# Veritas Storage Foundation™ Cluster File System High Availability 6.0.1 Installation Guide - Solaris

February 2015

Symantec™

# Veritas Storage Foundation™ Cluster File System 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: 6.0.1

Document version: 6.0.1 Rev 7

## Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark 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 website at the following URL:

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

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

## Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

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

## Licensing and registration

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

www.symantec.com/business/support/

## Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

## Support agreement resources

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

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

## Documentation

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

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

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

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

## About Symantec Connect

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

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

# Contents

Technical Support ..... 4

Section 1 Installation overview and planning ..... 23

Chapter 1 Introducing Storage Foundation Cluster File System High Availability ..... 24

About Veritas Storage Foundation Cluster File System High Availability ..... 24
About I/O fencing ..... 25
About Veritas Operations Manager ..... 26
About Veritas Operations Manager ..... 26
About configuring SFCFSHA clusters for data integrity ..... 27
About I/O fencing for SFCFSHA in virtual machines that do not support SCSI-3 PR ..... 27
About I/O fencing components ..... 28
About data disks ..... 28
About coordination points ..... 28
About preferred fencing ..... 30

Chapter 2 System requirements ..... 31

Release notes ..... 31
Hardware compatibility list (HCL) ..... 32
Supported operating systems ..... 32
Veritas Storage Foundation Cluster File System High Availability hardware requirements ..... 32
I/O fencing requirements ..... 33
Coordinator disk requirements for I/O fencing ..... 33
CP server requirements ..... 34
Non-SCSI-3 I/O fencing requirements ..... 37
Veritas File System requirements ..... 38
Database requirements ..... 39
Database configuration requirements ..... 39
Disk space requirements ..... 39
Synchronizing time on Cluster File Systems ..... 40

Discovering product versions and various requirement information ..... 40
Number of nodes supported ..... 40

Chapter 3 Planning to install SFCFSHA ..... 41

About planning for SFCFSHA installation ..... 41
About installation and configuration methods ..... 42
About response files ..... 43
About the Veritas installer ..... 44
Downloading the Veritas Storage Foundation Cluster File System High Availability software ..... 46
Optimizing LLT media speed settings on private NICs ..... 47
Guidelines for setting the media speed of the LLT interconnects ..... 48
Prerequisites for installing Veritas Storage Foundation Cluster File System High Availability ..... 48
Sample SFCFSHA configuration on a Fibre Channel fabric ..... 49
About the VRTSspt package troubleshooting tools ..... 50

Chapter 4 Licensing SFCFSHA ..... 51

About Veritas product licensing ..... 51
Setting or changing the product level for keyless licensing ..... 52
Installing Veritas product license keys ..... 54

Section 2 Preinstallation tasks ..... 55

Chapter 5 Preparing to install SFCFSHA ..... 56

Installation preparation overview ..... 56
About using ssh or rsh with the Veritas installer ..... 57
Setting up shared storage ..... 58
Setting up shared storage: SCSI disks ..... 58
Setting up shared storage: Fibre Channel ..... 61
Creating root user ..... 62
Creating the /opt directory ..... 63
Setting environment variables ..... 63
Mounting the product disc ..... 63
Assessing the system for installation readiness ..... 64
About Symantec Operations Readiness Tools ..... 64
Prechecking your systems using the Veritas installer ..... 65
Making the IPS publisher accessible ..... 66

Section 3 Installation using the script-based installer ..... 68

Chapter 6 Installing SFCFSHA ..... 69

Installing Storage Foundation Cluster File System High Availability using the product installer ..... 69
Installing language packages ..... 72

