5.1SP1.

- 2 Take all the service groups offline.

```
# hagrps -offline servicegroup1 -sys host1
```

- 3 Unmount all the file systems from all the nodes that are not under VCS control.

```
# umount /mnt1
```

- 4 Freeze all the service groups in the configuration.

```
# haconf -makerw  
# hagrps -freeze servicegroup1 -persistent  
# hagrps -dump -makero
```

- 5 Stop VCS on all the nodes. Run the following command on any one node in the cluster.

```
# hastop -all
```

- 6 If fencing is configured with VCS, you must disable fencing before proceeding to upgrade.

To disable fencing, perform the following steps:

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

- On each node, edit the `/etc/vxfenmode` file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode  
vxfen_mode=disabled
```

- Stop I/O fencing on each node:

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

Upgrading HP-UX

Upgrade the HP-UX operating system to the latest available HP-UX 11i v3 fusion release. The Base-VxFS-50, Base-VxVM-50 and Base-VxTools-50 bundles need to be selected while upgrading using update-ux(1M).

If patches to HP-UX 11i v3 are required, apply the patches before upgrading the Veritas product.

See [“Upgrading the HP-UX operating system”](#) on page 218.

Upgrading SFHA on HP-UX 11i v2 to 5.1 SP1

Use the product installer to upgrade the packages of SFHA from 4.1 or 5.0 to SFHA 5.1SP1. SFHA 5.1SP1 is only supported on HP-UX 11i v3. If you are already running Storage Foundation High Availability 4.1 or 5.0 on HP-UX 11i v2, you must upgrade the operating system to HP-UX 11i v3. Then upgrade Storage Foundation High Availability to Storage Foundation High Availability 5.1 SP1.

Note: If you are upgrading from Storage Foundation for Oracle:

See [“Tasks for upgrading the Storage Foundation for Databases \(SFDB\) tools”](#) on page 192.

To upgrade from Storage Foundation HA 4.1 or 5.0 on HP-UX 11i v2 to Storage Foundation HA 5.1 SP1

- 1 Check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctl status
```

- 2 If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctl stop
```

- 3 Insert the appropriate software disc into your system's DVD drive.
- 4 Create a directory in which to mount the software disc and mount the disc using the appropriate drive name. For example:

```
# mkdir -p /dvdrom  
# /usr/sbin/mount -F cdfs /dev/dsk/c3t2d0 /dvdrom
```

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

```
# cd /dvdrom
```

- 6** Install Storage Foundation High Availability 5.1 SP1 on HP-UX 11i v3 using the installer script.

```
# ./installer
```

- 7** Enter **G** to upgrade and press **Return**.
- 8** You are prompted to enter the system names on which the software is to be installed. Enter the system name or names and then press Return.

Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.

- 9** You are prompted to agree with the End User License Agreement. Enter **y** and press Return.

```
Do you agree with the terms of the End User License Agreement as specified
in the storage_foundation/EULA/en/EULA_SF_Ux_5.1SP1.pdf file present on
media? [y,n,q,?] y
```

- 10** The installer lists the packages that will be installed or updated. You are prompted to confirm that you are ready to stop SF processes.

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

If you select **y**, the installer stops the product processes and makes some configuration updates before upgrading.

- 11** The installer uninstalls and reinstalls the listed packages.
- 12** Uncomment the entries in `/etc/fstab` which were commented as part of the pre-upgrade steps.
- 13** Enable I/O fencing if required. Perform the following steps to enable fencing.

- Change the `/etc/vxfenmode` file to enable fencing.

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

- Set the clusterwide attribute "UseFence" to use SCSI3. Add the following line to the `/etc/VRTSvcs/conf/config/main.cf` file:

```
UseFence=SCSI3
```

- Verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file by running the following commands:

```
# cd /etc/VRTSvcs/conf/config  
# /opt/VRTS/bin/hacf -verify .
```

14 Reboot all the nodes.

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

15 After reboot, check if the VEA service has restarted:

```
# /opt/VRTS/bin/vxsvcctl status
```

16 If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctl start
```

17 Disk groups that were created using VxVM 4.1 or VxVM 5.0 can be imported after upgrading to VxVM 5.1.100. However, we recommend upgrading the VxVM disk groups to the latest version.

See [“Upgrading VxVM disk group versions”](#) on page 256.

18 Once the product is up and running, perform all the necessary post-upgrade steps. See chapter 15.

Upgrading SFHA with the Veritas Web-based installer

This section describes how to upgrade SFHA with the Veritas Web-based installer. 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.

To upgrade SFHA

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

- 3 Start the Web-based installer.
See “Starting the Veritas Web-based installer” on page 71.
- 4 On the Select a task and a product page, select **Upgrade a Product**.
The installer detects the product that is installed on the specified system.
- 5 Indicate the systems on which to upgrade. Enter one or more system names, separated by spaces. Click **Validate**.
- 6 On the License agreement page, select whether you accept the terms of the End User License Agreement (EULA). To continue, select **Yes I agree** and click **Next**.
- 7 Click **Next** to complete the upgrade.
After the upgrade completes, the installer displays the location of the log and summary files. If required, view the files to confirm the installation status.
- 8 After the upgrade, if the product is not configured, the web-based installer asks: "Do you want to configure this product?" If the product is already configured, it will not ask any questions.
- 9 Click **Finish**. The installer prompts you for another task.
- 10 If you want to upgrade VCS or SFHA 5.1 on the CP server systems to version Storage Foundation 5.1 SP1, make sure that you upgraded all application clusters to version Storage Foundation 5.1 SP1. Then, upgrade VCS or SFHA on the CP server systems. For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

If you are upgrading from 4.x, you may need to create new VCS accounts if you used native operating system accounts.

Upgrading the HP-UX operating system

If you are on an unsupported version of the operating system, you need to upgrade it to HP-UX B.11.31.1009, HP-UX 11i Version 3 September 2010 Operating Environments Update Release or later.

If you are upgrading the operating system from HP-UX 11i v2, make sure that you choose the following depots along with the HP-UX 11i v3 September 2010 OEUR release depots:

- Base-VxFS-50
- Base-VxTools-50
- Base-VxVM-50

To upgrade the operating system from HP-UX 11i v2, run the `update-ux` command specifying the Veritas depots along with the HP-UX operating system depots:

```
# swinstall -s os_path Update-UX
# update-ux -s os_path HPUX11i-DC-OE \
Base-VxFS-50 Base-VxTools-50 Base-VxVM-50
```

where `os_path` is the full path of the directory containing the operating system depots.

To upgrade the operating system from HP-UX 11i v3, run the `update-ux` command as follows:

```
# update-ux -s os_path HPUX11i-DC-OE
```

where `os_path` is the full path of the directory containing the operating system depots.

For detailed instructions on upgrading the operating system, see the operating system documentation.

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.

See [“Upgrading VVR without disrupting replication”](#) on page 219.

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 198.

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 4.1 or later 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 198.

Performing a phased upgrade

This chapter includes the following topics:

- [About phased upgrade](#)
- [Performing a phased upgrade](#)

About phased upgrade

Perform a phased upgrade to minimize the downtime for the cluster. Depending on the situation, you can calculate the approximate downtime as follows:

You can fail over all your service groups to the nodes that are up.	Downtime equals the time that is taken to offline and online the service groups.
---	--

You have a service group that you cannot fail over to a node that runs during upgrade.	Downtime for that service group equals the time that is taken to perform an upgrade and restart the node.
--	---

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 the movement of the service groups from one node to another to minimize the downtime for any particular service group.

Some rough guidelines follow:

- Split the cluster into two subclusters of equal or near equal size.
- 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.
- When you start the installer, only select SFHA.
- While you perform the upgrades, do not add or remove service groups from 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.

Phased upgrade example

In this example, you have four nodes: node01, node02, node03, and node04. You also have four service groups: sg1, sg2, sg3, and sg4. For the purposes of this example, the cluster is split into two subclusters. The nodes node01 and node02 are in the first subcluster, which you first upgrade. The nodes node03 and node04 are in the second subcluster, which you upgrade last.

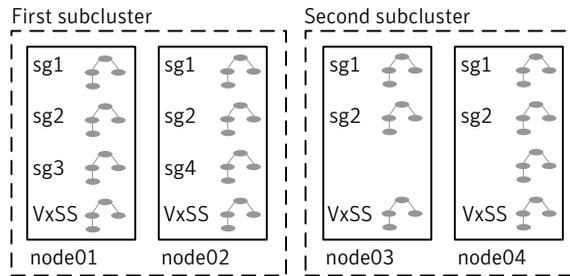
Each service group is running on the nodes as follows:

- sg1 and sg2 are parallel service groups and run on all the nodes.
- sg3 and sg4 are failover service groups. sg3 runs on node01 and sg4 runs on node02.
- VxSS service group runs on all nodes (secure mode is enabled)

In your system list, you have each service group that fails over to other nodes as follows:

- sg1 and sg2 are running on all the nodes.
- sg3 and sg4 can fail over to any of the nodes in the cluster.
- VxSS service group runs on all nodes

Figure 14-1 Example of phased upgrade set up



Phased upgrade example overview

This example's upgrade path follows:

- Move all the service groups from the first subcluster to the second subcluster.
- Upgrade the operating system on the first subcluster's nodes, if required.
- On the first subcluster, start the upgrade using the installation program.
- Get the second subcluster ready.
- Activate the first subcluster.
- Upgrade the operating system on the second subcluster's nodes, if required.
- On the second subcluster, start the upgrade using the installation program.
- Activate the second subcluster.

See [“Performing a phased upgrade”](#) on page 223.

Performing a phased upgrade

This section explains how to perform a phased upgrade of SFHA on four nodes with four service groups. Note that in this scenario, VCS and the service groups cannot stay online on the second subcluster during the upgrade of the second subcluster and vice versa. Do not add, remove, or change resources or service groups on any nodes during the upgrade. These changes are likely to get lost after the upgrade. The following example illustrates the steps to perform a phased upgrade. The phased upgrade is on a secure cluster.

You can perform a phased upgrade from SFHA 5.0.1 to Storage Foundation 5.1 SP1.

See [“About phased upgrade”](#) on page 221.

See [“Phased upgrade example”](#) on page 222.

Moving the service groups to the second subcluster

Perform the following steps to establish the service group's status and to switch the service groups.

To move service groups to the second subcluster

- 1 On the first subcluster, determine where the service groups are online.

```
# hagrps -state
```

The output resembles the following:

#Group	Attribute	System	Value
sg1	State	node01	ONLINE
sg1	State	node02	ONLINE
sg1	State	node03	ONLINE
sg1	State	node04	ONLINE
sg2	State	node01	ONLINE
sg2	State	node02	ONLINE
sg2	State	node03	ONLINE
sg2	State	node04	ONLINE
sg3	State	node01	ONLINE
sg3	State	node02	OFFLINE
sg3	State	node03	OFFLINE
sg3	State	node04	OFFLINE
sg4	State	node01	OFFLINE
sg4	State	node02	ONLINE
sg4	State	node03	OFFLINE
sg4	State	node04	OFFLINE
VxSS	State	node01	ONLINE
VxSS	State	node02	ONLINE
VxSS	State	node03	ONLINE
VxSS	State	node04	ONLINE

- 2 Take the parallel service groups (sg1 and sg2) and the VXSS group offline from the first subcluster. Switch the failover service groups (sg3 and sg4) from the first subcluster (node01 and node02) to the nodes on the second subcluster (node03 and node04).

```
# hagrps -offline sg1 -sys node01
# hagrps -offline sg2 -sys node01
# hagrps -offline sg1 -sys node02
# hagrps -offline sg2 -sys node02
# hagrps -offline VxSS -sys node01
# hagrps -offline VxSS -sys node02
# hagrps -switch sg3 -to node03
# hagrps -switch sg4 -to node04
```

3 On the nodes in the first subcluster, stop all VxVM volumes (for each disk group) that VCS does not manage.

4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

5 Freeze the nodes in the first subcluster.

```
# hasys -freeze -persistent node01
```

```
# hasys -freeze -persistent node02
```

6 Dump the configuration and make it read-only.

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

7 Verify that the service groups are offline on the first subcluster that you want to upgrade.

```
# hagrps -state
```

Output resembles:

```
#Group Attribute System Value
sg1 State node01 |OFFLINE|
sg1 State node02 |OFFLINE|
sg1 State node03 |ONLINE|
sg1 State node04 |ONLINE|
sg2 State node01 |OFFLINE|
sg2 State node02 |OFFLINE|
sg2 State node03 |ONLINE|
sg2 State node04 |ONLINE|
sg3 State node01 |OFFLINE|
sg3 State node02 |OFFLINE|
sg3 State node03 |ONLINE|
sg3 State node04 |OFFLINE|
sg4 State node01 |OFFLINE|
sg4 State node02 |OFFLINE|
sg4 State node03 |OFFLINE|
sg4 State node04 |ONLINE|
VxSS State node01 |OFFLINE|
VxSS State node02 |OFFLINE|
VxSS State node03 |ONLINE|
VxSS State node04 |ONLINE|
```

8 Perform this step on the nodes (node01 and node02) in the first subcluster if the cluster uses I/O Fencing. Use an editor of your choice and change the following:

- In the `/etc/vxfenmode` file, change the value of the `vxfen_mode` variable from `scsi3` to `disabled`. You want the line in the `vxfenmode` file to resemble:

```
vxfen_mode=disabled
```

- In the `/etc/VRTSvcs/conf/config/main.cf` file, change the value of the `UseFence` attribute from `SCSI3` to `NONE`. You want the line in the `main.cf` file to resemble:

```
UseFence = NONE
```

9 Back up the `llttab`, `llthosts`, `gabtab`, `types.cf`, `main.cf` and AT configuration files on the first subcluster.

```
# cp /etc/llttab /etc/llttab.bkp
# cp /etc/llthosts /etc/llthosts.bkp
# cp /etc/gabtab /etc/gabtab.bkp
# cp /etc/VRTSvcs/conf/config/main.cf \
    /etc/VRTSvcs/conf/config/main.cf.bkp
# cp /etc/VRTSvcs/conf/config/types.cf \
    /etc/VRTSvcs/conf/config/types.cf.bkp
# /opt/VRTSat/bin/vssat showbackuplist
B|/var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
B|/var/VRTSat/.VRTSat/profile/certstore
B|/var/VRTSat/ABAuthSource
B|/etc/vx/vss/VRTSat.conf
Quiescing ...
Snapshot Directory :/var/VRTSatSnapShot
```

Upgrading the operating system on the first subcluster

You can perform the operating system upgrade on the first subcluster, if required. Refer to the operating system's documentation for more information.

Upgrading the first subcluster

You now navigate to the installer program and start it.

To start the installer for the phased upgrade

- 1 Confirm that you are logged on as the superuser and you mounted the product disc.

- 2 Navigate to the folder that contains `installsfha`.

```
# cd /storage_foundation_high_availability
```

- 3 Make sure that you can use secure shell or remote shell to connect from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

- 4 Start the `installsfha` program, specify the nodes in the first subcluster (`node1` and `node2`).

```
# ./installsfha node1 node2
```

The program starts with a copyright message and specifies the directory where it creates the logs.

- 5 Enter **y** to agree to the End User License Agreement (EULA).

```
Do you agree with the terms of the End User License Agreement
as specified in the storage_foundation_high_availability/
EULA/<lang>/EULA_sFHA_Ux_5.1SP1.pdf
file present on media? [y,n,q,?] y
```

- 6 Review the available installation options.

- 1 Installs only the minimal required SFHA depots that provides basic functionality of the product.

- 2 Installs the recommended SFHA depots that provides complete functionality of the product.

Note that this option is the default.

- 3 Installs all the SFHA depots.

You must choose this option to configure any optional SFHA feature.

- 4 Displays the SFHA depots for each option.

For this example, select **3** for all depots.

```
Select the depots to be installed on all systems? [1-4,q,?]
(2) 3
```

7 The installer performs a series of checks and tests to ensure communications, licensing, and compatibility. The installer discovers some warning messages and notes on the systems.

8 When you are prompted, reply **y** to continue with the upgrade.

```
Do you want to continue? [y,n,q] (y)
```

9 The installer displays the list of depots that get installed or upgraded on the selected systems.

10 When you are prompted, reply **y** to stop appropriate processes.

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

The upgrade is finished on the first subcluster. Do not reboot the nodes in the first subcluster until you complete the [Preparing the second subcluster](#) procedure.

Preparing the second subcluster

Perform the following steps on the second subcluster before rebooting nodes in the first subcluster.

To prepare to upgrade the second subcluster

1 Get the summary of the status of your resources.

```
# hastatus -summ
-- SYSTEM STATE
-- System                State                Frozen

A  node01                EXITED                1
A  node02                EXITED                1
A  node03                RUNNING              0
A  node04                RUNNING              0

-- GROUP STATE
-- Group                System  Probed    AutoDisabled  State

B  SG1                  node01  Y         N              OFFLINE
B  SG1                  node02  Y         N              OFFLINE
B  SG1                  node03  Y         N              ONLINE
B  SG1                  node04  Y         N              ONLINE
B  SG2                  node01  Y         N              OFFLINE
B  SG2                  node02  Y         N              OFFLINE
B  SG2                  node03  Y         N              ONLINE
B  SG2                  node04  Y         N              ONLINE
B  SG3                  node01  Y         N              OFFLINE
B  SG3                  node02  Y         N              OFFLINE
B  SG3                  node03  Y         N              ONLINE
B  SG3                  node04  Y         N              OFFLINE
B  SG4                  node01  Y         N              OFFLINE
B  SG4                  node02  Y         N              OFFLINE
B  SG4                  node03  Y         N              OFFLINE
B  SG4                  node04  Y         N              ONLINE
B  VxSS                 node01  Y         N              OFFLINE
B  VxSS                 node02  Y         N              OFFLINE
B  VxSS                 node03  Y         N              ONLINE
B  VxSS                 node04  Y         N              ONLINE
```

- 2** Stop all VxVM volumes (for each disk group) that VCS does not manage.
- 3** Make the configuration writable on the second subcluster.

```
# haconf -makerw
```

4 Unfreeze the service groups.

```
# hagr -unfreeze sg1 -persistent
# hagr -unfreeze sg2 -persistent
# hagr -unfreeze sg3 -persistent
# hagr -unfreeze sg4 -persistent
# hagr -unfreeze VxSS -persistent
```

5 Dump the configuration and make it read-only.

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

6 Take the service groups offline on node03 and node04.

```
# hagr -offline sg1 -sys node03
# hagr -offline sg1 -sys node04
# hagr -offline sg2 -sys node03
# hagr -offline sg2 -sys node04
# hagr -offline sg3 -sys node03
# hagr -offline sg4 -sys node04
# hagr -offline VxSS -sys node03
# hagr -offline VxSS -sys node04
```

7 Verify the state of the service groups.

```
# hagr -state
#Group      Attribute  System  Value
SG1         State     node01  |OFFLINE|
SG1         State     node02  |OFFLINE|
SG1         State     node03  |OFFLINE|
SG1         State     node04  |OFFLINE|
SG2         State     node01  |OFFLINE|
SG2         State     node02  |OFFLINE|
SG2         State     node03  |OFFLINE|
SG2         State     node04  |OFFLINE|
SG3         State     node01  |OFFLINE|
SG3         State     node02  |OFFLINE|
SG3         State     node03  |OFFLINE|
SG3         State     node04  |OFFLINE|
VxSS        State     node01  |OFFLINE|
VxSS        State     node02  |OFFLINE|
VxSS        State     node03  |OFFLINE|
VxSS        State     node04  |OFFLINE|
```

- 8 Perform this step on node03 and node04 if the cluster uses I/O Fencing. Use an editor of your choice and change the following:

- In the `/etc/vxfenmode` file, change the value of the `vxfen_mode` variable from `scsi3` to `disabled`. You want the line in the `vxfenmode` file to resemble:

```
vxfen_mode=disabled
```

- In the `/etc/VRTSvcs/conf/config/main.cf` file, change the value of the `UseFence` attribute from `SCSI3` to `NONE`. You want the line in the `main.cf` file to resemble:

```
UseFence = NONE
```

- 9 Stop VCS, I/O Fencing, GAB, and LLT on node03 and node04.

```
# hstop -local  
# /sbin/init.d/vxfen stop  
# /sbin/init.d/gab stop  
# /sbin/init.d/llt stop
```

Activating the first subcluster

Get the first subcluster ready for the service groups.