Chapter 7 Preparing to configure SFCFSHA clusters for data integrity ..... 73

About planning to configure I/O fencing ..... 73
Typical SFCFSHA cluster configuration with server-based I/O fencing ..... 77
Recommended CP server configurations ..... 78
Setting up the CP server ..... 81
Planning your CP server setup ..... 81
Installing the CP server using the installer ..... 82
Configuring the CP server cluster in secure mode ..... 83
Setting up shared storage for the CP server database ..... 84
Configuring the CP server using the installer program ..... 85
Configuring the CP server manually ..... 94
Verifying the CP server configuration ..... 96
Configuring the CP server using the Web-based installer ..... 96

Chapter 8 Configuring SFCFSHA ..... 98

Overview of tasks to configure SFCFSHA using the script-based installer ..... 99
Starting the software configuration ..... 100
Specifying systems for configuration ..... 100
Configuring the cluster name ..... 101
Configuring private heartbeat links ..... 102
Configuring the virtual IP of the cluster ..... 105
Configuring Veritas Storage Foundation Cluster File System High Availability in secure mode ..... 107
Configuring a secure cluster node by node ..... 108
Configuring the first node ..... 108
Configuring the remaining nodes ..... 109
Completing the secure cluster configuration ..... 110
Adding VCS users ..... 112
Configuring SMTP email notification ..... 113

Configuring SNMP trap notification ..... 114
Configuring global clusters ..... 116
Completing the SFCFSHA configuration ..... 117
Verifying and updating licenses on the system ..... 118
Checking licensing information on the system ..... 118
Updating product licenses ..... 119
Configuring the Storage Foundation for Databases repository database after installation ..... 120

Chapter 9 Configuring SFCFSHA clusters for data integrity ..... 121

Setting up disk-based I/O fencing using installsfcfsha ..... 121
Configuring disk-based I/O fencing using installsfcfsha ..... 121
Initializing disks as VxVM disks ..... 124
Checking shared disks for I/O fencing ..... 125
Setting up server-based I/O fencing using installsfcfsha ..... 129
Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsfcfsha ..... 137
Enabling or disabling the preferred fencing policy ..... 139

Section 4 Installation using the Web-based installer ..... 142

Chapter 10 Installing SFCFSHA ..... 143

About the Web-based installer ..... 143
Before using the Veritas Web-based installer ..... 144
Starting the Veritas Web-based installer ..... 144
Obtaining a security exception on Mozilla Firefox ..... 145
Performing a pre-installation check with the Veritas Web-based installer ..... 146
Installing SFCFSHA with the Web-based installer ..... 146

Chapter 11 Configuring SFCFSHA ..... 149

Configuring SFCFSHA using the Web-based installer ..... 149
Configuring SFCFSHA for data integrity using the Web-based installer ..... 154

Section 5 Automated installation using response files ..... 162

Chapter 12 Performing an automated SFCFSHA installation ..... 163

Installing SFCFSHA using response files ..... 163
Response file variables to install Veritas Storage Foundation Cluster File System High Availability ..... 164
Sample response file for Veritas Storage Foundation Cluster File System High Availability installation ..... 166

Chapter 13 Performing an automated SFCFSHA configuration ..... 168

Configuring SFCFSHA using response files ..... 168
Response file variables to configure Veritas Storage Foundation Cluster File System High Availability ..... 169
Sample response file for Veritas Storage Foundation Cluster File System High Availability configuration ..... 178

Chapter 14 Performing an automated I/O fencing configuration using response files ..... 180

Configuring I/O fencing using response files ..... 180
Response file variables to configure disk-based I/O fencing ..... 181
Sample response file for configuring disk-based I/O fencing ..... 184
Configuring CP server using response files ..... 185
Response file variables to configure CP server ..... 185
Sample response file for configuring the CP server on single node VCS cluster ..... 187
Sample response file for configuring the CP server on SFHA cluster ..... 188
Response file variables to configure server-based I/O fencing ..... 189
Sample response file for configuring server-based I/O fencing ..... 190
Response file variables to configure non-SCSI-3 server-based I/O fencing ..... 191
Sample response file for configuring non-SCSI-3 server-based I/O fencing ..... 192

Section 6 Installation using operating system-specific methods ..... 193

Chapter 15 Installing SFCFSHA using operating system-specific methods ..... 194

Installing SFCFSHA on Solaris 11 using Automated Installer ..... 194
About Automated Installation ..... 195
Using Automated Installer ..... 195
Using AI to install the Solaris 11 operating system and SFHA products ..... 196
Manually installing packages on Solaris brand non-global zones ..... 201
Manually installing packages on solaris10 brand zones ..... 203
Installing SFCFSHA on Solaris 10 using JumpStart ..... 203
Overview of JumpStart installation tasks ..... 203
Generating the finish scripts ..... 204
Preparing installation resources ..... 205
Adding language pack information to the finish file ..... 206
Using a Flash archive to install SFCFSHA and the operating system ..... 207
Creating the Veritas post-deployment scripts ..... 208
Installing SFCFSHA using the system command ..... 209

Chapter 16 Configuring SFCFSHA using operating system-specific methods ..... 212

Configuring Veritas Storage Foundation Cluster File System High Availability manually ..... 212
Configuring Veritas Volume Manager ..... 212
Configuring Veritas File System ..... 219

Chapter 17 Manually configuring SFCFSHA clusters for data integrity ..... 221

Setting up disk-based I/O fencing manually ..... 221
Identifying disks to use as coordinator disks ..... 222
Setting up coordinator disk groups ..... 222
Creating I/O fencing configuration files ..... 223
Modifying VCS configuration to use I/O fencing ..... 224
Verifying I/O fencing configuration ..... 226
Setting up server-based I/O fencing manually ..... 226
Preparing the CP servers manually for use by the SFCFSHA cluster ..... 227

Configuring server-based fencing on the SFCFSHA cluster manually ..... 230
Configuring CoordPoint agent to monitor coordination points ..... 236
Verifying server-based I/O fencing configuration ..... 238
Setting up non-SCSI-3 fencing in virtual environments manually ..... 239
Sample /etc/vxfenmode file for non-SCSI-3 fencing ..... 241

Section 7 Upgrade of SFCFSHA ..... 245

Chapter 18 Planning to upgrade SFCFSHA ..... 246

Upgrade methods for SFCFSHA ..... 246
Supported upgrade paths for SFCFSHA 6.0.1 ..... 247
About using the installer to upgrade when the root disk is encapsulated ..... 249
Preparing to upgrade SFCFSHA ..... 250
Getting ready for the upgrade ..... 250
Creating backups ..... 252
Determining if the root disk is encapsulated ..... 253
Pre-upgrade planning for Veritas Volume Replicator ..... 253
Preparing to upgrade VVR when VCS agents are configured ..... 256
Verifying that the file systems are clean ..... 260
Upgrading the array support ..... 261

Chapter 19 Performing a typical Storage Foundation Cluster File System High Availability upgrade using the installer ..... 263

Performing a full upgrade ..... 263
Ensuring the file systems are clean ..... 263
Modifying the main.cf file ..... 264
Performing the upgrade ..... 267

Chapter 20 Performing a rolling upgrade of SFCFSHA ..... 272

Performing a rolling upgrade using the installer ..... 272
About rolling upgrades ..... 272
Supported rolling upgrade paths ..... 275
Performing a rolling upgrade using the script-based installer ..... 275
Performing a rolling upgrade of SFCFSHA using the Web-based installer ..... 278

Chapter 21 Performing a phased upgrade of SFCFSHA ..... 282

Performing a phased upgrade of SFCFSHA ..... 282
Prerequisites for a phased upgrade ..... 282
Planning for a phased upgrade ..... 283
Phased upgrade limitations ..... 283
Moving the service groups to the second subcluster ..... 283
Upgrading the SFCFSHA stack on the first subcluster ..... 286
Preparing the second subcluster ..... 287
Activating the first subcluster ..... 290
Upgrading the operating system on the second subcluster ..... 291
Upgrading the second subcluster ..... 292
Completing the phased upgrade ..... 292