To activate the first subcluster

- 1 Perform this step on node01 and node02 if the cluster uses I/O Fencing. Use an editor of your choice and revert the following to an enabled state before you reboot the first subcluster's nodes:

- In the `/etc/VRTSvcs/conf/config/main.cf` file, change the value of the `UseFence` attribute from `NONE` to `SCSI3`. You want the line in the `main.cf` file to resemble:

```
UseFence = SCSI3
```

- In the `/etc/vxfenmode` file, change the value of the `vxfen_mode` variable from `disabled` to `scsi3`. You want the line in the `vxfenmode` file to resemble:

```
vxfen_mode=scsi3
```

- 2 Reboot the node01 and node02 in the first subcluster.

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

- 3 Seed node01 and node02 in the first subcluster.

```
# gabconfig -xc
```

- 4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

- 5 Unfreeze the nodes in the first subcluster.

```
# hasys -unfreeze -persistent node01  
# hasys -unfreeze -persistent node02
```

- 6 Dump the configuration and make it read-only.

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

- 7 Bring the service groups online on node01 and node02.

```
# hagr -online sg1 -sys node01  
# hagr -online sg1 -sys node02  
# hagr -online sg2 -sys node01  
# hagr -online sg2 -sys node02  
# hagr -online sg3 -sys node01  
# hagr -online sg4 -sys node02  
# hagr -online VxSS -sys node01  
# hagr -online VxSS -sys node02
```

Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required. Refer to the operating system's documentation for more information.

Upgrading the second subcluster

Perform the following procedure to upgrade the second subcluster (node03 and node04).

To start the installer to upgrade the second subcluster

- 1 Confirm that you are logged on as the superuser and you mounted the product disc.

- 2 Navigate to the folder that contains `installsfha`.

```
# cd /storage_foundation_high_availability
```

- 3 Confirm that SFHA is stopped on node03 and node04. Start the `installsfha` program, specify the nodes in the second subcluster (node3 and node4).

```
# ./installsfha node3 node4
```

The program starts with a copyright message and specifies the directory where it creates the logs.

- 4 Enter **y** to agree to the End User License Agreement (EULA).

```
Do you agree with the terms of the End User License Agreement
as specified in the storage_foundation_high_availability/
EULA/<lang>/EULA_SFHA_Ux_5.1SP1.pdf
file present on media? [y,n,q,?] y
```

- 5 Review the available installation options.

- 1 Installs only the minimal required SFHA depots that provides basic functionality of the product.

- 2 Installs the recommended SFHA depots that provides complete functionality of the product.

Note that this option is the default.

- 3 Installs all the SFHA depots.

You must choose this option to configure any optional SFHA feature.

- 4 Displays the SFHA depots for each option.

For this example, select **3** for all depots.

```
Select the depots to be installed on all systems? [1-4,q,?]
(2) 3
```

- 6 The installer performs a series of checks and tests to ensure communications, licensing, and compatibility. The installer discovers some warning messages and notes on the systems.

- 7 When you are prompted, reply **y** to continue with the upgrade.

```
Do you want to continue? [y,n,q] (y)
```

- 8 The installer displays the list of depots to get installed or upgraded on the selected systems.
- 9 When you are prompted, reply **y** to stop appropriate processes.

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

- 10 Monitor the installer program answering questions as appropriate until the upgrade completes.

Finishing the phased upgrade

You now have to reboot the nodes in the second subcluster.

To finish the upgrade

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

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-remsh]
-clus -display node1 [node2 ...]
```

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 [-remsh] -clus
-copy -from_sys node01 -to_sys node03 node04
```

- 2 Perform this step on node03 and node04 if the cluster uses I/O Fencing. Use an editor of your choice and revert the following to an enabled state before you reboot the second subcluster's nodes:
 - In the `/etc/vxfenmode` file, change the value of the `vxfen_mode` variable from disabled to `scsi3`. You want the line in the `vxfenmode` file to resemble:

```
vxfen_mode=scsi3
```

- 3 Reboot the node03 and node04 in the second subcluster.

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

The nodes in the second subcluster join the nodes in the first subcluster.

4 Check to see if SFHA and High Availabiltiy and its components are up.

```
# gabconfig -a
```

```
GAB Port Memberships
```

```
=====
```

```
Port a gen nxxxxnn membership 0123
```

```
Port b gen nxxxxnn membership 0123
```

```
Port h gen nxxxxnn membership 0123
```

5 Run an `hastatus -sum` command to determine the status of the nodes, service groups, and cluster.

```
# hastatus -sum

-- SYSTEM STATE
-- System          State          Frozen

A node01          RUNNING       0
A node02          RUNNING       0
A node03          RUNNING       0
A node04          RUNNING       0

-- GROUP STATE
-- Group           System         Probed   AutoDisabled  State

B VxSS            node01        Y        N              ONLINE
B VxSS            node02        Y        N              ONLINE
B VxSS            node03        Y        N              ONLINE
B VxSS            node04        Y        N              ONLINE
B sg1             node01        Y        N              ONLINE
B sg1             node02        Y        N              ONLINE
B sg1             node03        Y        N              ONLINE
B sg1             node04        Y        N              ONLINE
B sg2             node01        Y        N              ONLINE
B sg2             node02        Y        N              ONLINE
B sg2             node03        Y        N              ONLINE
B sg2             node04        Y        N              ONLINE
B sg3             node01        Y        N              OFFLINE
B sg3             node02        Y        N              OFFLINE
B sg3             node03        Y        N              OFFLINE
B sg3             node04        Y        N              OFFLINE
B sg4             node01        Y        N              OFFLINE
B sg4             node02        Y        N              OFFLINE
B sg4             node03        Y        N              OFFLINE
B sg4             node04        Y        N              OFFLINE
```

6 After the upgrade is complete, mount the VxFS file systems and start the VxVM volumes (for each disk group) that VCS does not manage.

In this example, you have performed a phased upgrade of SFHA. The service groups were down when you took them offline on node03 and node04, to the time SFHA brought them online on node01 or node02.

Note: 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, see the VCS or SFHA Installation Guide.

Performing post-upgrade tasks

This chapter includes the following topics:

- [Optional configuration steps](#)
- [Post upgrade tasks for migrating the SFDB repository database](#)
- [Recovering VVR if automatic upgrade fails](#)
- [Post-upgrade tasks when VCS agents for VVR are configured](#)
- [Upgrading disk layout versions](#)
- [Upgrading the VxVM cluster protocol version](#)
- [Changing permissions for Storage Foundation for Databases](#)
- [Editing the snapplan after upgrading Veritas Storage Foundation for Oracle](#)
- [Migrating from /etc/vx/vxdba to /var/vx/vxdba for Oracle](#)
- [About upgrading disk layout versions](#)
- [Upgrading VxVM disk group versions](#)
- [Updating variables](#)
- [Setting the default disk group](#)
- [Configuring Powerfail Timeout after upgrade](#)
- [Converting from QuickLog to Multi-Volume support](#)
- [About enabling LDAP authentication for clusters that run in secure mode](#)

- [Verifying the Veritas Storage Foundation upgrade](#)

Optional configuration steps

After the upgrade is complete, additional tasks may need to be performed.

You can perform the following optional configuration steps:

- If Veritas Volume Replicator (VVR) is configured, do the following steps in the order shown:
 - Reattach the RLINKs.
 - Associate the SRL.
- To upgrade VxFS Disk Layout versions and VxVM Disk Group versions, follow the upgrade instructions.
See [“Upgrading VxVM disk group versions”](#) on page 256.

Post upgrade tasks for migrating the SFDB repository database

To continue using the checkpoints or tering policies you created with a 5.0x or earlier version of Storage Foundation for Oracle, you must perform one of the following procedures after upgrading SFHA to 5.1 SP1:

- After you upgrade from 5.0.x and before you migrate SFDB:
See [“After upgrading from 5.0.x and before migrating SFDB”](#) on page 411.
- Migrating from a 5.0 SFDB repository database
- Migrating from a 4.x SFDB repository database
- Upgrading without migrating existing Database Storage Checkpoints and SmartTier parameters

Migrating from a 5.0 repository database to 5.1 SP1

For clustered environments, perform the following on one node only.

To migrate from a 5.0 repository database to 5.1 SP1

1 When upgrading SFDB tools from the previous release in an HP Service Guard environment, first verify that the `cmviewc1` command can be executed by a non-root user.

2 Rename the startup script `NO_S*vxdbms3` to `S*vxdbms3`.

See “[After upgrading from 5.0.x and before migrating SFDB](#)” on page 411.

3 As root, set the Oracle group permission for various directories used by Oracle.

```
# /opt/VRTSdbed/common/bin/sfua_db_config
```

4 As root, dump out the old Sybase ASA repository. If you are using SFHA or SF Oracle RAC, you only need to this on one node.

```
# /opt/VRTSdbed/migrate/sfua_rept_migrate
```

5 On the same node that you ran `sfua_rept_migrate` run the following command as Oracle user. For each Oracle instance, migrate the old repository data to the SQLite repository.

For SF, use:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME
```

For SFHA, use:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME -G \  
Oracle_service_group
```

6 By default, the repository is created on the filesystem which contains the Oracle SYSTEM tablespace. If you need an alternative repository path, first verify the following requirements:

- Repository path has to be a directory writable by Oracle user.
- If you are using SFHA, the repository must be accessible by all nodes. You can put it in a resource group under VCS control so it can be failed over together with the Oracle database.
- The update commands will not be able to verify accessibility of the repository path and will fail if you have not set up the path correctly.

To create an alternate repository path:

For SF, use:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME -R \  
Alternate_path
```

For SFHA, use:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME \  
-G Oracle_service_group -R Alternate_path
```

- 7 If you are using Database Flashsnap for off-host processing, and if you have a repository on the secondary host that you need to migrate: perform the previous steps on the secondary host.

If you do not have a repository that you need to migrate from 5.0:

As root, set the Oracle group permission for various directories used by Oracle:

```
# /opt/VRTSdbed/common/bin/sfua_db_config
```

- 8** On the primary host, edit your snapplans to remove the "SNAPSHOT_DG=SNAP_*" parameter and add "SNAPSHOT_DG_PREFIX=SNAP_*. The parameter can be any PREFIX value and not necessarily "SNAP_*".

For example:

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.pdx.symantec.com
PRIMARY_DG=system1_data
SNAPSHOT_DG=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.pdx.symantec.com
PRIMARY_DG=judge_data
SNAPSHOT_DG_PREFIX=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

- 9 On the primary host, revalidate your snapshots using the following command:

```
$ /opt/VRTS/bin/dbed_vmchecksnap -S $ORACLE_SID \  
-H $ORACLE_HOME -f SNAPPLAN -o validate
```

This completes the migration of the repository for Database Storage Checkpoints and Database Tiered Storage parameters.

To begin using the Storage Foundation for Databases (SFDB) tools:

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

Migrating from a 4.x repository database to 5.1 SP1

If you are upgrading Veritas Storage Foundation for Oracle, you can migrate to `/var/vx/vxdba` to save space under the root partition. Migrating to `/var/vx/vxdba` is optional. However, if you do not perform this migration, you cannot remove any file or directory from `/etc/vx/vxdba` to ensure proper operation.

To migrate from `/etc/vx/vxdba` to `/var/vx/vxdba`

- 1 Copy the `/etc/vx/vxdba` directory and contents to `/var/vx/vxdba`.

```
# cp -rp /etc/vx/vxdba /var/vx/vxdba
```

- 2 Remove `/etc/vx/vxdba`.

```
# rm -rf /etc/vx/vxdba
```

- 3 Link the two directories.

```
# ln -s /var/vx/vxdba /etc/vx/vxdba
```

To upgrade the SFDB tools from 4.x to 5.1 SP1

- 1 As root, set Oracle group permission for various directories used by Oracle. For clustered environments, use the following on one node.

```
# /opt/VRTSdbed/common/bin/sfua_db_config
```

- 2 On one node, as Oracle user, for each Oracle instance, migrate the old repository data to SQLite repository.

For SF, use:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME
```

For SFHA, use:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME -G \  
Oracle_service_group
```

- 3 By default, the repository is created on the filesystem which contains the Oracle SYSTEM tablespace. If you need an alternative repository path, first verify the following requirements:

- The SFDB repository path has to be a directory writable by Oracle user.
- If you are using SFHA, the repository must be accessible by all nodes. You can put it in a resource group under VCS control so it can be failed over together with the Oracle database.
- The update commands will not be able to verify accessibility of the repository path and will fail if you have not set up the path correctly.

To create an alternate repository path:

For SF, use:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME -R \  
Alternate_path
```

For SFHA, on one node, use:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME \  
-G Oracle_service_group -R Alternate_path
```

- 4 On the primary host, edit your snapplans to remove the "SNAPSHOT_DG=SNAP_*" parameter and add "SNAPSHOT_DG_PREFIX=SNAP_*. The parameter can be any PREFIX value and not necessarily "SNAP_*".

For example:

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=4.0
PRIMARY_HOST=host1
SECONDARY_HOST=host1
PRIMARY_DG=PRODdg
SNAPSHOT_DG=SNAP_PRODdg
ORACLE_SID=PROD
ARCHIVELOG_DEST=/prod_ar
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no

$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=4.0
PRIMARY_HOST=host1
SECONDARY_HOST=host1
PRIMARY_DG=PRODdg
SNAPSHOT_DG_PREFIX=SNAP_PRODdg
ORACLE_SID=PROD
ARCHIVELOG_DEST=/prod_ar
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
```

- 5 If you are using Database Flashsnap for off-host processing, and if you have a repository on the secondary host that you need to migrate: perform steps 1-4 on the secondary host.

If you do not have a repository that you need to migrate from 4.x:

As root, set the Oracle group permission for various directories used by Oracle.

```
# /opt/VRTSdbed/common/bin/sfua_db_config
```

- 6 On the primary host, revalidate your snapshots using the following command:

```
$ /opt/VRTS/bin/dbed_vmchecksnap -S $ORACLE_SID \  
-H $ORACLE_HOME -f SNAPPLAN -o validate
```

This completes the migration of the SFDB repository.

To begin using the Storage Foundation for Databases (SFDB) tools:

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

Recovering VVR if automatic upgrade fails

If the upgrade fails during the configuration phase, after displaying the VVR upgrade directory, the configuration needs to be restored before the next attempt. Run the scripts in the upgrade directory in the following order to restore the configuration:

```
# restoresrl  
# adddcn  
# srlprot  
# attrlink  
# start.rvg
```

After the configuration is restored, the current step can be retried.

Post-upgrade tasks when VCS agents for VVR are configured

The following lists post-upgrade tasks with VCS agents for VVR:

- [Unfreezing the service groups](#)
- [Restoring the original configuration when VCS agents are configured](#)

Unfreezing the service groups

This section describes how to unfreeze services groups and bring them online.

To unfreeze the service groups

- 1 On any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

- 2 Edit the `/etc/VRTSvcs/conf/config/main.cf` file to remove the deprecated attributes, SRL and RLinks, in the RVG and RVGShared resources.
- 3 Verify the syntax of the main.cf file, using the following command:

```
# hacf -verify
```

- 4 Unfreeze all service groups that you froze previously. Enter the following command on any node in the cluster:

```
# hagrps -unfreeze service_group -persistent
```

- 5 Save the configuration on any node in the cluster.

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

- 6 If you are upgrading in a shared disk group environment, bring online the RVGShared groups with the following commands:

```
# hagrps -online RVGShared -sys masterhost
```

- 7 Bring the respective IP resources online on each node.

See [“Preparing for the upgrade when VCS agents are configured”](#) on page 202.

Type the following command on any node in the cluster.

```
# hares -online ip_name -sys system
```

This IP is the virtual IP that is used for replication within the cluster.

- 8 In shared disk group environment, online the virtual IP resource on the master node.

Restoring the original configuration when VCS agents are configured

This section describes how to restore a configuration with VCS configured agents.

Note: Restore the original configuration only after you have upgraded VVR on all nodes for the Primary and Secondary cluster.

To restore the original configuration

- 1 Import all the disk groups in your VVR configuration.

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

Each disk group should be imported onto the same node on which it was online when the upgrade was performed. The reboot after the upgrade could result in another node being online; for example, because of the order of the nodes in the AutoStartList. In this case, switch the VCS group containing the disk groups to the node on which the disk group was online while preparing for the upgrade.

```
# hagrps -switch grpname -to system
```

- 2 Recover all the disk groups by typing the following command on the node on which the disk group was imported in step 1.

```
# vxrecover -bs
```

- 3 Upgrade all the disk groups on all the nodes on which VVR has been upgraded:

```
# vxdg upgrade diskgroup
```

- 4 On all nodes that are Secondary hosts of VVR, make sure the data volumes on the Secondary are the same length as the corresponding ones on the Primary. To shrink volumes that are longer on the Secondary than the Primary, use the following command on each volume on the Secondary:

```
# vxassist -g diskgroup shrinkto volume_name volume_length
```

where *volume_length* is the length of the volume on the Primary.

Note: Do not continue until you complete this step on all the nodes in the Primary and Secondary clusters on which VVR is upgraded.

- 5 Restore the configuration according to the method you used for upgrade:
 If you upgraded with the VVR upgrade scripts

Complete the upgrade by running the `vvr_upgrade_finish` script on all the nodes on which VVR was upgraded. We recommend that you first run the `vvr_upgrade_finish` script on each node that is a Secondary host of VVR.

Perform the following tasks in the order indicated:

- To run the `vvr_upgrade_finish` script, type the following command:

```
# /disc_path/scripts/vvr_upgrade_finish
```

where `disc_path` is the location where the Veritas software disc is mounted.

- Attach the RLINKs on the nodes on which the messages were displayed:

```
# vxrlink -g diskgroup -f att rlink_name
```

If you upgraded with the product installer

Use the Veritas product installer and select Start an Installed Product. Or use the installation script with the `-start` option.

- 6 Bring online the RVGLogowner group on the master:

```
# hagrps -online RVGLogownerGrp -sys masterhost
```

- 7 Start and bring online the failover service groups on the remaining host:

```
# hagrps -online groupname -sys nodename
```

- 8 If you plan on using IPv6, you must bring up IPv6 addresses for virtual replication IP on primary/secondary nodes and switch from using IPv4 to IPv6 host names or addresses, enter:

```
# vradm changeip newpri=v6 newsec=v6
```

where `v6` is the IPv6 address.

- 9 Restart the applications that were stopped.

Upgrading disk layout versions

In this release, you can create and mount only file systems with disk layout Version 6, Version 7, and Version 8. No prior versions can be created or mounted.

Use the `vxfsconvert` or `vxupgrade` utilities to upgrade older disk layout versions to disk layout Version 8.

See the `vxfsconvert` or `vxupgrade` man pages.

For more information about disk layouts, see the *Veritas File System Administrator's Guide*.

Upgrading the VxVM cluster protocol version

If you are upgrading a cluster and you want to take advantage of the new features in this release, you must upgrade the version of the VxVM cluster protocol. To upgrade the protocol to version 70, enter the following command on the master node of the cluster:

```
# vxctl upgrade
```

Changing permissions for Storage Foundation for Databases

After installing Veritas Storage Foundation 5.1 SP1, follow these post-installation steps to ensure Veritas Storage Foundation for Oracle commands work correctly.

Note: Do not recursively change permissions, groups, or owners

To change permissions

- 1 Change permissions for the following directory, depending on which product you have installed:

For Veritas Storage Foundation for Oracle:

```
# chmod 550 /opt/VRTSdbed
```

- 2 Reset owner and group settings to the appropriate owner and group for the database administrators on your system.

For example, in Veritas Storage Foundation for Oracle, to change owner to the user oracle and the group dba, run the following command:

```
# chown oracle:dba /opt/VRTSdbed
```

Editing the snapplan after upgrading Veritas Storage Foundation for Oracle

After you upgrade to 5.1 SP1, upgrade any existing snapplan from a previous release. Complete this procedure before you re-validate the snapplan.

To upgrade the snapplan

- 1 Change to the directory containing the snapplan file:

```
# cd /snapplan
```

- 2 View the snapplan.

```
# cat snap1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=host1
SECONDARY_HOST=host1
PRIMARY_DG=PRODdg1
SNAPSHOT_DG=SNAP_PRODdg1
ORACLE_SID=PROD
ARCHIVELOG_DEST=/prod_ar
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=2
```

- 3 Open the snapplan in a text editor such as vi:

```
# vi snap1
```

- 4 Remove the line containing following parameter:

```
SNAPSHOT_DG=<Some text string>
```

- 5 Add one more line to the snapplan with the following parameter:

```
SNAPSHOT_DG_PREFIX=SNAP_
```

- 6 Save the snapplan file and exit.

7 View the snapplan.

```
# cat snap1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=host1
SECONDARY_HOST=host1
PRIMARY_DG=PRODdg1
ORACLE_SID=PROD
ARCHIVELOG_DEST=/prod_ar
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=2
SNAPSHOT_DG_PREFIX=SNAP_
```

8 Proceed to re-validate the snapplan.

Migrating from `/etc/vx/vxdba` to `/var/vx/vxdba` for Oracle

If you are upgrading Veritas Storage Foundation for Oracle, you can migrate to `/var/vx/vxdba` to save space under the root partition. Migrating to `/var/vx/vxdba` is optional. However, if you do not perform this migration, you cannot remove any file or directory from `/etc/vx/vxdba` to ensure proper operation. This procedure can be done at any time.

To migrate from `/etc/vx/vxdba` to `/var/vx/vxdba`

1 Copy the `/etc/vx/vxdba` directory and contents to `/var/vx/vxdba`.

```
# cp -rp /etc/vx/vxdba /var/vx/vxdba
```

2 Remove `/etc/vx/vxdba`.

```
# rm -rf /etc/vx/vxdba
```

3 Link the two directories.

```
# ln -s /var/vx/vxdba /etc/vx/vxdba
```

About upgrading disk layout versions

You must upgrade your older disk layout versions to make use of the extended features available in the Veritas File System 5.1 SP1 release.

See the *Veritas Storage Foundation Release Notes 5.1 SP1* for information on new features.

Use the `vxfsconvert` or `vxupgrade` utilities to upgrade older disk layout versions to disk layout Version 7.

See the `vxfsconvert` or `vxupgrade` man pages.

Warning: Never upgrade the `/` and `/stand` file systems to disk layout Version 7. The HP-UX bootloader does not support disk layout Version 7.

Upgrading VxFS disk layout versions

Veritas File System 5.1 SP1 allows Version 4, 5, 6 and 7 for locally mounted file systems and disk layout Versions 6 and 7 for cluster mounted file systems. If you have cluster-mounted file systems with disk layout Versions lower than 6, then after upgrading to VxFS 5.1 SP1, upgrade the disk layout. Perform the following additional steps to prepare the file system for being mounted on all nodes of the cluster.

Disk layout Versions 1, 2, and 3 are not supported by VxFS 5.1 SP1. All file systems created on VxFS 5.1 SP1 use disk layout Version 7 by default.

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

To upgrade VxFS disk layout versions

- 1 Select one of the nodes of the cluster and mount the file system locally on this node. Use the `mount`, but without the `-o cluster` option. For example:

```
# mount -F vxfs /dev/vx/dsk/sharedg/vol1 /mnt1
```

- 2 To find the current disk layout version on a file system:

```
# fstyp -v <char_device_path> | grep version | \
awk '{print $2}'
```

- 3 On the node selected in step 1, incrementally upgrade the disk layout of this file system to layout Version 6 or 7.

For example, if you had a cluster mounted file system of disk layout Version 4 running with previous version of VxFS, after upgrading to VxFS 5.1 SP1, you would need to upgrade the disk layout to Version 6 or 7. The incremental upgrade is as follows:

```
# vxupgrade -n 5 /mnt1
# vxupgrade -n 6 /mnt1
# vxupgrade -n 7 /mnt1
```

- 4 On the node selected in step 1, after the disk layout has been successfully upgraded, unmount the file system:

```
# umount /mnt1
```

- 5 This file system can be mounted on all nodes of the cluster.

When to use vxfsconvert

You can use the `vxfsconvert` command to convert an unmounted HFS file system to a Veritas file system with disk layout Version 7.

```
# vxfsconvert /device_name
```

See the `vxfsconvert(1M)` and `fsadm_vxfs(1M)` manual pages.

When to use vxupgrade

You can use the `vxupgrade` command to upgrade older VxFS disk layouts to disk layout Version 7 while the file system remains mounted.

```
# vxupgrade -n 7 /mount_point
```

See the `vxupgrade(1M)` and `fsadm_vxfs(1M)` manual pages.

Warning: The contents of intent logs created on a previous disk layout version cannot be used after the disk layout version is upgraded.

Requirements for upgrading to disk layout Version 7

Converting a previous disk layout to a Version 7 disk layout requires adequate free space. The space and time required to complete the upgrade increases with

the number of files, extended attributes, and hard links in the file system. Typical maximum space is at least two additional inodes with one block for every inode. Allow at least ten minutes to upgrade for every million inodes in the file system.

Upgrading VxVM disk group versions

All Veritas Volume Manager disk groups have an associated version number. Each VxVM release supports a specific set of disk group versions and can import and perform tasks on disk groups with those versions. Some new features and tasks work only on disk groups with the current disk group version. Before you can perform the tasks or use the features, upgrade the existing disk groups.

After upgrading to Storage Foundation 5.1 SP1, you must upgrade any existing disk groups that are organized by ISP. Without the version upgrade, configuration query operations continue to work fine. However, configuration change operations will not function correctly.

For 5.1 SP1, the Veritas Volume Manager disk group version is different than in previous VxVM releases. You must upgrade the disk group version if you upgraded from version 5.1 or earlier.

Use the following command to find the version of a disk group:

```
# vxdg list diskgroup
```

To upgrade a disk group to the current disk group version, use the following command:

```
# vxdg upgrade diskgroup
```

For more information about disk group versions, see the *Veritas Volume Manager Administrator's Guide*.

Updating variables

In `/etc/profile`, update the `PATH` and `MANPATH` variables as needed.

`MANPATH` could include `/opt/VRTS/man` and `PATH /opt/VRTS/bin`.

Setting the default disk group

In releases prior to Volume Manager 4.0, the default disk group was `rootdg` (the root disk group). For Volume Manager to function, the `rootdg` disk group had to exist and it had to contain at least one disk.

This requirement no longer exists; however, you may find it convenient to create a system-wide default disk group. The main benefit of creating a default disk group is that VxVM commands default to the default disk group. You do not need to use the `-g` option.

You can set the name of the default disk group after installation by running the following command on a system:

```
# vxctl defaulttdg diskgroup
```

See the *Veritas Volume Manager Administrator's Guide*.

Configuring Powerfail Timeout after upgrade

When you install SFHA, SFHA configures Powerfail Timeout (PFTO) using tunable parameters. Starting with SFHA 5.0.1, the Powerfail Timeout (PFTO) has the following default values:

- disabled for devices using the HP-UX native multi-pathing
- enabled for devices using DMP

After installation, you can override the defaults, if required. You can explicitly enable or disable PFTO for native multi-pathing devices and DMP devices.

When you upgrade from SFHA release 5.0 or earlier, SFHA does not preserve any user-defined PFTO values. After the upgrade, the PFTO default values apply to all devices. If you want to use the device settings from the previous release, you must set the desired value explicitly. For example, in an SFHA 5.0 installation, you have set the PFTO state to enabled for a native multi-pathing device. After you upgrade from SFHA 5.0 to SFHA 5.1SP1, the native device is set to the default value, which is disabled. In order to use PFTO, you must explicitly enable the PFTO on that device.

When you upgrade from SFHA release 5.0.1 to a higher version, SFHA preserves the PFTO state for the devices. After the upgrade, the PFTO values are set to the same values that the device had before the upgrade. For example, in an SFHA 5.0.1 installation, you have set the PFTO state to enabled for a native multi-pathing device. After you upgrade from SFHA 5.0.1 to SFHA 5.1SP1, the native device is set to enabled.

For more information about controlling Powerfail Timeout, see the *Veritas Volume Manager Administrator's Guide*.

Converting from QuickLog to Multi-Volume support

The 4.1 release of the Veritas File System is the last major release to support QuickLog. The Version 6 or Version 7 disk layout does not support QuickLog. The functionality provided by the Veritas Multi-Volume Support (MVS) feature replaces most of the functionality provided by QuickLog.

The following procedure describes how to convert from QuickLog to MVS. Unlike QuickLog, which allowed logging of up to 31 VxFS file systems to one device, MVS allows intent logging of only one file system per device. Therefore, the following procedure must be performed for each file system that is logged to a QuickLog device if Version 6 or Version 7 disk layout is used.

The QuickLog device did not need to be related to the file system. For MVS, the log volume and the file system volume must be in the same disk group.

To convert Quicklog to MVS

- 1 Select a QuickLog-enabled file system to convert to MVS and unmount it.

```
# umount myfs
```

- 2 Detach one of the QuickLog volumes from the QuickLog device that the file system had been using. This volume will be used as the new intent log volume for the file system.

```
# qlogdetach -g diskgroup log_vol
```

- 3 Create the volume set.

```
# vxvset make myvset myfs_volume
```

- 4 Mount the volume set.

```
# mount -F vxfs /dev/vx/dsk/rootdg/myvset /mnt1
```

- 5 Upgrade the volume set's file system to Version 6 or Version 7 disk layout. See [“About upgrading disk layout versions”](#) on page 254.

For example:

```
# vxupgrade -n 6 /mnt1
```

- 6 Add the log volume from step 2 to the volume set.

```
# vxvset addvol myvset log_vol
```

- 7 Add the log volume to the file system. The size of the volume must be specified.

```
# fsvoladm add /mnt1 log_vol 50m
```

- 8 Move the log to the new volume.

```
# fsadm -o logdev=log_vol,logsize=16m /mnt1
```

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.

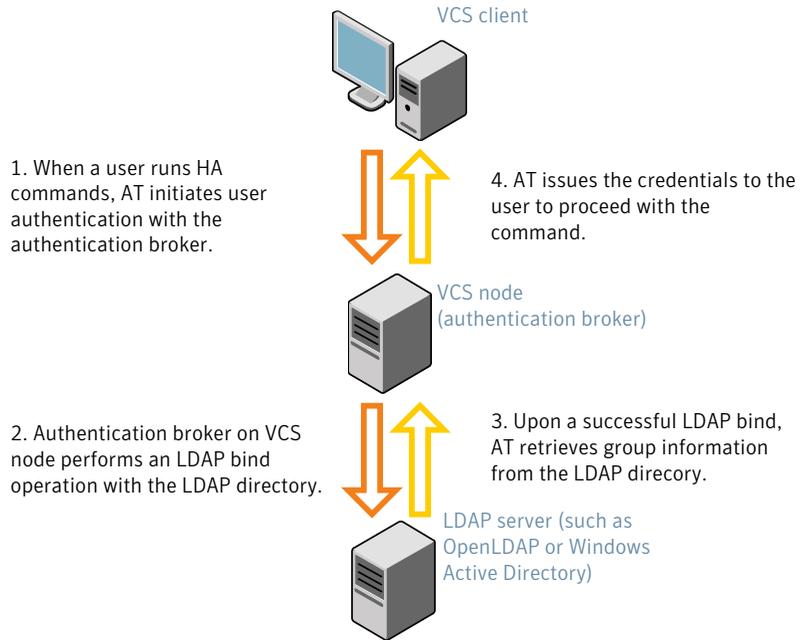
See [“Enabling LDAP authentication for clusters that run in secure mode”](#) on page 261.

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 15-1](#) depicts the SFHA cluster communication with the LDAP servers when clusters run in secure mode.

Figure 15-1 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/VRTSsat/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 SFHA 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/VRTSsat/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 SFHA 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 SFHA 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.

Verifying the Veritas Storage Foundation upgrade

Refer to the section about verifying the installation to verify the upgrade.

See [“Verifying that the products were installed”](#) on page 272.

Verification of the installation or the upgrade

- [Chapter 16. Verifying the installation](#)

Verifying the installation

This chapter includes the following topics:

- [About using the postcheck option](#)
- [Performing a postcheck on a node](#)
- [Verifying that the products were installed](#)
- [Installation log files](#)
- [Starting and stopping processes for the Veritas products](#)
- [Checking Veritas Volume Manager processes](#)
- [Checking Veritas File System installation](#)
- [Verifying the LLT, GAB, and VCS configuration files](#)
- [Verifying LLT, GAB, and cluster operation](#)

About using the postcheck option

You can use the installer's post-check to determine installation-related problems.

Note: This command option requires downtime for the node.

When you use the `postcheck` option, it returns the results of the following commands for VCS and SFCFS:

- `lltconfig` (to check LLT's status)
- `lltstat -nvv` (to check LLT's status)
- `gabconfig -a` (to check ports a, b, and h)

- `vxfenadm -d` (to check fencing)
- `/opt/VRTS/bin/hasys -state` (to check systems' states)
- `/opt/VRTS/bin/hagrp -state` (to check service groups' states)
- `/opt/VRTS/bin/hares -state` (to check resources' states)

See [“Performing a postcheck on a node”](#) on page 272.

Performing a postcheck on a node

The installer's `postcheck` command can help you to determine installation-related problems.

See [“About using the postcheck option”](#) on page 271.

Note: This command option requires downtime for the node.

To run the postcheck command on a node

- ◆ Run the installer with the `-postcheck` option.

```
# ./installer -postcheck system_name
```

The installer reports some errors or warnings if any of the following issues occur:

- Any processes or drivers do not start
- LLT is not configured
- GAB ports are not started
- Etc.

Verifying that the products were installed

Verify that the SFHA products are installed.

You can use the `swlist` command to check which depots have been installed:

```
# swlist -l product | grep VRTS
```

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.

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 `vxiod`, `vxconfigd`, `vxnotify`, `vxesd`, `vxrelocd`, `vxpal`, `vxcached`, `vxconfigbackupd`, and `vxsvc` processes should appear in the output from this command. If you disable hot-relocation, the `vxrelocd` and `vxnotify` processes are not displayed.

If you installed Storage Foundation and High Availability, the `vxodmd` and `vxdbd_11.31` processes are also displayed.

Checking Veritas File System installation

The Veritas File System package consists of a kernel component and administrative commands.

Command installation verification

The Veritas File System commands are installed in the `/opt/VRTS/bin` directory. To verify, determine that the subdirectory is present:

```
# ls /opt/VRTS/bin
```

Make sure you have adjusted your environment variables accordingly.

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 363.
See [“About the VCS configuration files”](#) on page 366.

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 275.
- 4 Verify GAB operation.
- 5 Verify the cluster operation.
See [“Verifying the cluster”](#) on page 278.

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
              lan1 UP    08:00:20:93:0E:34
              lan2 UP    08:00:20:93:0E:38
1 nebula     OPEN
              lan1 UP    08:00:20:8F:D1:F2
              lan2 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/llttab` 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
63    gab        0x1F
      opens:   0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
      connects: 0 1
    
```

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 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    CPUBinding                               BindTo None CPUNumber 0
galaxy    CPUThresholdLevel                       Critical 90 Warning 80 Note 70
                                                Info 60
galaxy    CPUUsage                                 0
galaxy    CPUUsageMonitoring                      Enabled 0 ActionThreshold 0
                                                ActionTimeLimit 0 Action NONE
                                                NotifyThreshold 0 NotifyTimeLimit 0

galaxy    Capacity                                 100
galaxy    ConfigBlockCount                        141
galaxy    ConfigChecksum                          33975
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
galaxy    DynamicLoad                              0
galaxy    EngineRestarted                        0
```

galaxy	EngineVersion	5.1.10.0
galaxy	FencingWeight	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	SwapThresholdLevel	Critical 90 Warning 80 Note 70 Info 60
galaxy	SysInfo	HP-UX:galaxy,U,B.11.31,ia64
galaxy	SysName	galaxy
galaxy	SysState	RUNNING
galaxy	SystemLocation	
galaxy	SystemOwner	
galaxy	TFrozen	0
galaxy	TRSE	0
galaxy	UpDownState	Up

galaxy	UserInt	0
galaxy	UserStr	
galaxy	VCSFeatures	DR
galaxy	VCSMode	

Adding and removing nodes

- [Chapter 17. Adding a node to a cluster](#)
- [Chapter 18. Removing a node from a cluster](#)

Adding a node to a cluster

This chapter includes the following topics:

- [About adding a node to a cluster](#)
- [Before adding a node to a cluster](#)
- [Preparing to add a node to a cluster](#)
- [Adding a node to a cluster](#)
- [Configuring server-based fencing on the new node](#)
- [After adding the new node](#)
- [Updating the Storage Foundation for Databases \(SFDB\) repository after adding a node](#)

About adding a node to a cluster

After you install SFHA 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 SFHA cluster, verify the following:

- Hardware and software requirements are met.
See [“Meeting hardware and software requirements”](#) on page 286.
- Hardware is set up for the new node.
See [“Setting up the hardware”](#) on page 286.
- The existing cluster is a SFHA cluster and that SFHA 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

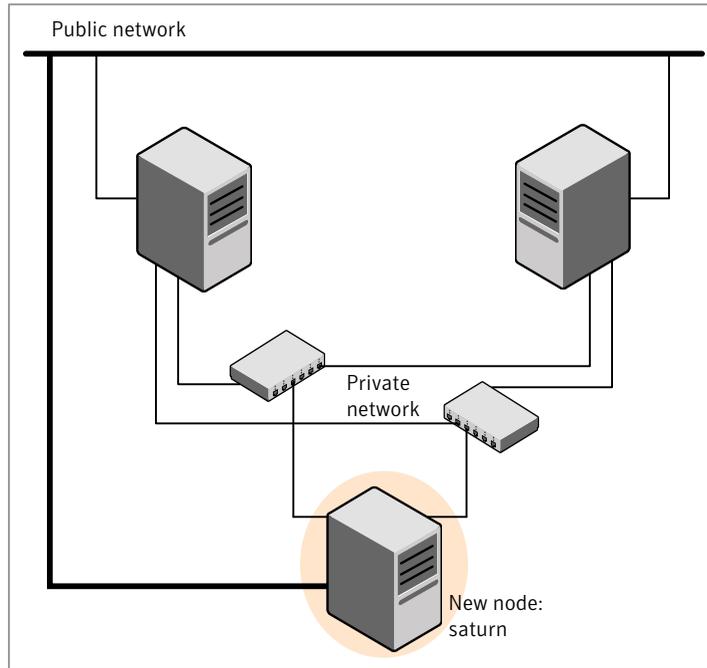
The system you add to the cluster must meet the hardware and software requirements.

See [“Hardware compatibility list \(HCL\)”](#) on page 36.

Setting up the hardware

[Figure 17-1](#) shows that before you configure a new system on an existing cluster, you must physically add the system to the cluster.

Figure 17-1 Adding a node to a two-node cluster using two switches



To set up the hardware

1 Connect the SFHA 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 17-1 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 SFHA cluster.

To prepare the new node

- 1 Verify that the new node meets installation requirements.