Chapter 22 Performing an automated SFCFSHA upgrade using response files ..... 293

Upgrading SFCFSHA using response files ..... 293
Response file variables to upgrade Veritas Storage Foundation Cluster File System High Availability ..... 294
Sample response file for upgrading Veritas Storage Foundation Cluster File System High Availability ..... 295

Chapter 23 Upgrading the operating system ..... 297

Upgrading the Solaris operating system ..... 297

Chapter 24 Upgrading Veritas Volume Replicator ..... 301

Upgrading Veritas Volume Replicator ..... 301
Upgrading VVR without disrupting replication ..... 301

Chapter 25 Upgrading language packages ..... 304

Upgrading language packages ..... 304

Chapter 26 Migrating from SFHA to SFCFSHA ..... 305

Migrating from SFHA to SFCFSHA 6.0.1 ..... 305

Chapter 27 Upgrading SFCFSHA using Live Upgrade ..... 308

About Live Upgrade ..... 308
About Live Upgrade in a Veritas Volume Replicator (VVR) environment ..... 309
Supported upgrade paths for Live Upgrade ..... 310

Performing Live Upgrade in a Solaris zone environment ..... 311
Before you upgrade SFCFSHA using Solaris Live Upgrade ..... 312
Upgrading SFCFSHA and Solaris using Live Upgrade ..... 315
Creating a new boot environment on the alternate boot disk ..... 316
Upgrading SFCFSHA using the installer for a Live Upgrade ..... 319
Upgrading SFCFSHA manually ..... 320
Completing the Live Upgrade ..... 322
Verifying Live Upgrade of SFCFSHA ..... 323
Upgrading Solaris using Live Upgrade ..... 324
Removing and reinstalling SFCFSHA using the installer ..... 325
Upgrading SFCFSHA using Live Upgrade ..... 326
Administering boot environments ..... 326
Reverting to the primary boot environment ..... 326
Switching the boot environment for Solaris SPARC ..... 327
Switching the boot environment for Solaris x86-64 ..... 328

Chapter 28 Performing post-upgrade tasks ..... 331

Re-joining the backup boot disk group into the current disk group ..... 331
Reverting to the backup boot disk group after an unsuccessful upgrade ..... 332

Section 8 Post-installation tasks ..... 333

Chapter 29 Performing post-installation tasks ..... 334

Changing root user into root role ..... 334
About enabling LDAP authentication for clusters that run in secure mode ..... 335
Enabling LDAP authentication for clusters that run in secure mode ..... 336
Starting and stopping processes for the Veritas products ..... 341

Chapter 30 Verifying the SFCFSHA installation ..... 343

Performing a postcheck on a node ..... 343
Verifying that the products were installed ..... 344
Installation log files ..... 344
Using the installation log file ..... 345
Using the summary file ..... 345
Checking Veritas Volume Manager processes ..... 345
Checking Veritas File System installation ..... 345
Verifying Veritas File System kernel installation ..... 345
Verifying command installation ..... 346

Verifying agent configuration for Storage Foundation Cluster File System High Availability ..... 346
Configuring VCS for Storage Foundation Cluster File System High Availability ..... 347
main.cf file ..... 347
Storage Foundation Cluster File System HA Only ..... 349
Veritas Cluster Server application failover services ..... 349
Configuring the cluster UUID when creating a cluster manually ..... 349
About the cluster UUID ..... 350
Verifying the LLT, GAB, and VCS configuration files ..... 350
Verifying LLT, GAB, and cluster operation ..... 350
Verifying LLT ..... 351
Verifying GAB ..... 353
Verifying the cluster ..... 355
Verifying the cluster nodes ..... 355