```
# ./installsfha -precheck saturn
```

- 2 Install SFHA on the new system.

Note: Use the `-install` option to install SFHA. Do not configure SFHA after the installation.

```
Would you like to configure SFHA 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 32.

Adding a node to a cluster

You can use one of the following methods to add a node to an existing SFHA cluster:

SFHA installer	See “Adding a node to a cluster using the SFHA installer” on page 288.
	See “Adding a node using the Web-based installer” on page 292.
Manual	See “Adding the node to a cluster manually” on page 293.

Note: Before you add the node, make sure that SFHA is not configured on the node.

Adding a node to a cluster using the SFHA installer

You can add a node using the `-addnode` option with the SFHA installer.

The SFHA 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/`
- 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.

At the end of the process, the new node joins the SFHA 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 SFHA installer with the `-addnode` option.

```
# cd /opt/VRTS/install  
# ./installsfha -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 SFHA cluster. The installer uses the node information to identify the existing cluster.

```
Enter a node name in the SFHA 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,?] lan1
```

- 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,?] lan2
```

- 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: lan3
```

- 12** 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 SFHA 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 SFHA installer.

- 13** 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 SFHA 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 294.
- 2 Configure LLT and GAB.
See [“Configuring LLT and GAB on the new node”](#) on page 295.
- 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 296.

- 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 298.
- 5 Start VCS.
See [“To start VCS on the new node”](#) on page 301.
- 6 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 299.

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 `installsfha` 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 VxVM uses license keys to control access. As you run the utility, answer **n** when prompted about licensing; you installed the appropriate license when you ran the `installsfha` utility.
- 3 Enter **n** when prompted to set up a system wide disk group for the system. The installation completes.
- 4 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

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/llttab` file on the new system. For example:

```
set-node saturn
set-cluster 101

link lan1 /dev/lan:1 - ether --
link lan2 /dev/lan:2 - ether --
```

Except for the first line that refers to the node, the file resembles the `/etc/llttab` files on the existing nodes. The second line, the cluster ID, must be the same as in the existing nodes.

- 4 Use `vi` or another text editor to create the file `/etc/gabtab` on the new node. This file must contain a line that resembles the following example:

```
/sbin/gabconfig -c -nN
```

Where `N` represents the number of systems in the cluster. 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 -remsh -clus -copy \  
-from_sys galaxy -to_sys saturn
```

- 8

```
# /sbin/init.d/llt start  
  
# sbin/init.d/gab start  
  
# /sbin/init.d/vxfen start  
  
# kcmodule vxgms=loaded  
  
# kcmodule odm=loaded  
  
# /sbin/init.d/odm stop  
  
# /sbin/init.d/odm start
```

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 17-1](#) uses the following information for the following command examples.

Table 17-1 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 flurbdicatc \  
-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 SFHA related security configuration

Perform the following steps to configure SFHA related security settings.

Setting up SFHA related security configuration

1 Start `/opt/VRTSat/bin/vxatd` process.

2 Create `HA_SERVICES` domain for SFHA.

```
# vssat createpd --pdrtype ab --domain HA_SERVICES
```

3 Add SFHA 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
```

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:

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.

```
# hagrps -modify ClusterService SystemList -add saturn 2  
# hagrps -modify ClusterService AutoStartList -add saturn
```

- 3 Modify the IP address and NIC resource in the existing group for the new node.

```
# hares -modify gcoip Device lan0 -sys saturn  
# hares -modify gconic Device lan0 -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
```

After adding the new node

Start VCS on the new node.

To start VCS on the new node

- ◆ Start VCS on the new node:

```
# hstart
```

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*.

Removing a node from a cluster

This chapter includes the following topics:

- [Removing a node from a cluster](#)

Removing a node from a cluster

[Table 18-1](#) specifies the tasks that are involved in removing a node from a cluster. In the example procedure, the cluster consists of nodes galaxy, nebula, and saturn; node saturn is to leave the cluster.

Table 18-1 Tasks that are involved in removing a node

Task	Reference
<ul style="list-style-type: none"> ■ Back up the configuration file. ■ Check the status of the nodes and the service groups. 	See “Verifying the status of nodes and service groups” on page 304.
<ul style="list-style-type: none"> ■ Switch or remove any SFHA service groups on the node departing the cluster. ■ Delete the node from SFHA configuration. 	See “Deleting the departing node from SFHA configuration” on page 305.
Modify the llthosts and gabtab files to reflect the change.	See “Modifying configuration files on each remaining node” on page 308.
If the existing cluster is configured to use server-based I/O fencing, remove the node configuration from the CP server.	See “Removing the node configuration from the CP server” on page 308.

Table 18-1 Tasks that are involved in removing a node (*continued*)

Task	Reference
For a cluster that is running in a secure mode, remove the security credentials from the leaving node.	See “Removing security credentials from the leaving node” on page 309.
On the node departing the cluster: <ul style="list-style-type: none">■ Modify startup scripts for LLT, GAB, and SFHA to allow reboot of the node without affecting the cluster.■ Unconfigure and unload the LLT and GAB utilities.■ Remove the SFHA depots.	See “Unloading LLT and GAB and removing VCS on the departing node” on page 310.

Verifying the status of nodes and service groups

Start by issuing the following commands from one of the nodes to remain, node galaxy or node nebula.

To verify the status of the nodes and the service groups

- 1 Make a backup copy of the current configuration file, main.cf.

```
# cp -p /etc/VRTSvcs/conf/config/main.cf\  
/etc/VRTSvcs/conf/config/main.cf.goodcopy
```

- 2 Check the status of the systems and the service groups.

```
# hastatus -summary  
  
-- SYSTEM STATE  
-- System      State      Frozen  
A galaxy      RUNNING    0  
A nebula      RUNNING    0  
A saturn      RUNNING    0  
  
-- GROUP STATE  
-- Group      System      Probed    AutoDisabled  State  
B grp1       galaxy      Y         N              ONLINE  
B grp1       nebula      Y         N              OFFLINE  
B grp2       galaxy      Y         N              ONLINE  
B grp3       nebula      Y         N              OFFLINE  
B grp3       saturn      Y         N              ONLINE  
B grp4       saturn      Y         N              ONLINE
```

The example output from the `hastatus` command shows that nodes `galaxy`, `nebula`, and `saturn` are the nodes in the cluster. Also, service group `grp3` is configured to run on node `nebula` and node `saturn`, the departing node. Service group `grp4` runs only on node `saturn`. Service groups `grp1` and `grp2` do not run on node `saturn`.

Deleting the departing node from SFHA configuration

Before you remove a node from the cluster you need to identify the service groups that run on the node.

You then need to perform the following actions:

- Remove the service groups that other service groups depend on, or
- Switch the service groups to another node that other service groups depend on.

To remove or switch service groups from the departing node

- 1 Switch failover service groups from the departing node. You can switch grp3 from node saturn to node nebula.

```
# hagrps -switch grp3 -to nebula
```

- 2 Check for any dependencies involving any service groups that run on the departing node; for example, grp4 runs only on the departing node.

```
# hagrps -dep
```

- 3 If the service group on the departing node requires other service groups—if it is a parent to service groups on other nodes—unlink the service groups.

```
# haconf -makerw
# hagrps -unlink grp4 grp1
```

These commands enable you to edit the configuration and to remove the requirement grp4 has for grp1.

- 4 Stop SFHA on the departing node:

```
# hastop -sys saturn
```

- 5 Check the status again. The state of the departing node should be EXITED. Make sure that any service group that you want to fail over is online on other nodes.

```
# hastatus -summary
```

```
-- SYSTEM STATE
-- System      State          Frozen
A galaxy       RUNNING        0
A nebula       RUNNING        0
A saturn       EXITED         0

-- GROUP STATE
-- Group      System      Probed  AutoDisabled  State
B grp1       galaxy      Y       N              ONLINE
B grp1       nebula      Y       N              OFFLINE
B grp2       galaxy      Y       N              ONLINE
B grp3       nebula      Y       N              ONLINE
B grp3       saturn     Y       Y              OFFLINE
B grp4       saturn     Y       N              OFFLINE
```

- 6 Delete the departing node from the SystemList of service groups grp3 and grp4.

```
# hagrps -modify grp3 SystemList -delete saturn
# hagrps -modify grp4 SystemList -delete saturn
```

- 7 For the service groups that run only on the departing node, delete the resources from the group before you delete the group.

```
# hagrps -resources grp4
    processx_grp4
    processy_grp4
# hares -delete processx_grp4
# hares -delete processy_grp4
```

- 8 Delete the service group that is configured to run on the departing node.

```
# hagrps -delete grp4
```

- 9 Check the status.

```
# hastatus -summary
-- SYSTEM STATE
-- System      State      Frozen
A galaxy       RUNNING   0
A nebula       RUNNING   0
A saturn       EXITED    0

-- GROUP STATE
-- Group      System      Probed   AutoDisabled   State
B grp1       galaxy      Y        N               ONLINE
B grp1       nebula      Y        N               OFFLINE
B grp2       galaxy      Y        N               ONLINE
B grp3       nebula      Y        N               ONLINE
```

- 10 Delete the node from the cluster.

```
# hasys -delete saturn
```

- 11 Save the configuration, making it read only.

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

Modifying configuration files on each remaining node

Perform the following tasks on each of the remaining nodes of the cluster.

To modify the configuration files on a remaining node

- 1 If necessary, modify the `/etc/gabtab` file.

No change is required to this file if the `/sbin/gabconfig` command has only the argument `-c`. Symantec recommends using the `-nN` option, where N is the number of cluster systems.

If the command has the form `/sbin/gabconfig -c -nN`, where N is the number of cluster systems, make sure that N is not greater than the actual number of nodes in the cluster. When N is greater than the number of nodes, GAB does not automatically seed.

Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`.

- 2 Modify the `/etc/llthosts` file on each remaining nodes to remove the entry of the departing node.

For example, change:

```
0 galaxy
1 nebula
2 saturn
```

To:

```
0 galaxy
1 nebula
```

Removing the node configuration from the CP server

After removing a node from a SFHA 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 Cluster Server 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
```

Unloading LLT and GAB and removing VCS on the departing node

On the node departing the cluster, unconfigure and unload the LLT and GAB utilities, and remove the VCS depots.

If you have configured Storage Foundation and High Availability as part of the Storage Foundation and High Availability products, you may have to delete other dependent depots before you can delete all of the following ones.

Uninstallation of Storage Foundation and High Availability products

- [Chapter 19. Uninstalling Storage Foundation and High Availability products](#)

Uninstalling Storage Foundation and High Availability products

This chapter includes the following topics:

- [Disabling VCS agents for VVR the agents on a system](#)
- [Removing the Replicated Data Set](#)
- [Uninstalling SFHA depots using the script-based installer](#)
- [Uninstalling SFHA with the Veritas Web-based installer](#)
- [Removing license files \(Optional\)](#)
- [Removing the CP server configuration using the removal script](#)
- [Removing the Storage Foundation for Databases \(SFDB\) repository after removing the product](#)
- [Stopping the AMF driver](#)

Disabling VCS agents for VVR the agents on a system

This section explains how to disable a VCS agent for VVR on a system. To disable an agent, you must change the service group containing the resource type of the agent to an OFFLINE state. Then, you can stop the application or switch the application to another system.

To disable the agents

- 1 Check whether any service group containing the resource type of the agent is online by typing the following command:

```
# hagrps -state service_group -sys system_name
```

If none of the service groups is online, skip to 3.

- 2 If the service group is online, take it offline.

To take the service group offline without bringing it online on any other system in the cluster, enter:

```
# hagrps -offline service_group -sys system_name
```

- 3 Stop the agent on the system by entering:

```
# haagent -stop agent_name -sys system_name
```

When you get the message Please look for messages in the log file, check the file `/var/VRTSvcs/log/engine_A.log` for a message confirming that each agent has stopped.

You can also use the `ps` command to confirm that the agent is stopped.

- 4 Remove the system from the `SystemList` of the service group. If you disable the agent on all the systems in the `SystemList`, you can also remove the service groups and resource types from the VCS configuration.

Read information on administering VCS from the command line.

Refer to the *Veritas Cluster Server Administrator'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.

Go on to uninstalling Volume Manager to uninstall VVR.

- 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
```

- 6 Uninstall the VVR packages.

Uninstalling SFHA depots using the script-based installer

Use the following procedure to remove SFHA products.

Not all depots 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 381.

To shut down and remove the installed SFHA depots

- 1 Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/fstab`. 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 (`VRTSvxxvm`) 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

```
# ./uninstallsf
```

For Veritas Storage Foundation High Availability

```
# ./uninstallsfha
```
- 8 The uninstall script prompts for the system name. Enter one or more system names, separated by a space, from which to uninstall SFHA, for example, `host1`:

```
Enter the system names separated by spaces from which to  
uninstall Storage Foundation: host1
```
- 9 The uninstall script prompts you to stop the product processes. If you respond yes, the processes are stopped and the depots are uninstalled.
The uninstall script creates log files and displays the location of the log files.
- 10 Most depots have kernel components. In order to ensure complete removal, a system reboot is recommended after all depots have been removed.

Uninstalling SFHA with the Veritas Web-based installer

This section describes how to uninstall Storage Foundation or Storage Foundation High Availability with the Veritas Web-based installer.

To uninstall SFHA

- 1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.
- 2 In an HA configuration, stop VCS processes on either the local system or all systems.

To stop VCS processes on the local system:

```
# hactop -local
```

To stop VCS processes on all systems:

```
# hactop -all
```

- 3 Start the Web-based installer.
See [“Starting the Veritas Web-based installer”](#) on page 71.
- 4 On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.
- 5 Select Storage Foundation or Storage Foundation High Availability from the Product drop-down list, and click **Next**.
- 6 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Validate**.
- 7 After the validation completes successfully, click **Next** to uninstall SFHA on the selected system.
- 8 If there are any processes running on the target system, the installer stops the processes. Click **Next**.
- 9 After the installer stops the processes, the installer removes the products from the specified system.
Click **Next**.
- 10 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.
- 11 Click **Finish**.
The Web-based installer prompts you for another task.

Removing license files (Optional)

Optionally, you can remove the license files.

To remove the VERITAS license files

- 1 To see what license key files you have installed on a system, enter:

```
# /sbin/vxlicrep
```

The output lists the license keys and information about their respective products.

- 2 Go to the directory containing the license key files and list them:

```
# cd /etc/vx/licenses/lic  
# ls -a
```

- 3 Using the output from step 1, identify and delete unwanted key files listed in step 2. Unwanted keys may be deleted by removing the license key file.

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 SFHA cluster is using the CP server that will have its CP server configuration removed.

A configuration utility that is part of VRTSeps 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  
vxcperv 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.

Stopping the AMF driver

If the AMF driver is loaded, stop the driver before you run the uninstallation program. Check the setting of the `AMF_START` and `AMF_STOP` attributes in the `/etc/rc.config.d/amf` file to determine if the driver is loaded. The driver is loaded if the `AMF_START` is set to 1.

To stop the AMF driver

- 1 Update the `AMF_START` and `AMF_STOP` settings in the `/etc/rc.config.d/amf` file as follows:

```
AMF_START=0
```

```
AMF_STOP=1
```

- 2 Stop the AMF driver:

```
# /sbin/init.d/amf stop
```


Installation reference

- [Appendix A. Installation scripts](#)
- [Appendix B. Response files](#)
- [Appendix C. Configuring I/O fencing using a response file](#)
- [Appendix D. Configuration files](#)
- [Appendix E. Configuring the secure shell or the remote shell for communications](#)
- [Appendix F. Storage Foundation and High Availability components](#)
- [Appendix G. Troubleshooting installation issues](#)
- [Appendix H. Troubleshooting cluster installation](#)
- [Appendix I. Sample SFHA cluster setup diagrams for CP server-based I/O fencing](#)
- [Appendix J. Configuring LLT over UDP using IPv4](#)

Installation scripts

This appendix includes the following topics:

- [About installation scripts](#)
- [Installation script options](#)

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)	<code>installvcs</code>
Veritas Storage Foundation (SF)	<code>installsf</code>
Veritas Storage Foundation and High Availability (SFHA)	<code>installsfha</code>
Veritas Storage Foundation Cluster File System (SFCFS)	<code>installsfcfs</code>
Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)	<code>installsfrac</code>
Symantec Product Authentication Service (AT)	<code>installat</code>
Veritas Dynamic Multi-pathing	<code>installdmp</code>

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 327.

Table A-1 Available command line options

Command Line Option	Function
<i>system1 system2...</i>	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.
<code>-addnode</code>	Adds a node to a high availability cluster.
<code>-allpkgs</code>	Displays all depots and patches required for the specified product. The depots 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.
<code>-comcleanup</code>	The <code>-comcleanup</code> option removes the ssh or remsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or remsh are abruptly terminated.
<code>-configure</code>	Configures the product after installation.

Table A-1 Available command line options (*continued*)

Command Line Option	Function
<p><code>-copyinstallscripts</code></p>	<p>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.</p> <p>Use this option to copy the installation scripts to an alternate rootpath when you use it with the <code>-rootpath</code> option.</p> <p>The following examples demonstrate the usage for this option:</p> <ul style="list-style-type: none"> ■ <code>./installer -copyinstallscripts</code> Copies the installation and uninstallation scripts for all products in the release to <code>/opt/VRTS/install</code>. It also copies the installation Perl libraries to <code>/opt/VRTSperl/lib/site_perl/release_name</code>. ■ <code>./installproduct_name -copyinstallscripts</code> Copies the installation and uninstallation scripts for the specified product and any subset products for the product to <code>/opt/VRTS/install</code>. It also copies the installation Perl libraries to <code>/opt/VRTSperl/lib/site_perl/release_name</code>. ■ <code>./installer -copyinstallscripts -rootpath alt_root_path</code> The path <i>alt_root_path</i> can be a directory like <code>/rdisk2</code>. In that case, this command copies installation and uninstallation scripts for all the products in the release to <code>/rdisk2/opt/VRTS/install</code>. CPI perl libraries are copied to <code>/rdisk2/opt/VRTSperl/lib/site_perl/release_name</code>, where the <i>release_name</i> is a string that starts with UXRT and includes the release version with no punctuation.
<p><code>-fencing</code></p>	<p>Configures I/O fencing in a running cluster.</p>

Table A-1 Available command line options (*continued*)

Command Line Option	Function
-hostfile <i>full_path_to_file</i>	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 depots or patches are missed on the system.
-install	The -install option is used to install products on systems.
-installallpkgs	Specifies that all depots are installed.
-installminpkgs	Specifies that the minimum depot set is installed.
-installrecpkgs	Specifies that the required depot set is installed.
-keyfile <i>ssh_key_file</i>	Specifies a key file for secure shell (SSH) installs. This option passes -i <i>ssh_key_file</i> 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 <i>log_path</i>	Specifies a directory other than /opt/VRTS/install/logs as the location where installer log files, summary files, and response files are saved.
-makeresponsefile	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 depots and patches required for the specified product. The depots and patches are listed in correct installation order. Optional depots are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See allpkgs option.

Table A-1 Available command line options (*continued*)

Command Line Option	Function
-patchpath <i>patch_path</i>	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 depots 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 depots.
-pkgpath <i>package_path</i>	Designates the path of a directory that contains all depots to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
-pkgset	Discovers and displays the depot group (minimum, recommended, all) and depots that are installed on the specified systems.
-pkgtable	Displays product's depots 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 depots and patches required for the specified product. The depots and patches are listed in correct installation order. Optional depots are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See <code>allpkgs</code> option.
-redirect	Displays progress details without showing the progress bar.

Table A-1 Available command line options (*continued*)

Command Line Option	Function
-requirements	The <code>-requirements</code> option displays required OS version, required patches, file system space, and other system requirements in order to install the product.
-responsefile <i>response_file</i>	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The <i>response_file</i> must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.
-rootpath <i>root_path</i>	Specifies an alternative root directory on which to install depots. On HP-UX operating systems, <code>-rootpath</code> passes <code>-I path</code> to <code>swinstall</code> .
-rsh	Specify this option when you want to use <code>remsh</code> and <code>rcp</code> for communication between systems instead of the default <code>ssh</code> and <code>scp</code> . See “About configuring secure shell or remote shell communication modes before installing products” on page 381.
-security	Enable or disable Symantec Product Authentication Service in a VCS cluster that is running. You can specify this option with the <code>installvcs</code> , <code>installsfha</code> or <code>installsfdfs</code> scripts. For more information about Symantec Product Authentication Service in a VCS cluster, see the <i>Veritas Cluster Server Installation Guide</i> .
-serial	Specifies that the installation script performs <code>install</code> , <code>uninstall</code> , <code>start</code> , and <code>stop</code> 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.

Table A-1 Available command line options (*continued*)

Command Line Option	Function
-stop	Stops the daemons and processes for the specified product.
-tmppath <i>tmp_path</i>	Specifies a directory other than <code>/var/tmp</code> as the working directory for the installation scripts. This destination is where initial logging is performed and where depots are copied on remote systems before installation.
-uninstall	The <code>-uninstall</code> option is used to uninstall products from systems.
-upgrade	Specifies that an existing version of the product exists and you plan to upgrade it.
-version	Checks and reports the installed products and their versions. Identifies the installed and missing depots and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing depots and patches where applicable.

Response files

This appendix includes the following topics:

- [About response files](#)
- [Installing Storage Foundation or Storage Foundation and High Availability using response files](#)
- [Configuring SFHA using response files](#)
- [Upgrading Storage Foundation or Storage Foundation and High Availability using response files](#)
- [Uninstalling Storage Foundation or Storage Foundation and High Availability using response files](#)
- [Syntax in the response file](#)
- [Response file variables to install, upgrade, or uninstall Storage Foundation or Storage Foundation and High Availability](#)
- [Response file variables to configure SFHA](#)
- [Sample response file for SFHA configuration](#)
- [Sample response file for SFHA install](#)
- [Sample response file for SF upgrade](#)
- [Sample response file for SFHA upgrade](#)

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 328.

Installing Storage Foundation or Storage Foundation and High Availability using response files

Typically, you can use the response file that the installer generates after you perform SFHA installation on one cluster to install SFHA on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To install Storage Foundation or Storage Foundation and High Availability using response files

- 1 Make sure the systems where you want to install SFHA 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 SFHA.
- 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
# ./installsf -responsefile /tmp/response_file
# ./installsfha -responsefile /tmp/response_file
```

Where `/tmp/response_file` is the response file's full path name.

Configuring SFHA using response files

Typically, you can use the response file that the installer generates after you perform SFHA configuration on one cluster to configure SFHA on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To configure SFHA using response files

- 1 Make sure the SFHA depots are installed on the systems where you want to configure SFHA.
- 2 Copy the response file to one of the cluster systems where you want to configure SFHA.
- 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 SFHA](#)” on page 342.

- 4 Start the configuration from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/installsfha -responsefile /tmp/response_file
```

Where `/tmp/response_file` is the response file's full path name.

Upgrading Storage Foundation or Storage Foundation and High Availability using response files

Typically, you can use the response file that the installer generates after you perform SFHA upgrade on one cluster to upgrade SFHA on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To perform automated Storage Foundation or Storage Foundation High Availability upgrade

- 1 Make sure the systems where you want to upgrade SFHA 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 SFHA.
- 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
# ./installsf -responsefile /tmp/response_file
# ./installsfha -responsefile /tmp/response_file
```

Where `/tmp/response_file` is the response file's full path name.

Uninstalling Storage Foundation or Storage Foundation and High Availability using response files

Typically, you can use the response file that the installer generates after you perform SFHA uninstallation on one cluster to uninstall SFHA on other clusters.

To perform an automated uninstallation

- 1 Make sure that you meet the prerequisites to uninstall SFHA.
- 2 Copy the response file to one of the cluster systems where you want to uninstall SFHA.
- 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/uninstallsf -responsefile /tmp/response_file
# /opt/VRTS/install/uninstallsfha -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 or Storage Foundation and High Availability

[Table B-1](#) lists the response file variables that you can define to configure Storage Foundation or Storage Foundation and High Availability.

Table B-1 Response file variables to specific installing, upgrading, or uninstalling Storage Foundation or Storage Foundation and High Availability

Variable	Description
CFG{opt}{install}	Installs SFHA depots. Configuration can be performed at a later time using the <code>-configure</code> option. List or scalar: scalar Optional or required: optional
CFG{accepteula}	Specifies whether you agree with the <code>EULA.pdf</code> 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

Table B-1 Response file variables to specific installing, upgrading, or uninstalling Storage Foundation or Storage Foundation and High Availability (*continued*)

Variable	Description
CFG{systemscfs}	<p>List of systems for configuration if secure environment prevents the installer to install SFHA on all systems at once.</p> <p>List or scalar: list</p> <p>Optional or required: required</p>
CFG{prod}	<p>Defines the product to be installed or uninstalled.</p> <p>List or scalar: scalar</p> <p>Optional or required: required</p>
CFG{opt}{keyfile}	<p>Defines the location of an ssh keyfile that is used to communicate with all remote systems.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{at_rootdomain}	<p>Defines the name of the system where the root broker is installed.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{opt}{patchpath}	<p>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.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{opt}{pkgpath}	<p>Defines a location, typically an NFS mount, from which all remote systems can install product depots. The location must be accessible from all target systems.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>

Table B-1 Response file variables to specific installing, upgrading, or uninstalling Storage Foundation or Storage Foundation and High Availability (*continued*)

Variable	Description
CFG{opt}{tmppath}	<p>Defines the location where a working directory is created to store temporary files and the depots that are needed during the install. The default location is <code>/var/tmp</code>.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{opt}{rsh}	<p>Defines that <code>rsh</code> must be used instead of <code>ssh</code> as the communication method between systems.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{donotinstall} {depot}	<p>Instructs the installation to not install the optional depots in the list.</p> <p>List or scalar: list</p> <p>Optional or required: optional</p>
CFG{donotremove} {depot}	<p>Instructs the uninstallation to not remove the optional depots in the list.</p> <p>List or scalar: list</p> <p>Optional or required: optional</p>
CFG{opt}{logpath}	<p>Mentions the location where the log files are to be copied. The default location is <code>/opt/VRTS/install/logs</code>.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
\$CFG{opt}{prodmode}	<p>List of modes for product</p> <p>List or scalar: list</p> <p>Optional or required: optional</p>
CFG{opt}{upgrade}	<p>Upgrades all depots installed, without configuration.</p> <p>List or scalar: list</p> <p>Optional or required: optional</p>

Table B-1 Response file variables to specific installing, upgrading, or uninstalling Storage Foundation or Storage Foundation and High Availability (*continued*)

Variable	Description
CFG{opt}{uninstall}	Uninstalls SFHA depots. List or scalar: scalar Optional or required: optional

Response file variables to configure SFHA

[Table B-2](#) lists the response file variables that you can define to configure SFHA.

Table B-2 Response file variables specific to configuring SFHA

Variable	List or Scalar	Description
CFG{opt}{configure}	Scalar	Performs the configuration if the depots are already installed. (Required)
CFG{accepteula}	Scalar	Specifies whether you agree with <code>EULA.pdf</code> 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 <code>remsh</code> must be used instead of <code>ssh</code> as the communication method between systems. (Optional)

Table B-2 Response file variables specific to configuring SFHA (*continued*)

Variable	List or Scalar	Description
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is <code>/opt/VRTS/install/logs</code> . Note: The installer copies the response files and summary files also to the specified <i>logpath</i> location. (Optional)
\$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 `smtserver`, `smtprec`, 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 SFHA cluster.

Table B-3 Response file variables specific to configuring a basic SFHA 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)

Table B-3 Response file variables specific to configuring a basic SFHA cluster
(continued)

Variable	List or Scalar	Description
CFG{vcs_allowcomms}	Scalar	Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)
\$CFG{fencingenabled}	Scalar	In a SFHA 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)

Table B-4 Response file variables specific to configuring private LLT over Ethernet (*continued*)

Variable	List or Scalar	Description
CFG{vcs_lltlinklowpri#} {"system"}	Scalar	<p>Defines a low-priority heartbeat link. Typically, lltlinklowpri is used on a public network link to provide an additional layer of communication.</p> <p>If you use different media speed for the private NICs, you can configure the NICs with lesser speed as low-priority links to enhance LLT performance. For example, lltlinklowpri1, lltlinklowpri2, and so on.</p> <p>You must enclose the system name within double quotes.</p> <p>(Optional)</p>

[Table 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	<p>Indicates whether to configure heartbeat link using LLT over UDP.</p> <p>(Required)</p>
CFG{vcs_udplink<n>_address} {<system1>}	Scalar	<p>Stores the IP address (IPv4 or IPv6) that the heartbeat link uses on node1.</p> <p>You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links.</p> <p>(Required)</p>

Table B-5 Response file variables specific to configuring LLT over UDP
(continued)

Variable	List or Scalar	Description
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)
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 SFHA cluster.

Table B-6 Response file variables specific to configuring virtual IP for SFHA 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 SFHA cluster in secure mode.

Table B-7 Response file variables specific to configuring SFHA 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. <ul style="list-style-type: none"> ■ 1—Automatic ■ 2—Semi-automatic ■ 3—Manual (Optional)

Table B-7 Response file variables specific to configuring SFHA cluster in secure mode (*continued*)

Variable	List or Scalar	Description
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)

Table B-8 Response file variables specific to configuring VCS users (*continued*)

Variable	List or Scalar	Description
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_smtprecip}	List	List of full email addresses (example: user@symantecexample.com) of SMTP recipients. (Optional)
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 SFHA global clusters.

Table B-11 Response file variables specific to configuring SFHA 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 SFHA configuration

The following example shows a response file for configuring Storage Foundation High Availability.

```
#####  
#Auto generated sfha responsefile #  
#####  
  
our %CFG;  
$CFG{accepteula}=1;  
$CFG{opt}{rsh}=1;  
$CFG{vcs_allowcomms}=1;  
$CFG{opt}{gco}=1;  
$CFG{opt}{vvr}=1;  
$CFG{opt}{prodmode}="SF Enterprise HA";  
$CFG{opt}{configure}=1;  
$CFG{prod}="SFHA51";  
$CFG{systems}=[ qw( system01 system02 ) ];  
$CFG{vm_restore_cfg}{system01}=0;  
$CFG{vm_restore_cfg}{system02}=0;  
$CFG{vcs_clusterid}=127;  
$CFG{vcs_clustername}="clus1";  
$CFG{vcs_username}=[ qw(admin operator) ];  
$CFG{vcs_userenpw}=[ qw(JlmElgLimHmmKumGlj bQOsOUUnVQoOUUnTQsOSnUQuOUUnPQtOS) ];  
$CFG{vcs_userpriv}=[ qw(Administrators Operators) ];  
$CFG{vcs_lltlink1}{system01}="lan0";  
$CFG{vcs_lltlink2}{system01}="lan1";  
$CFG{vcs_lltlink1}{system02}="lan0";  
$CFG{vcs_lltlink2}{system02}="lan1";  
$CFG{opt}{uuid}=normC;  
$CFG{opt}{logpath}="/opt/VRTS/install/logs/installsf-xxxxxx/installsf-xxxxxx.response";  
  
1;
```

Sample response file for SFHA install

The following example shows a response file for installing Storage Foundation High Availability.

```
#####  
#Auto generated sfha responsefile #  
#####
```

```

our %CFG;
$CFG{accepteula}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vvr}=1;
$CFG{opt}{prodmode}="SF Enterprise HA";
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{prod}="SFHA51";
$CFG{systems}=[ qw( system01 system02 ) ];
$CFG{keys}{system01}=["XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX"];
$CFG{keys}{system02}=["XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX"];
$CFG{opt}{uuid}=normI;
$CFG{opt}{logpath}="/opt/VRTS/install/logs/SxRT-5.1-2009-03-10a";

1;

```

Sample response file for SF upgrade

The following example shows a response file for upgrading Storage Foundation.

```

our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{upgrade}=1;
$CFG{systems}=[ qw(system01) ];

1;

```

Sample response file for SFHA upgrade

The following example shows a response file for upgrading Storage Foundation High Availability.

```

our %CFG;
$CFG{accepteula}=1;
$CFG{opt}{upgrade}=1;
$CFG{systems}=[ qw(system01 system02) ];
$CFG{vcs_allowcomms}=1;

1;

```

The `vcs_allowcomms` variable is set to 0 if it is a single-node cluster, and the `llt` and `gab` processes are not started before upgrade.

Configuring I/O fencing using a response file

This appendix includes the following topics:

- [Configuring I/O fencing using response files](#)
- [Response file variables to configure disk-based I/O fencing](#)
- [Sample response file for configuring disk-based I/O fencing](#)
- [Response file variables to configure server-based I/O fencing](#)
- [Sample response file for configuring non-SCSI3 server-based I/O fencing](#)
- [Response file variables to configure non-SCSI3 server-based I/O fencing](#)

Configuring I/O fencing using response files

Typically, you can use the response file that the installer generates after you perform I/O fencing configuration to configure I/O fencing for SFHA.

To configure I/O fencing using response files

- 1 Make sure that SFHA 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 86.

- 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 355.
 See “[Sample response file for configuring server-based I/O fencing](#)” on page 358.
- 4 Edit the values of the response file variables as necessary.
 See “[Response file variables to configure disk-based I/O fencing](#)” on page 354.
 See “[Response file variables to configure server-based I/O fencing](#)” on page 356.
- 5 Start the configuration from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/installsfha -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 SFHA.

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. <ul style="list-style-type: none"> ■ 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 354.

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

$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;

$CFG{prod}="SFHA51";

$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(c1t1d0 c2t1d0 c3t1d0) ];
$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 SFHA 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 SFHA 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 SFHA 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 SFHA 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	<p>Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not.</p> <p>Enter "0" if you do not want to configure the Coordination Point agent using the installer.</p> <p>Enter "1" if you want to use the installer to configure the Coordination Point agent.</p>
fencing_cpc_cpagentgrp	<p>Name of the service group which will have the Coordination Point agent resource as part of it.</p> <p>Note: This field is obsolete if the <code>fencing_cpc_config_cpagent</code> field is given a value of '0'.</p>
fencing_cpc_cps	<p>Virtual IP address or Virtual hostname of the CP servers.</p>
fencing_cpc_reusedg	<p>This response file field indicates whether to reuse an existing DG name for the fencing configuration in customized fencing (CP server and coordinator disks).</p> <p>Enter either a "1" or "0".</p> <p>Entering a "1" indicates reuse, and entering a "0" indicates do not reuse.</p> <p>When reusing an existing DG name for the mixed mode fencing configuration, you need to manually add a line of text, such as <code>"\$CFG{fencing_cpc_reusedg}=0"</code> or <code>"\$CFG{fencing_cpc_reusedg}=1"</code> before proceeding with a silent installation.</p>
fencing_cpc_dgname	<p>The name of the disk group to be used in the customized fencing, where at least one disk is being used.</p>