Section 9 Configuration of disaster recovery environments ..... 359

Chapter 31 Configuring disaster recovery environments ..... 360

Disaster recovery options for SFCFSHA ..... 360
About setting up a campus cluster for disaster recovery ..... 361
About setting up a global cluster environment for SFCFSHA ..... 363
About configuring a parallel global cluster using Veritas Volume Replicator (VVR) for replication ..... 364

Section 10 Uninstallation of SFCFSHA ..... 367

Chapter 32 Uninstalling Storage Foundation Cluster File System High Availability ..... 368

About removing Veritas Storage Foundation Cluster File System High Availability ..... 368
Preparing to uninstall ..... 369
Shutting down cluster operations ..... 378
Disabling the agents on a system ..... 378
Removing the Replicated Data Set ..... 379
Uninstalling SFCFSHA packages using the script-based installer ..... 381
Uninstalling SFCFSHA with the Veritas Web-based installer ..... 382
Uninstalling Storage Foundation using the pkgrm command ..... 383

Uninstalling the language packages using the pkgrm command ... 383 384
Removing the CP server configuration using the installer program ... 385
Removing the Storage Foundation for Databases (SFDB) repository after removing the product ... 387

Chapter 33 Uninstalling using response files ... 390

Uninstalling SFCFSHA using response files ... 390
Response file variables to uninstall Veritas Storage Foundation Cluster File System High Availability ... 391
Sample response file for Veritas Storage Foundation Cluster File System High Availability uninstallation ... 392

Section 11 Adding and removing nodes ... 393

Chapter 34 Adding a node to SFCFSHA clusters ... 394

About adding a node to a cluster ... 394
Before adding a node to a cluster ... 395
Adding a node to a cluster using the SFCFSHA installer ... 398
Adding a node using the Web-based installer ... 401
Adding the node to a cluster manually ... 402
Starting Veritas Volume Manager (VxVM) on the new node ... 403
Configuring cluster processes on the new node ... 403
Setting up the node to run in secure mode ... 405
Starting fencing on the new node ... 408
After adding the new node ... 409
Configuring Cluster Volume Manager (CVM) and Cluster File System (CFS) on the new node ... 409
Configuring the ClusterService group for the new node ... 410
Configuring server-based fencing on the new node ... 411
Adding the new node to the vxfen service group ... 412
Updating the Storage Foundation for Databases (SFDB) repository after adding a node ... 413
Sample configuration file for adding a node to the cluster ... 414

Chapter 35 Removing a node from SFCFSHA clusters ... 418

About removing a node from a cluster ... 418
Removing a node from a cluster ... 419
Modifying the VCS configuration files on existing nodes ... 420

Modifying the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node ..... 423
Removing the node configuration from the CP server ..... 423
Removing security credentials from the leaving node ..... 424
Updating the Storage Foundation for Databases (SFDB) repository after removing a node ..... 425
Sample configuration file for removing a node from the cluster ..... 425

Section 12 Installation reference ..... 428

Appendix A Installation scripts ..... 429

Installation script options ..... 429
About using the postcheck option ..... 434

Appendix B Tunable files for installation ..... 437

About setting tunable parameters using the installer or a response file ..... 437
Setting tunables for an installation, configuration, or upgrade ..... 438
Setting tunables with no other installer-related operations ..... 439
Setting tunables with an un-integrated response file ..... 440
Preparing the tunables file ..... 441
Setting parameters for the tunables file ..... 441
Tunables value parameter definitions ..... 442

Appendix C Configuration files ..... 449

About the LLT and GAB configuration files ..... 449
About the AMF configuration files ..... 451
About I/O fencing configuration files ..... 452
Sample configuration files for CP server ..... 454
CP server hosted on a single node main.cf file ..... 455
CP server hosted on an SFHA cluster main.cf file ..... 457
Sample main.cf file for CP server hosted on a single node that runs VCS ..... 461
Sample main.cf file for CP server hosted on a two-node SFHA cluster ..... 463
Sample CP server configuration (/etc/vxcps.conf) file output ..... 466