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 SFHA 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 <i>cps</i> .
fencing_cpc_ccab	The name of the authentication broker (AB) for any one of the SFHA 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}="SF51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{vxfen_config_fencing_option}=1;

```

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}="SF51";
$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 SFHA in virtual machines that do not support SCSI-3 PR” on page 26.

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.
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 <code>fencing_cpc_config_cpagent</code> 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 SFHA 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.

Table C-3 Non-SCSI3 server-based I/O fencing response file definitions
(continued)

Response file field	Definition
CFG {fencing_cpc_ports}	The port of the CP server that is denoted by <i>cps</i> .
CFG {fencing_cpc_ccab}	The name of the authentication broker (AB) for any one of the SFHA 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.
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.

Configuration files

This appendix includes the following topics:

- [About the LLT and GAB configuration files](#)
- [About the AMF configuration files](#)
- [About the VCS configuration files](#)
- [About I/O fencing configuration files](#)
- [Sample configuration files for CP server](#)

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 D-1](#) lists the LLT configuration files and the information that these files contain.

Table D-1 LLT configuration files

File	Description
/etc/rc.config.d/lltconf	<p>This file stores the start and stop environment variables for LLT:</p> <ul style="list-style-type: none"> ■ LLT_START—Defines the startup behavior for the LLT module after a system reboot. Valid values include: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 1—Indicates that LLT is enabled to shut down. 0—Indicates that LLT is disabled to shut down. <p>The installer sets the value of these variables to 1 at the end of SFHA configuration.</p>
/etc/llthosts	<p>The file <code>llthosts</code> 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.</p> <p>For example, the file <code>/etc/llthosts</code> contains the entries that resemble:</p> <pre>0 galaxy 1 nebula</pre>
/etc/llttab	<p>The file <code>llttab</code> contains the information that is derived during installation and used by the utility <code>lltconfig(1M)</code>. After installation, this file lists the LLT network links that correspond to the specific system.</p> <p>For example, the file <code>/etc/llttab</code> contains the entries that resemble:</p> <pre>set-node galaxy set-cluster 2 link lan1 /dev/lan:1 - ether - - link lan2 /dev/lan:2 - ether - -</pre> <p>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 <code>link</code> command. These lines identify the two network cards that the LLT protocol uses.</p> <p>If you configured a low priority link under LLT, the file also includes a "link-lowpri" line.</p> <p>Refer to the <code>llttab(4)</code> manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the <code>llttab</code> file.</p>

Table D-2 lists the GAB configuration files and the information that these files contain.

Table D-2 GAB configuration files

File	Description
/etc/rc.config.d/ gabconf	<p>This file stores the start and stop environment variables for GAB:</p> <ul style="list-style-type: none"> ■ GAB_START—Defines the startup behavior for the GAB module after a system reboot. Valid values include: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 1—Indicates that GAB is enabled to shut down. 0—Indicates that GAB is disabled to shut down. <p>The installer sets the value of these variables to 1 at the end of SFHA configuration.</p>
/etc/gabtab	<p>After you install SFHA, the file /etc/gabtab contains a <code>gabconfig (1)</code> command that configures the GAB driver for use.</p> <p>The file /etc/gabtab contains a line that resembles:</p> <pre style="margin-left: 40px;">/sbin/gabconfig -c -nN</pre> <p>The <code>-c</code> option configures the driver for use. The <code>-nN</code> specifies that the cluster is not formed until at least <i>N</i> nodes are ready to form the cluster. Symantec recommends that you set <i>N</i> to be the total number of nodes in the cluster.</p> <p>Note: Symantec does not recommend the use of the <code>-c -x</code> option for <code>/sbin/gabconfig</code>. Using <code>-c -x</code> can lead to a split-brain condition.</p>

About the AMF configuration files

Asynchronous Monitoring Framework (AMF) kernel driver provides asynchronous event notifications to the VCS agents that are enabled for intelligent resource monitoring.

[Table D-3](#) lists the AMF configuration files.

Table D-3 AMF configuration files

File	Description
<code>/etc/rc.config.d/amfconf</code>	<p>This file stores the start and stop environment variables for AMF:</p> <ul style="list-style-type: none"> ■ AMF_START—Defines the startup behavior for the AMF module after a system reboot or when AMF is attempted to start using the init script. Valid values include: <ul style="list-style-type: none"> 1—Indicates that AMF is enabled to start up. 0—Indicates that AMF is disabled to start up. (default) ■ AMF_STOP—Defines the shutdown behavior for the AMF module during a system shutdown or when AMF is attempted to stop using the init script. Valid values include: <ul style="list-style-type: none"> 1—Indicates that AMF is enabled to shut down. (default) 0—Indicates that AMF is disabled to shut down.
<code>/etc/amftab</code>	<p>After you install VCS, the file <code>/etc/amftab</code> contains a <code>amfconfig(1)</code> command that configures the AMF driver for use.</p> <p>The AMF init script uses this <code>/etc/amftab</code> file to configure the AMF driver. The <code>/etc/amftab</code> file contains the following line by default:</p> <pre><code>/opt/VRTSamf/bin/amfconfig -c</code></pre>

About the VCS configuration files

VCS configuration files include the following:

- `main.cf`
The installer creates the VCS configuration file in the `/etc/VRTSvcs/conf/config` folder by default during the SFHA configuration. The `main.cf` file contains the minimum information that defines the cluster and its nodes.
See [“Sample main.cf file for VCS clusters”](#) on page 368.
See [“Sample main.cf file for global clusters”](#) on page 370.
- `types.cf`
The file `types.cf`, which is listed in the include statement in the `main.cf` file, defines the VCS bundled types for VCS resources. The file `types.cf` is also located in the folder `/etc/VRTSvcs/conf/config`.
Additional files similar to `types.cf` may be present if agents have been added, such as `OracleTypes.cf`.

- `/etc/rc.config.d/vcsconf`

This file stores the start and stop environment variables for VCS engine:

- **VCS_START**—Defines the startup behavior for VCS engine after a system reboot. Valid values include:
 - 1—Indicates that VCS engine is enabled to start up.
 - 0—Indicates that VCS engine is disabled to start up.
- **VCS_STOP**—Defines the shutdown behavior for VCS engine during a system shutdown. Valid values include:
 - 1—Indicates that VCS engine is enabled to shut down.
 - 0—Indicates that VCS engine is disabled to shut down.

The installer sets the value of these variables to 1 at the end of SFHA configuration.

Note the following information about the VCS configuration file after installing and configuring VCS:

- The cluster definition includes the cluster information that you provided during the configuration. This definition includes the cluster name, cluster address, and the names of users and administrators of the cluster. Notice that the cluster has an attribute `UserNames`. The `installsfha` creates a user "admin" whose password is encrypted; the word "password" is the default password.
- If you set up the optional I/O fencing feature for VCS, then the `UseFence = SCSI3` attribute is present.
- If you configured the cluster in secure mode, the `main.cf` includes the `VxSS` service group and "`SecureClus = 1`" cluster attribute.
- The `installsfha` creates the `ClusterService` service group if you configured the virtual IP, SMTP, SNMP, or global cluster options.

The service group also has the following characteristics:

- The group includes the IP and NIC resources.
- The service group also includes the notifier resource configuration, which is based on your input to `installsfha` prompts about notification.
- The `installsfha` also creates a resource dependency tree.
- If you set up global clusters, the `ClusterService` service group contains an Application resource, `wac` (wide-area connector). This resource's attributes contain definitions for controlling the cluster in a global cluster environment.

Refer to the *Veritas Cluster Server Administrator's Guide* for information about managing VCS global clusters.

Refer to the *Veritas Cluster Server Administrator's Guide* to review the configuration concepts, and descriptions of `main.cf` and `types.cf` files for HP-UX systems.

Sample `main.cf` file for VCS clusters

The following sample `main.cf` file is for a cluster in secure mode.

```
include "types.cf"
include "OracleTypes.cf"
include "OracleASMTypes.cf"
include "Db2udbTypes.cf"
include "SybaseTypes.cf"

cluster vcs_cluster2 (
    UserNames = { admin = cDRpdXpmHpzS, smith = dKLhKJkHLh }
    ClusterAddress = "192.168.1.16"
    Administrators = { admin, smith }
    CounterInterval = 5
    SecureClus = 1
)

system galaxy (
)

system nebula (
)

group ClusterService (
    SystemList = { galaxy = 0, nebula = 1 }
    UserStrGlobal = "LocalCluster@https://10.182.2.76:8443;"
    AutoStartList = { galaxy, nebula }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

IP webip (
    Device = lan0
    Address = "192.168.1.16"
    NetMask = "255.255.240.0"
)
```

```
NIC csgnic (
    Device = lan0
    NetworkHosts = { "192.168.1.17", "192.168.1.18" }
)

NotifierMngr ntfr (
    SnmpConsoles = { "saturn" = Error, "jupiter" = SevereError }
    SntpServer = "smtp.example.com"
    SntpRecipients = { "ozzie@example.com" = Warning,
                      "harriet@example.com" = Error }
)

webip requires csgnic
ntfr requires csgnic

// resource dependency tree
//
//     group ClusterService
//     {
//     NotifierMngr ntfr
//         {
//         NIC csgnic
//         }
//     }
// }

group VxSS (
    SystemList = { galaxy = 0, nebula = 1 }
    Parallel = 1
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

Phantom phantom_vxss (
)

ProcessOnOnly vxatd (
    IgnoreArgs = 1
    PathName = "/opt/VRTSat/bin/vxatd"
)

```

```
// resource dependency tree
//
// group VxSS
// {
//   Phantom phantom_vxss
//   ProcessOnOnly vxatd
// }
```

Sample main.cf file for global clusters

If you installed SFHA with the Global Cluster option, note that the ClusterService group also contains the Application resource, wac. The wac resource is required to control the cluster in a global cluster environment.

```
.
.
group ClusterService (
    SystemList = { galaxy = 0, nebula = 1 }

    UserStrGlobal = "LocalCluster@https://10.182.2.78:8443;"

    AutoStartList = { galaxy, nebula }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

Application wac (
    StartProgram = "/opt/VRTSvcs/bin/wacstart"
    StopProgram = "/opt/VRTSvcs/bin/wacstop"
    MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
    RestartLimit = 3
)
.
.
```

In the following main.cf file example, bold text highlights global cluster specific entries.

```
include "types.cf"

cluster vcs03 (
    ClusterAddress = "10.182.13.50"
    SecureClus = 1
)
```

```
system sysA (
)

system sysB (
)

system sysC (
)

group ClusterService (
    SystemList = { sysA = 0, sysB = 1, sysC = 2 }
    AutoStartList = { sysA, sysB, sysC }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

Application wac (
    StartProgram = "/opt/VRTSvcs/bin/wacstart"
    StopProgram = "/opt/VRTSvcs/bin/wacstop"
    MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
    RestartLimit = 3
)

IP gcoip (
    Device = lan0
    Address = "10.182.13.50"
    NetMask = "255.255.240.0"
)

NIC csgnic (
    Device = lan0
)

NotifierMngr ntfr (
    SnmpConsoles = { jupiter" = SevereError }
    Smtperver = "smtp.example.com"
    Smtpercipients = { "ozzie@example.com" = SevereError }
)

gcoip requires csgnic
ntfr requires csgnic
wac requires gcoip
```

```

// resource dependency tree
//
//   group ClusterService
//   {
//     NotifierMngr ntr
//     {
//       NIC csgnic
//     }
//     Application wac
//     {
//       IP gcoip
//       {
//         NIC csgnic
//       }
//     }
//   }

group VxSS (
    SystemList = { sysA = 0, sysB = 1, sysC = 2 }
    Parallel = 1
    AutoStartList = { sysA, sysB, sysC }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

Phantom phantom_vxss (
)

ProcessOnOnly vxatd (
    IgnoreArgs = 1
    PathName = "/opt/VRTSat/bin/vxatd"
)

// resource dependency tree
//
//   group VxSS
//   {
//     Phantom phantom_vxss
//     ProcessOnOnly vxatd
//   }

```

About I/O fencing configuration files

[Table D-4](#) lists the I/O fencing configuration files.

Table D-4 I/O fencing configuration files

File	Description
/etc/rc.config.d/vxfenconf	<p>This file stores the start and stop environment variables for I/O fencing:</p> <ul style="list-style-type: none"> ■ VXFEN_START—Defines the startup behavior for the I/O fencing module after a system reboot. Valid values include: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 1—Indicates that I/O fencing is enabled to shut down. 0—Indicates that I/O fencing is disabled to shut down. <p>The installer sets the value of these variables to 1 at the end of SFHA configuration.</p>
/etc/vxfendg	<p>This file includes the coordinator disk group information.</p> <p>This file is not applicable for server-based fencing.</p>

Table D-4 I/O fencing configuration files (*continued*)

File	Description
/etc/vxfenmode	<p>This file contains the following parameters:</p> <ul style="list-style-type: none"> ■ vxfen_mode <ul style="list-style-type: none"> ■ 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 You must configure the vxfen module to use DMP devices or iSCSI devices, and set the SCSI-3 disk policy as dmp. ■ 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 SFHA 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 D-4 I/O fencing configuration files (*continued*)

File	Description
<code>/etc/vxfentab</code>	<p>When I/O fencing starts, the vxfen startup script creates this <code>/etc/vxfentab</code> file on each node. The startup script uses the contents of the <code>/etc/vxfendg</code> and <code>/etc/vxfenmode</code> files. Any time a system is rebooted, the fencing driver reinitializes the <code>vxfentab</code> file with the current list of all the coordinator points.</p> <p>Note: The <code>/etc/vxfentab</code> file is a generated file; do not modify this file.</p> <p>An example of the <code>/etc/vxfentab</code> file in a disk-based fencing configuration on one node resembles as follows:</p> <pre style="margin-left: 20px;">/dev/vx/rdmp/clt1d0 /dev/vx/rdmp/c2t1d0 /dev/vx/rdmp/c3t1d0</pre> <p>For server-based fencing, the <code>/etc/vxfentab</code> file also includes the security settings information.</p> <p>For server-based fencing with single CP server, the <code>/etc/vxfentab</code> file also includes the <code>single_cp</code> settings information.</p>

Sample configuration files for CP server

The following are example `main.cf` files for a CP server that is hosted on a single node, and a CP server that is hosted on an SFHA cluster.

- The `main.cf` file for a CP server that is hosted on a single node:
 See [“Sample main.cf file for CP server hosted on a single node that runs VCS”](#) on page 375.
- The `main.cf` file for a CP server that is hosted on an SFHA cluster:
 See [“Sample main.cf file for CP server hosted on a two-node SFHA cluster”](#) on page 378.

Note: The CP server supports Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with SFHA clusters. The following example `main.cf` files use IPv4 addresses.

Sample `main.cf` file for CP server hosted on a single node that runs VCS

The following is an example of a single CP server node `main.cf`.

For this CP server single node main.cf, note the following values:

- Cluster name: cps1
- Node name: mycps1

```
include "types.cf"

// cluster name: cps1
// CP server: mycps1

cluster cps1 (
    UserNames = { admin = bMNFmHmJNiNNlVNhMK, haris = fopKojNvpHouNn,
                 "mycps1.symantecexample.com@root@vx" = aj,
                 "root@mycps1.symantecexample.com" = hq }
    Administrators = { admin, haris,
                      "mycps1.symantecexample.com@root@vx",
                      "root@mycps1.symantecexample.com" }
    SecureClus = 1
    HacliUserLevel = COMMANDROOT
)

system mycps1 (
)

group CPSSG (
    SystemList = { mycps1 = 0 }
    AutoStartList = { mycps1 }
)

IP cpsvip (
    Device @mycps1 = lan0
    Address = "10.209.3.1"
    NetMask = "255.255.252.0"
)

NIC cpsnic (
    Device @mycps1 = lan0
)

Process vxcpserv (
    PathName = "/opt/VRTScps/bin/vxcpserv"
    ConfInterval = 30
    RestartLimit = 3
)
```

```

        )

cpsvip requires cpsnic
vxcpsserv requires cpsvip

// resource dependency tree
//
// group CPSSG
// {
// Process vxcpsserv
//     {
//     IP cpsvip
//         {
//         NIC cpsnic
//         }
//     }
// }

group VxSS (
    SystemList = { mycps1 = 0 }
    Parallel = 1
    AutoStartList = { mycps1 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

Phantom phantom_vxss (
)

ProcessOnOnly vxatd (
    IgnoreArgs = 1
    PathName = "/opt/VRTSat/bin/vxatd"
)

// resource dependency tree
//
// group VxSS
// {
// Phantom phantom_vxss

```

```
// ProcessOnOnly vxatd
// }
```

Sample main.cf file for CP server hosted on a two-node SFHA cluster

The following is an example of a main.cf, where the CP server is hosted on an SFHA cluster.

For this CP server hosted on an SFHA cluster main.cf, note the following values:

- Cluster name: cps1
- Nodes in the cluster: mycps1, mycps2

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"

// cluster: cps1
// CP servers:
// mycps1
// mycps2

cluster cps1 (
    UserNames = { admin = ajkCjeJgkFkkIskEjh,
                  "mycps1.symantecexample.com@root@vx" = JK,
                  "mycps2.symantecexample.com@root@vx" = dl }
    Administrators = { admin, "mycps1.symantecexample.com@root@vx",
                       "mycps2.symantecexample.com@root@vx" }
    SecureClus = 1
)

system mycps1 (
)

system mycps2 (
)

group CPSSG (
    SystemList = { mycps1 = 0, mycps2 = 1 }
    AutoStartList = { mycps1, mycps2 } )

DiskGroup cpsdg (
    DiskGroup = cps_dg
```

```

    )

IP cpsvip (
    Device @mycps1 = lan0
    Device @mycps2 = lan0
    Address = "10.209.81.88"
    NetMask = "255.255.252.0"
)

Mount cpsmount (
    MountPoint = "/etc/VRTScps/db"
    BlockDevice = "/dev/vx/dsk/cps_dg/cps_volume"
    FSType = vxfs
    FsckOpt = "-y"
)

NIC cpsnic (
    Device @mycps1 = lan0
    Device @mycps2 = lan0
)

Process vxcpserv (
    PathName = "/opt/VRTScps/bin/vxcpserv"
)

Volume cpsvol (
    Volume = cps_volume
    DiskGroup = cps_dg
)

cpsmount requires cpsvol
cpsvip requires cpsnic
cpsvol requires cpsdg
vxcpserv requires cpsmount
vxcpserv requires cpsvip

// resource dependency tree
//
// group CPSSG
// {
// Process vxcpserv
//     {

```

```
//      Mount cpsmount
//      {
//      Volume cpsvol
//      {
//      DiskGroup cpsdg
//      }
//      }
//      IP cpsvip
//      {
//      NIC cpsnic
//      }
//      }
// }

group VxSS (
    SystemList = { mycps1 = 0, mycps2 = 1 }
    Parallel = 1
    AutoStartList = { mycps1, mycps2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

Phantom phantom_vxss (
)

ProcessOnOnly vxatd (
    IgnoreArgs = 1
    PathName = "/opt/VRTSat/bin/vxatd"
)

// resource dependency tree
//
// group VxSS
// {
// Phantom phantom_vxss
// ProcessOnOnly vxatd
// }
```

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](#)
- [Configuring and enabling ssh](#)
- [Enabling remsh](#)

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 `remsh` (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 (`remsh`). Symantec recommends that you use `ssh` as it is more secure than `remsh`.

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.

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 Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems (system2 in this example).

To enable SFTP, the `/opt/ssh/etc/sshd_config` file must contain the following two lines:

```
PermitRootLogin          yes
Subsystem sftp            /opt/ssh/libexec/sftp-server
```

- 2 If the lines are not there, add them and restart ssh:

```
system1 # /sbin/init.d/secsh start
```

- 3 From the source system (system1), move the public key to a temporary file on the target system (system2).

Use the secure file transfer program.

In this example, the file name `id_dsa.pub` in the root directory is the name for the temporary file for the public key.

Use the following command for secure file transfer:

```
system1 # sftp system2
```

If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

```
Connecting to system2 ...  
The authenticity of host 'system2 (10.182.00.00)'  
can't be established. DSA key fingerprint is  
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.  
Are you sure you want to continue connecting (yes/no)?
```

- 4 Enter `yes`.

Output similar to the following is displayed:

```
Warning: Permanently added 'system2,10.182.00.00'  
(DSA) to the list of known hosts.  
root@system2 password:
```

- 5 Enter the root password of system2.
- 6 At the `sftp` prompt, type the following command:

```
sftp> put /.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /.ssh/id_dsa.pub to /id_dsa.pub
```

- 7 To quit the SFTP session, type the following command:

```
sftp> quit
```

- 8** To begin the `ssh` session on the target system (system2 in this example), type the following command on system1:

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

- 9** After you log in to system2, enter the following command to append the `id_dsa.pub` file to the `authorized_keys` file:

```
system2 # cat /id_dsa.pub >> /.ssh/authorized_keys
```

- 10** After the `id_dsa.pub` public key file is copied to the target system (system2), and added to the authorized keys file, delete it. To delete the `id_dsa.pub` public key file, enter the following command on system2:

```
system2 # rm /id_dsa.pub
```

- 11** To log out of the `ssh` session, enter the following command:

```
system2 # exit
```

- 12** When you install from a source system that is also an installation target, also add the local system `id_dsa.pub` key to the local `authorized_keys` file. The installation can fail if the installation source system is not authenticated.

To add the local system `id_dsa.pub` key to the local `authorized_keys` file, enter the following command:

```
system1 # cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys
```

- 13** Run the following commands on the source installation system. If your `ssh` session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and make the key globally available to the user `root`:

```
system1 # exec /usr/bin/ssh-agent $SHELL
system1 # ssh-add
```

```
Identity added: //./ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

To verify that you can connect to a target system

- 1 On the source system (system1), enter the following command:

```
system1 # ssh -l root system2 uname -a
```

where system2 is the name of the target system.

- 2 The command should execute from the source system (system1) to the target system (system2) without the system requesting a passphrase or password.
- 3 Repeat this procedure for each target system.

Enabling remsh

Remote shell functionality is enabled automatically after installing HP-UX .

Typically, the only requirement to enable remote installations is to modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. You must modify this file for each user who remotely accesses the system using `remsh`. Each line of the `.rhosts` file must contain a fully qualified domain name or IP address for each remote system that has access to the local system. For example, if the root user must remotely access `system1` from `system2`, add an entry for `system2.companyname.com` to the `.rhosts` file on `system1`.

```
# echo "system2.companyname.com" >> $HOME/.rhosts
```

After you complete an installation procedure, delete the `.rhosts` file from each user's `$HOME` directory to ensure security:

```
# rm -f $HOME/.rhosts
```

For more information on configuring the remote shell, see the operating system documentation and the `remsh(1M)` manual page.

Storage Foundation and High Availability components

This appendix includes the following topics:

- [Storage Foundation and High Availability installation depots](#)
- [Veritas Cluster Server installation depots](#)
- [Veritas Storage Foundation obsolete and reorganized installation depots](#)

Storage Foundation and High Availability installation depots

[Table F-1](#) shows the depot name and contents for each English language depot for Storage Foundation and High Availability. The table also gives you guidelines for which depots to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Storage Foundation and High Availability and Veritas Cluster Server (VCS) depots, the combined functionality is called Storage Foundation and High Availability and High Availability.

See “[Veritas Cluster Server installation depots](#)” on page 389.

Table F-1 Storage Foundation and High Availability depots

depots	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 depot 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
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 F-1 Storage Foundation and High Availability depots (*continued*)

depots	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 depot 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 depots

[Table F-2](#) shows the depot name and contents for each English language depot for Veritas Cluster Server (VCS). The table also gives you guidelines for which depots to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Storage Foundation and VCS depots, the combined functionality is called Storage Foundation and High Availability.

See “[Storage Foundation and High Availability installation depots](#)” on page 387.

Table F-2 VCS installation depots

depot	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
VRTSvc	Veritas Cluster Server	Minimum
VRTSvcsg	Veritas Cluster Server Bundled Agents	Minimum
VRTSvcxfen	Veritas I/O Fencing	Minimum
VRTSvcsea	Consolidated database and enterprise agent depots	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 Storage Foundation obsolete and reorganized installation depots

[Table F-3](#) lists the depots that are obsolete or reorganized for Storage Foundation and Storage Foundation High Availability.

Table F-3 Veritas Storage Foundation obsolete and reorganized depots

depot	Description
Infrastructure	
SYMClma	Obsolete
VRTSaa	Included in VRTSsfmh

Table F-3 Veritas Storage Foundation obsolete and reorganized depots
(continued)

depot	Description
VRTSccg	Included in VRTSsfmh
VRTSdbms3	Obsolete
VRTSicsco	Obsolete
VRTSjre	Obsolete
VRTSjre15	Obsolete
VRTSmh	Included in VRTSsfmh
VRTSobc33	Obsolete
VRTSobgui	Obsolete
VRTSpbx	Obsolete
VRTSsfm	Obsolete
VRTSweb	Obsolete
Product depots	
VRTSacclib	<p>Obsolete</p> <p>The following information is for installations, upgrades, and uninstalls using the script- or Web-based installer.</p> <ul style="list-style-type: none"> ■ For fresh installations VRTSacclib is not installed. ■ For upgrades, VRTSacclib is not uninstalled. ■ For uninstalls, VRTSacclib is not uninstalled.
VRTSalloc	Obsolete
VRTScmccc	Obsolete
VRTScmcs	Obsolete
VRTScscm	Obsolete
VRTScscw	Obsolete
VRTScsocw	Obsolete

Table F-3 Veritas Storage Foundation obsolete and reorganized depots
(continued)

depot	Description
VRTScssim	Obsolete
VRTScutil	Obsolete
VRTSdcli	Obsolete
VRTSddlpr	Obsolete
VRTSdsa	Obsolete
VRTSfsman	Included in mainpkg
VRTSfsmnd	Included in mainpkg
VRTSfspro	Included in VRTSsfmh
VRTSvcldb	Included in VRTSvcsea
VRTSvcsor	Included in VRTSvcsea
VRTSvcsvr	Included in VRTSvc
VRTSvdid	Obsolete
VRTSvmman	Included in mainpkg
VRTSvmpro	Included in VRTSsfmh
VRTSvrpro	Included in VRTSob
VRTSvrw	Obsolete
VRTSvxmsa	Obsolete
Documentation	All Documentation depots obsolete

Troubleshooting installation issues

This appendix includes the following topics:

- [Restarting the installer after a failed connection](#)
- [What to do if you see a licensing reminder](#)
- [Incorrect permissions for root on remote system](#)
- [Resource temporarily unavailable](#)
- [Inaccessible system](#)
- [Upgrading Veritas Storage Foundation for Databases \(SFDB\) tools from 5.0MP2 to 5.1SP1 \(2003131\)](#)
- [Upgrading Veritas Storage Foundation for Databases \(SFDB\) tools from 5.0.x to 5.1SP1 \(2184482\)](#)

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 46.

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>

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.

```
Checking ssh communication with system01 ..... permission denied
installer requires that ssh commands used between systems execute without
prompting for passwords or confirmations. Please run installer again with
the ssh configured for password free logins, or configure rsh and use the
-rsh option.
```

```
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 381.

Note: Remove remote shell permissions after completing the SFHA 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 `nkthread` tunable parameter may not be large enough. The `nkthread` tunable requires a minimum value of 600 on all systems in the cluster. To determine the current value of `nkthread`, enter:

```
# kctune -q nkthread
```

If necessary, you can change the value of `nkthread` using the SAM (System Administration Manager) interface, or by running the `kctune` command. If you change the value of `nkthread`, the kernel must be rebuilt for the new value to take effect. It is easier to change the value using SAM because there is an option to process the new kernel immediately.

See the `kctune(1M)` and `sam(1M)` 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.

```
Checking communication with system01 ..... FAILED
  System not accessible : system01

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 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.

If a system cannot access the software source depot, either `swagentd` is not running on the target system or the `swlist` command cannot see the source depot.

```
Correct /etc/{hosts, nsswitch.conf} and continue from here
Continue? [Y/N] :
```

Suggested solutions: check that `swagentd` is running. Check whether there is an entry for the target system in `/etc/hosts`. If there is no entry, then ensure the `hosts` file is not the primary lookup for the "hosts" entry.

Upgrading Veritas Storage Foundation for Databases (SFDB) tools from 5.0MP2 to 5.1SP1 (2003131)

While upgrading from 50mp2 to 51SP1 the following error message could be seen when running `sfua_rept_migrate`:

```
# /opt/VRTSdbed/migrate/sfua_rept_migrate
Mounting SFUA Sybase ASA repository.
SFORA sfua_rept_migrate ERROR V-81-8903 Could not start repository database
/usr/lib/dld.sl: Can't find path for shared library: libcur_colr.1
/usr/lib/dld.sl: No such file or directory
sh: 3845 Abort(coredump)
Symantec DBMS 3.0.85.0 vxdbsms_start_db utility
ASA failed. Sybase ASA error code: [134].
Sybase ASA Error text: {{{}}}
```

SFORA sfua_rept_migrate ERROR V-81-9160 Failed to mount repository.

Workaround

To upgrade without an existing SFDB repository set up

- 1 Verify X/Open curses is installed on the system.
- 2 Create the following link: `ln -s /usr/lib/libxcurses.1 /usr/lib/libcur_colr.1`
- 3 Run:

```
# sfua_rept_migrate
```

Upgrading Veritas Storage Foundation for Databases (SFDB) tools from 5.0.x to 5.1SP1 (2184482)

When upgrading from SFHA version 5.0 or 5.0.1 to SFHA 5.1SP1 the `S*vxdbsms3` startup script is renamed to `NO_S*vxdbsms3`. The `S*vxdbsms3` startup script is required by `sfua_rept_upgrade`. Thus when `sfua_rept_upgrade` is run, it is unable to find the `S*vxdbsms3` startup script and gives the error message:

```
/sbin/rc3.d/S*vxdbsms3 not found
SFORA sfua_rept_migrate ERROR V-81-3558 File: is missing.
SFORA sfua_rept_migrate ERROR V-81-9160 Failed to mount repository.
```

Workaround

Before running `sfua_rept_migrate`, rename the startup script `NO_S*vxdbms3` to `S*vxdbms3`.

Troubleshooting cluster installation

This appendix includes the following topics:

- [Unmount failures](#)
- [Command failures](#)
- [Installer cannot create UUID for the cluster](#)
- [The vxfsentsthdw utility fails when SCSI TEST UNIT READY command fails](#)
- [Troubleshooting server-based I/O fencing](#)
- [Troubleshooting server-based fencing on the SFHA cluster nodes](#)
- [Troubleshooting server-based I/O fencing in mixed mode](#)
- [After upgrading from 5.0.x and before migrating SFDB](#)

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.

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 56.

- 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.

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 SFHA configuration, upgrade, or when you add a node to the cluster using the installer.

Workaround: To start SFHA, 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 `vxfcntlsthdw` utility fails when `SCSI TEST UNIT READY` command fails

While running the `vxfcntlsthdw` 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 `vxcperv` process fails on the CP server, then review the following diagnostic files:
 - `/var/VRTScps/diag/FFDC_CPS_pid_vxcperv.log`
 - `/var/VRTScps/diag/stack_pid_vxcperv.txt`

Note: If the `vxcperv` process fails on the CP server, these files are present in addition to a core file. VCS restarts `vxcperv` 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 SFHA cluster (client cluster) node.

See [“Troubleshooting issues related to the CP server service group”](#) on page 401.

See [“Checking the connectivity of CP server”](#) on page 402.

See [“Issues during fencing startup on SFHA cluster nodes set up for server-based fencing”](#) on page 403.

See [“Issues during online migration of coordination points”](#) on page 405.

See [“Troubleshooting server-based I/O fencing in mixed mode”](#) on page 406.

See [“Checking keys on coordination points when `vxfen_mechanism` value is set to `cps`”](#) on page 410.

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 SFHA 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 SFHA 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 SFHA cluster (client cluster) node.

Issues during fencing startup on SFHA cluster nodes set up for server-based fencing

Table H-1 Fencing startup issues on SFHA cluster (client cluster) nodes

Issue	Description and resolution
<p><code>cpsadm</code> command on the SFHA cluster gives connection error</p>	<p>If you receive a connection error message after issuing the <code>cpsadm</code> command on the SFHA cluster, perform the following actions:</p> <ul style="list-style-type: none"> ■ Ensure that the CP server is reachable from all the SFHA cluster nodes. ■ Check that the SFHA cluster nodes use the correct CP server virtual IP or virtual hostname and the correct port number. Check the <code>/etc/vxfenmode</code> file. ■ Ensure that the running CP server is using the same virtual IP/virtual hostname and port number.
<p>Authorization failure</p>	<p>Authorization failure occurs when the CP server's nodes or users are not added in the CP server configuration. Therefore, fencing on the SFHA 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.</p> <p>To resolve this issue, add the CP server node and user in the CP server configuration and restart fencing.</p> <p>See “Preparing the CP servers manually for use by the SFHA cluster” on page 173.</p>

Table H-1 Fencing startup issues on SFHA cluster (client cluster) nodes
(continued)

Issue	Description and resolution
Authentication failure	<p>If you had configured secure communication between the CP server and the SFHA cluster (client cluster) nodes, authentication failure can occur due to the following causes:</p> <ul style="list-style-type: none"> ■ Symantec Product Authentication Services (AT) is not properly configured on the CP server and/or the SFHA cluster. ■ The CP server and the SFHA cluster nodes use the same root broker but the certificate hash of the root broker is not same on the SFHA cluster and the CP server. Run the following command on both the CP server and the SFHA cluster to see the certificate hash: <pre># cpsat showalltrustedcreds</pre> ■ The CP server and the SFHA cluster nodes use different root brokers, and trust is not established between the authentication brokers: ■ The hostname of the SFHA cluster nodes is not the same hostname used when configuring AT. <p>The hostname of the SFHA cluster nodes must be set to the hostname used when configuring AT. You can view the fully qualified hostname registered with AT using the <code>cpsat showcred</code> command. After entering this command, the hostname appears in the User Name field.</p> ■ The CP server and SFHA cluster do not have the same security setting. <p>In order to configure secure communication, both the CP server and the SFHA cluster must have same security setting.</p> <p>In order to have the same security setting, the security parameter must have same value in the <code>/etc/vxcps.conf</code> file on CP server and in the <code>/etc/vxfenmode</code> file on the SFHA cluster (client cluster) nodes.</p>

Table H-1 Fencing startup issues on SFHA cluster (client cluster) nodes
(continued)

Issue	Description and resolution
Preexisting split-brain	<p>Assume the following situations to understand preexisting split-brain in server-based fencing:</p> <ul style="list-style-type: none"> ■ 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 SFHA 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. <p>These situations are similar to that of preexisting split-brain with coordinator disks, where the problem is solved by the administrator running the <code>vxfenclearpre</code> command. A similar solution is required in server-based fencing using the <code>cpsadm</code> command.</p> <p>Run the <code>cpsadm</code> command to clear a registration on a CP server:</p> <pre># cpsadm -s cp_server -a unreg_node -c cluster_name -n nodeid</pre> <p>where <code>cp_server</code> is the virtual IP address or virtual hostname on which the CP server is listening, <code>cluster_name</code> is the VCS name for the SFHA cluster, and <code>nodeid</code> specifies the node id of SFHA cluster node. Ensure that fencing is not already running on a node before clearing its registration on the CP server.</p> <p>After removing all stale registrations, the joiner node will be able to join the cluster.</p>

Issues during online migration of coordination points

During online migration of coordination points using the `vxfen` 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 SFHA 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 SFHA 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 SFHA cluster nodes to the CP server(s).
- Cluster, nodes, or users for the SFHA 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 SFHA 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 SFHA 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 SFHA cluster nodes:

```
# cat /etc/vxfenmode

vxfen_mode=customized
vxfen_mechanism=cps
scsi3_disk_policy=dmp
security=0
cps1=[10.140.94.101]:14250
vxfendg=vxfencoordg
```

- 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 SFHA 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 SFHA 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 SFHA 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 SFHA cluster.

After upgrading from 5.0.x and before migrating SFDB

When upgrading from SFHA version 5.0 or 5.0.1 to SFHA 5.1 SP1 the S*vxdms3 startup script is renamed to NO_S*vxdms3. The S*vxdms3 startup script is required by sfua_rept_migrate. Thus when sfua_rept_migrate is run, it is unable to find the S*vxdms3 startup script and gives the error message:

```
/sbin/rc3.d/S*vxdms3 not found
SFORA sfua_rept_migrate ERROR V-81-3558 File: is missing.
SFORA sfua_rept_migrate ERROR V-81-9160 Failed to mount repository.
```

To prevent S*vxdms3 startup script error

- ◆ Rename the startup script NO_S*vxdms3 to S*vxdms3.

When upgrading SFDB tools from the previous release in an HP Service Guard environment, first verify that the `cmviewcl` command can be executed by a non-root user. This permission change must be done before executing SFDB upgrade commands.

Sample SFHA cluster setup diagrams for CP server-based I/O fencing

This appendix includes the following topics:

- [Configuration diagrams for setting up server-based I/O fencing](#)

Configuration diagrams for setting up server-based I/O fencing

The following CP server configuration diagrams can be used as guides when setting up CP server within your configuration:

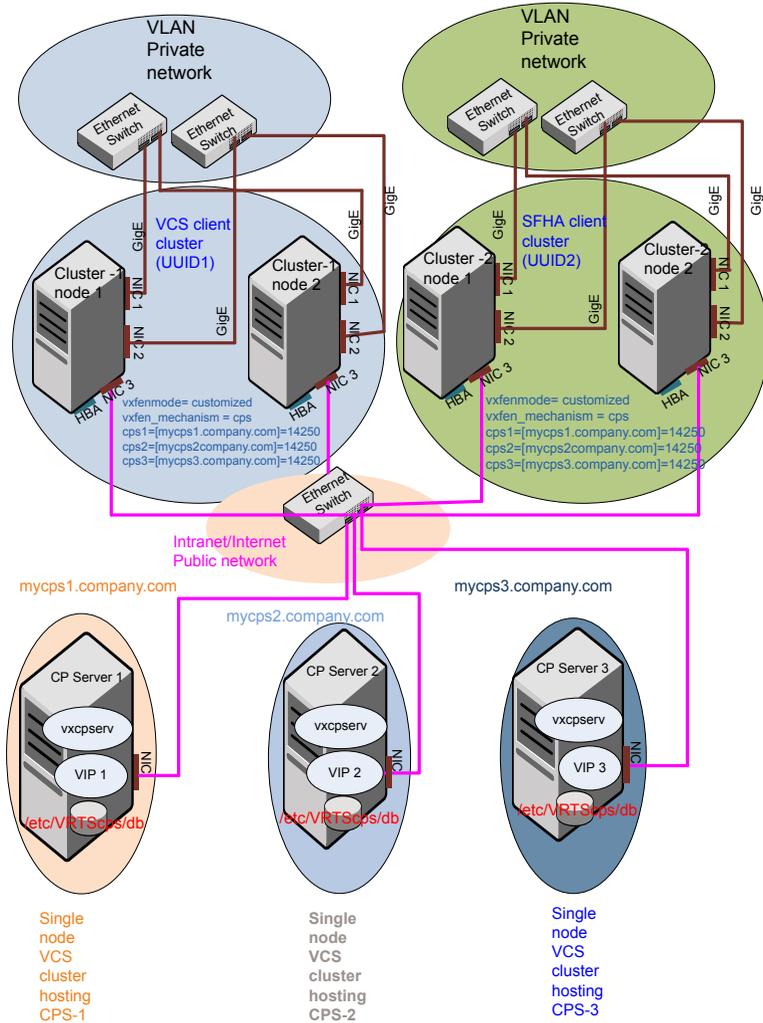
- Two unique client clusters that are served by 3 CP servers:
See [Figure I-1](#) on page 414.
- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:
- Two node campus cluster that is served by remote CP server and 2 SCSI-3 disks:
- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:

Two unique client clusters served by 3 CP servers

[Figure 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



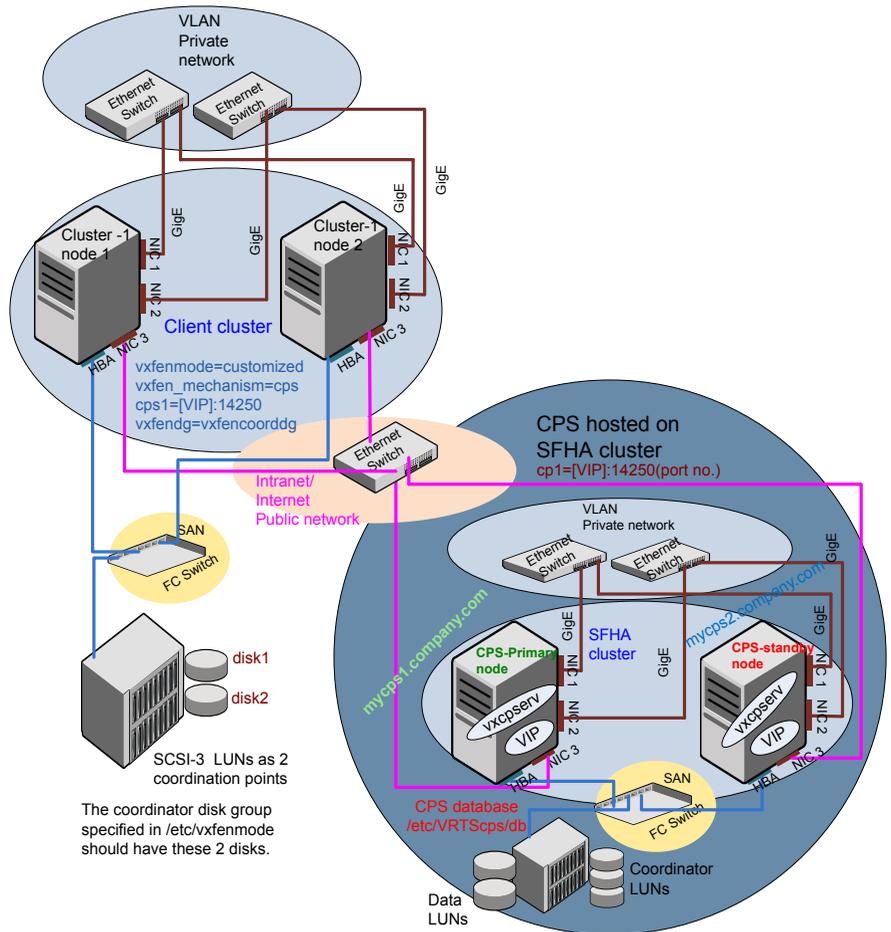
Client cluster served by highly available CPS and 2 SCSI-3 disks

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



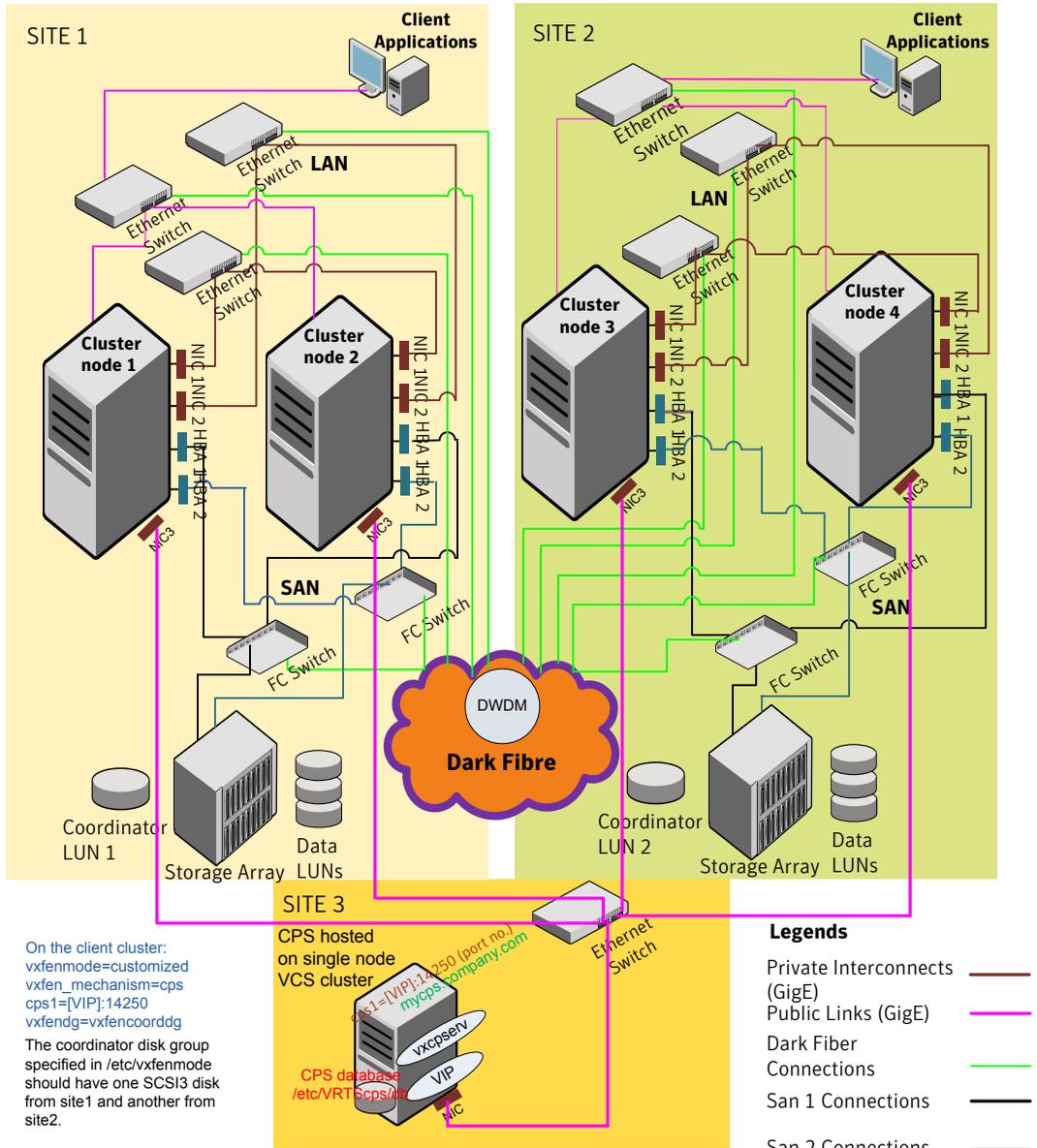
Two node campus cluster served by remote CP server and 2 SCSI-3 disks

[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 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.

Configuring LLT over UDP using IPv4

This appendix includes the following topics:

- [Using the UDP layer for LLT](#)
- [Manually configuring LLT over UDP using IPv4](#)

Using the UDP layer for LLT

Storage Foundation 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/llttab` explicitly depending on the subnet for each link.

See [“Broadcast address in the `/etc/llttab` file”](#) on page 422.

- Make sure that each NIC has an IP address that is configured before configuring LLT.
- Make sure the IP addresses in the `/etc/llttab` files are consistent with the IP addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port.
See [“Selecting UDP ports”](#) on page 424.
- Set the broadcast address correctly for direct-attached (non-routed) links.
See [“Sample configuration: direct-attached links”](#) on page 426.
- For the links that cross an IP router, disable broadcast features and specify the IP address of each link manually in the `/etc/llttab` file.
See [“Sample configuration: links crossing IP routers”](#) on page 428.

Broadcast address in the `/etc/llttab` file

The broadcast address is set explicitly for each link in the following example.

- Display the content of the `/etc/llttab` file on the first node galaxy:

```
galaxy # cat /etc/llttab
set-node galaxy
set-cluster 1
link link1 /dev/udp - udp 50000 - 192.168.9.1 192.168.9.255
link link2 /dev/udp - udp 50001 - 192.168.10.1 192.168.10.255
```

Verify the subnet mask using the `ifconfig` command to ensure that the two links are on separate subnets.

```
galaxy # ifconfig lan1
lan1: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
       inet 192.168.9.1 netmask ffffffff broadcast 192.168.9.255
galaxy # ifconfig lan2
lan2: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
       inet 192.168.10.1 netmask ffffffff broadcast 192.168.10.255
```

- Display the content of the `/etc/llttab` file on the second node nebula:

```
nebula # cat /etc/llttab
set-node nebula
```

```
set-cluster 1
link link1 /dev/udp - udp 50000 - 192.168.9.2 192.168.9.255
link link2 /dev/udp - udp 50001 - 192.168.10.2 192.168.10.255
```

Verify the subnet mask using the `ifconfig` command to ensure that the two links are on separate subnets.

```
nebula # ifconfig lan1
lan1: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
      inet 192.168.9.2 netmask fffffff0 broadcast 192.168.9.255
nebula # ifconfig lan2
lan2: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
      inet 192.168.10.2 netmask fffffff0 broadcast 192.168.10.255
```

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 426.
- See [“Sample configuration: links crossing IP routers”](#) on page 428.

Table J-1 describes the fields of the link command that are shown in the `/etc/llttab` file examples. Note that some of the fields differ from the command for standard LLT links.

Table J-1 Field description for link command in `/etc/llttab`

Field	Description
<i>tag-name</i>	A unique string that is used as a tag by LLT; for example link1, link2,....
<i>device</i>	The device path of the UDP protocol; for example <code>/dev/udp</code> .
<i>node-range</i>	Nodes using the link. "-" indicates all cluster nodes are to be configured for this link.
<i>link-type</i>	Type of link; must be "udp" for LLT over UDP.
<i>udp-port</i>	Unique UDP port in the range of 49152-65535 for the link. See “Selecting UDP ports” on page 424.
<i>MTU</i>	"-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the <code>lltstat -l</code> command to display the current value.

Table J-1 Field description for link command in `/etc/llttab` (*continued*)

Field	Description
<i>IP address</i>	IP address of the link on the local node.
<i>bcast-address</i>	<ul style="list-style-type: none"> ■ 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/llttab` file

The `set-addr` command in the `/etc/llttab` file is required when the broadcast feature of LLT is disabled, such as when LLT must cross IP routers.

See [“Sample configuration: links crossing IP routers”](#) on page 428.

[Table J-2](#) describes the fields of the `set-addr` command.

Table J-2 Field description for set-addr command in `/etc/llttab`

Field	Description
<i>node-id</i>	The ID of the cluster node; for example, 0.
<i>link tag-name</i>	The string that LLT uses to identify the link; for example link1, link2,....
<i>address</i>	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 | head -2 ; netstat -a | grep udp
Active Internet connections (including servers)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
udp	0	0	*.ntalk	*.*	
udp	0	0	*.*	*.*	
udp	0	0	*.49193	*.*	
udp	0	0	*.49152	*.*	
udp	0	0	*.portmap	*.*	
udp	0	0	*.*	*.*	
udp	0	0	*.135	*.*	
udp	0	0	*.2121	*.*	
udp	0	0	*.xdmcp	*.*	
udp	0	0	*.49196	*.*	
udp	0	0	*.*	*.*	
udp	0	0	*.snmp	*.*	
udp	0	0	*.*	*.*	
udp	0	0	*.49153	*.*	
udp	0	0	*.echo	*.*	
udp	0	0	*.discard	*.*	
udp	0	0	*.daytime	*.*	
udp	0	0	*.chargen	*.*	
udp	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:

```
# set_parms ip_address
```

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/llttab` depending on the subnet that the links are on.

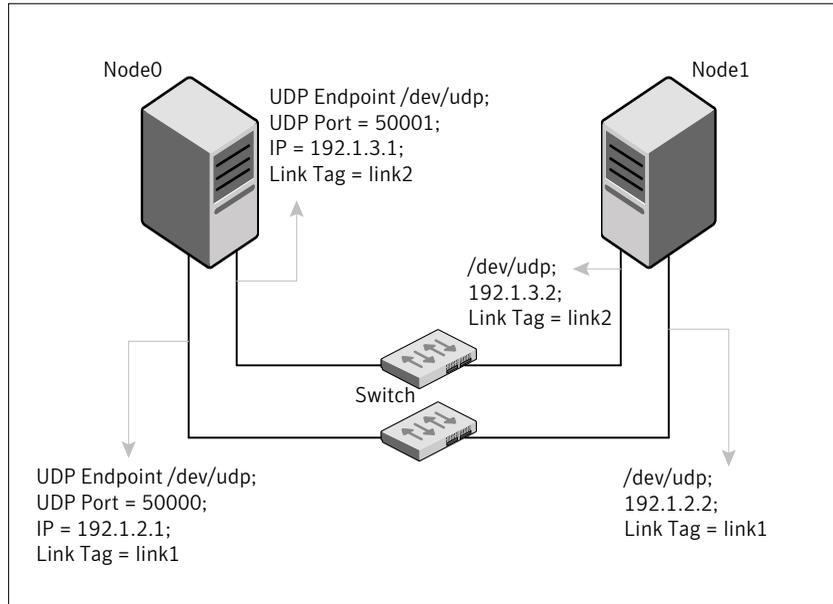
An example of a typical `/etc/llttab` file when nodes are on different subnets. Note the explicitly set broadcast address for each link.

```
# cat /etc/llttab  
set-node nodexyz  
set-cluster 100  
  
link link1 /dev/udp - udp 50000 - 192.168.30.1 192.168.30.255  
link link2 /dev/udp - udp 50001 - 192.168.31.1 192.168.31.255
```

Sample configuration: direct-attached links

[Figure J-1](#) depicts a typical configuration of direct-attached links employing LLT over UDP.

Figure J-1 A typical configuration of direct-attached links that use LLT over UDP



The configuration that the `/etc/llttab` file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT broadcasts requests peer nodes to discover their addresses. So the addresses of peer nodes do not need to be specified in the `/etc/llttab` file using the `set-addr` command. For direct attached links, you do need to set the broadcast address of the links in the `/etc/llttab` file. Verify that the IP addresses and broadcast addresses are set correctly by using the `ifconfig interface_name` command.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.1 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.1 192.1.3.255
```

The file for Node 1 resembles:

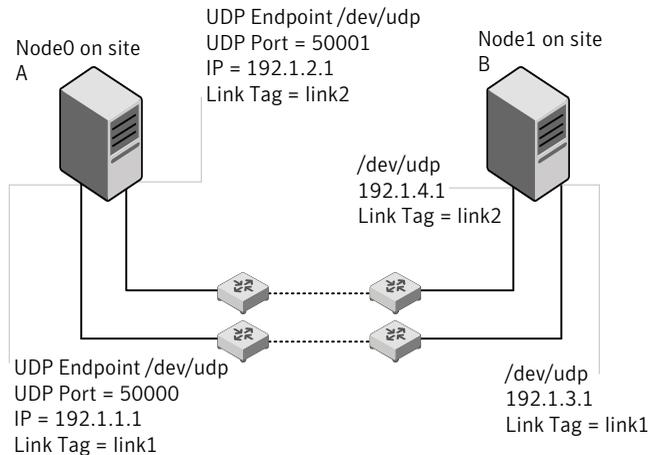
```
set-node Node1
set-cluster 1
```

```
#configure Links
#link tag-name device node-range link-type udp port MTU \
  IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.2 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.2 192.1.3.255
```

Sample configuration: links crossing IP routers

Figure J-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 J-2 A typical configuration of links crossing an IP router



The configuration that the following `/etc/llttab` file represents for Node 1 has links crossing IP routers. Notice that IP addresses are shown for each link on each peer node. In this configuration broadcasts are disabled. Hence, the broadcast address does not need to be set in the `link` command of the `/etc/llttab` file.

```
set-node Node1
set-cluster 1

link link1 /dev/udp - udp 50000 - 192.1.3.1 -
link link2 /dev/udp - udp 50001 - 192.1.4.1 -
#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 0 link1 192.1.1.1
set-addr 0 link2 192.1.2.1
set-addr 2 link1 192.1.5.2
set-addr 2 link2 192.1.6.2
```

```
set-addr      3 link1 192.1.7.3
set-addr      3 link2 192.1.8.3
```

```
#disable LLT broadcasts
set-bcasthb   0
set-arp       0
```

The /etc/llttab file on Node 0 resembles:

```
set-node Node0
set-cluster 1

link link1 /dev/udp - udp 50000 - 192.1.1.1 -
link link2 /dev/udp - udp 50001 - 192.1.2.1 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr      1 link1 192.1.3.1
set-addr      1 link2 192.1.4.1
set-addr      2 link1 192.1.5.2
set-addr      2 link2 192.1.6.2
set-addr      3 link1 192.1.7.3
set-addr      3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb   0
set-arp       0
```


Index

A

- about
 - global clusters 29
- adding
 - users 132
- agents
 - disabling 313
- applications, stopping 202
- attributes
 - UseFence 159

C

- cables
 - cross-over Ethernet 287
 - for SCSI devices 51
- cluster
 - removing a node from 303
 - verifying operation 278
- cluster functionality
 - enabling 113
 - environment requirements 36
 - shared disks 114
- command failures 400
- commands
 - hastatus 278
 - hasys 278
 - lltconfig 363
 - lltstat 275
 - vxdisksetup (initializing disks) 149
 - vxlicinst 139–140
 - vxlicrep 139
- configuration
 - restoring the original 248
- configuration daemon (vxconfigd)
 - starting 111
- configuring
 - remsh 50
 - shared disks 114
 - ssh 50
- configuring SFHA
 - script-based installer 120

- configuring VCS
 - adding users 132
 - event notification 132, 134
 - global clusters 136
 - secure mode 128
 - starting 121
- coordinator disks
 - DMP devices 27
 - for I/O fencing 27
 - setting up 157

D

- data disks
 - for I/O fencing 27
- disabling the agents 313
- disks
 - adding and initializing 149
 - coordinator 157
 - testing with vxfentsthdw 150
 - verifying node access 151

E

- Ethernet controllers 287

F

- freezing service groups 202

G

- GAB
 - description 24
- gabtab file
 - verifying after installation 363
- global clusters 29
 - configuration 136

H

- hastatus -summary command 278
- hasys -display command 278

hubs
 independent 287

I

I/O daemon (vxiod)
 starting 112
 I/O fencing
 checking disks 150
 setting up 156
 shared storage 150
 I/O fencing requirements
 non-SCSI3 42
 Installing
 SFHA with the Web-based installer 72
 installing
 post 137
 Root Broker 81

K

kctune command 396

L

license keys
 adding with vxlicinst 139
 replacing demo key 140
 licenses
 information about 139
 links
 private network 363
 LLT
 description 24
 interconnects 25
 verifying 275
 lltconfig command 363
 llthosts file
 verifying after installation 363
 lltstat command 275
 llttab file
 verifying after installation 363
 log files 401

M

main.cf file
 contents after installation 368
 main.cf files 375
 manual pages
 potential problems 399
 troubleshooting 399

media speed 25
 optimizing 24
 mounting
 software disc 57

N

nodes
 adding application nodes
 configuring GAB 295
 configuring LLT 295
 configuring VXFEN 295
 starting Volume Manager 294
 non-SCSI3 fencing
 manual configuration 180
 setting up 180
 non-SCSI3 I/O fencing
 requirements 42

O

optimizing
 media speed 24
 original configuration
 restoring the 248

P

PATH variable
 VCS commands 275
 persistent reservations
 SCSI-3 51
 phased 221
 phased upgrade 221
 example 222
 planning an upgrade from
 previous VVR version 198
 planning to upgrade VVR 197
 preinstallation 197
 preparing to upgrade VVR 202
 previous VVR version
 planning an upgrade from 198
 problems
 accessing manual pages 399
 executing file system commands 400

R

removing
 the Replicated Data Set 314
 removing a system from a cluster 303

- remsh 122
 - configuration 50
- Replicated Data Set
 - removing the 314
- restoring the original configuration 248
- Root Broker
 - installing 81
- S**
- sam command 396
- script-based installer
 - SFHA configuration overview 120
- SCSI
 - changing initiator IDs 52
- SCSI-3
 - persistent reservations 51
- SCSI-3 persistent reservations
 - verifying 156
- service groups
 - freezing 202
 - unfreezing 248
- SFHA
 - configuring 120
 - coordinator disks 157
- SFHA installation
 - verifying
 - cluster operations 275
 - GAB operations 275
 - LLT operations 275
- shared disks, configuring 114
- Shared storage
 - Fibre Channel 54
- shared storage 51
 - SCSI 51
- SMTP email notification 132
- SNMP trap notification 134
- ssh 122
 - configuration 50
- starting configuration
 - installvcs program 122
 - Veritas product installer 122
- starting vxconfigd configuration daemon 111
- starting vxiod daemon 112
- stopping
 - applications 202
- Symantec Product Authentication Service 81, 128
- system state attribute value 278

T

- troubleshooting
 - accessing manual pages 399
 - executing file system commands 400

U

- unfreezing service groups 248
- upgrade
 - phased 221
- upgrading
 - clustered environment 115
 - phased 221
- upgrading VVR
 - planning 197
 - preparing 202

V

- VCS
 - command directory path variable 275
 - configuration files
 - main.cf 366
- VEA
 - client, starting 146
- verifying installation
 - kernel component 274
- Veritas Operations Manager 23
- vradmin
 - delpri 315
 - stoprep 315
- vvr_upgrade_finish script 250
- vxconfigd configuration daemon
 - starting 111
- vxctl mode command 112
- vxdisksetup command 149
- vxiod I/O daemon
 - starting 112
- vxlicinst command 139
- vxlicrep command 139

W

- Web-based installer 72