Appendix D Configuring the secure shell or the remote shell for communications ..... 467

About configuring secure shell or remote shell communication modes before installing products ..... 467
Manually configuring and passwordless ssh ..... 468
Restarting the ssh session ..... 472
Enabling and disabling rsh for Solaris ..... 473

Appendix E Storage Foundation Cluster File System High Availability components ..... 475

Veritas Storage Foundation Cluster File System High Availability installation packages ..... 475
Veritas Cluster Server installation packages ..... 478
Veritas Cluster File System installation packages ..... 479
Chinese language packages ..... 479
Japanese language packages ..... 480
Veritas Storage Foundation obsolete and reorganized installation packages ..... 480

Appendix F High availability agent information ..... 484

About agents ..... 484
VCS agents included within SFCFSHA ..... 485
Enabling and disabling intelligent resource monitoring for agents manually ..... 485
Administering the AMF kernel driver ..... 487
CVMCluster agent ..... 488
Entry points for CVMCluster agent ..... 489
Attribute definition for CVMCluster agent ..... 489
CVMCluster agent type definition ..... 490
CVMCluster agent sample configuration ..... 490
CVMVxconfigd agent ..... 491
Entry points for CVMVxconfigd agent ..... 491
Attribute definition for CVMVxconfigd agent ..... 492
CVMVxconfigd agent type definition ..... 493
CVMVxconfigd agent sample configuration ..... 494
CVMVolDg agent ..... 494
Entry points for CVMVolDg agent ..... 494
Attribute definition for CVMVolDg agent ..... 495
CVMVolDg agent type definition ..... 496
CVMVolDg agent sample configuration ..... 497
CFSMount agent ..... 497

Entry points for CFSMount agent ..... 498
Attribute definition for CFSMount agent ..... 498
CFSMount agent type definition ..... 500
CFSMount agent sample configuration ..... 501
CFSfsckd agent ..... 501
Entry points for CFSfsckd agent ..... 501
Attribute definition for CFSfsckd agent ..... 502
CFSfsckd agent type definition ..... 503
CFSfsckd agent sample configuration ..... 504

Appendix G Troubleshooting the SFCFSHA installation ..... 505

Restarting the installer after a failed connection ..... 505
What to do if you see a licensing reminder ..... 506
Storage Foundation Cluster File System High Availability installation issues ..... 506
Incorrect permissions for root on remote system ..... 506
Inaccessible system ..... 508
Storage Foundation Cluster File System High Availability problems ..... 508
Unmount failures ..... 508
Mount failures ..... 508
Command failures ..... 509
Performance issues ..... 510
High availability issues ..... 510
Installer cannot create UUID for the cluster ..... 511
The vxfentsthdw utility fails when SCSI TEST UNIT READY command fails ..... 512
Troubleshooting CP server ..... 512
Troubleshooting issues related to the CP server service group ..... 513
Checking the connectivity of CP server ..... 513
Troubleshooting server-based fencing on the SFCFSHA cluster nodes ..... 513
Issues during fencing startup on SFCFSHA cluster nodes set up for server-based fencing ..... 514
Issues during online migration of coordination points ..... 514
Troubleshooting the webinstaller ..... 515

Appendix H Sample SFCFSHA cluster setup diagrams for CP server-based I/O fencing ..... 517

Configuration diagrams for setting up server-based I/O fencing ..... 517
Two unique client clusters served by 3 CP servers ..... 517

Client cluster served by highly available CPS and 2 SCSI-3 disks ..... 518
Two node campus cluster served by remote CP server and 2 SCSI-3 disks ..... 520
Multiple client clusters served by highly available CP server and 2 SCSI-3 disks ..... 522

Appendix I Reconciling major/minor numbers for NFS shared disks ..... 524

Reconciling major/minor numbers for NFS shared disks ..... 524
Checking major and minor numbers for disk partitions ..... 525
Checking the major and minor number for VxVM volumes ..... 528

Appendix J Configuring LLT over UDP ..... 531

Using the UDP layer for LLT ..... 531
When to use LLT over UDP ..... 531
Manually configuring LLT over UDP using IPv4 ..... 531
Broadcast address in the /etc/llttab file ..... 532
The link command in the /etc/llttab file ..... 533
The set-addr command in the /etc/llttab file ..... 533
Selecting UDP ports ..... 534
Configuring the netmask for LLT ..... 535
Configuring the broadcast address for LLT ..... 535
Sample configuration: direct-attached links ..... 536
Sample configuration: links crossing IP routers ..... 538
Using the UDP layer of IPv6 for LLT ..... 540
When to use LLT over UDP ..... 541
Manually configuring LLT over UDP using IPv6 ..... 541
The link command in the /etc/llttab file ..... 541
The set-addr command in the /etc/llttab file ..... 542
Selecting UDP ports ..... 542
Sample configuration: direct-attached links ..... 544
Sample configuration: links crossing IP routers ..... 545

Appendix K Compatability issues when installing Storage Foundation Cluster File System High Availability with other products ..... 548

Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present ..... 548
Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present ..... 549

Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present ..... 549

Index ..... 550

Section 1

# Installation overview and planning


- Chapter 1. Introducing Storage Foundation Cluster File System High Availability
- Chapter 2. System requirements
- Chapter 3. Planning to install SFCFSHA
- Chapter 4. Licensing SFCFSHA

Chapter 1

# Introducing Storage Foundation Cluster File System High Availability

This chapter includes the following topics:


- About Veritas Storage Foundation Cluster File System High Availability
- About I/O fencing
- About Veritas Operations Manager
- About configuring SFCFSHA clusters for data integrity
- About I/O fencing for SFCFSHA in virtual machines that do not support SCSI-3 PR
- About I/O fencing components


## About Veritas Storage Foundation Cluster File System High Availability

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

Veritas Storage Foundation Cluster File System High Availability also provides increased automation and intelligent management of availability and performance.

Veritas Storage Foundation Cluster File System High Availability includes Veritas Cluster Server, which adds high availability functionality to the product.

To install the product, follow the instructions in the *Veritas Storage Foundation Cluster File System High Availability Installation Guide*.

For information on high availability environments, read the Veritas Cluster Server documentation.

# About I/O fencing

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

The fencing operation determines the following:

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

This decision prevents possible data corruption. When you install SFCFSHA, the installer installs the `VRTSvxfen` package, which includes the I/O fencing driver. To protect data on shared disks, you must configure I/O fencing after you install and configure SFCFSHA.

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

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

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

See “About planning to configure I/O fencing” on page 73.

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

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

# About Veritas Operations Manager

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

## About Veritas Operations Manager

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.

Symantec recommends using Veritas Operations Manager (VOM) to manage Storage Foundation and Cluster Server environments.

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.

The Veritas Enterprise Administrator (VEA) console is no longer packaged with Storage Foundation products. If you want to continue using VEA, a software version is available for download from http://www.symantec.com/operations-manager/support. Veritas Storage Foundation Management Server is deprecated.

If you want to manage a single cluster using Cluster Manager (Java Console), a version is available for download from https://www4.symantec.com/Vrt/offer?a_id=89446. You cannot manage the new features of this release using the Java Console. Veritas Cluster Server Management Console is deprecated.

# About configuring SFCFSHA clusters for data integrity

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

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

- Broken set of private networks
  If a system in a two-node cluster fails, the system stops sending heartbeats over the private interconnects. The remaining node then takes corrective action. The failure of the private interconnects, instead of the actual nodes, presents identical symptoms and causes each node to determine its peer has departed. This situation typically results in data corruption because both nodes try to take control of data storage in an uncoordinated manner.
- System that appears to have a system-hang
  If a system is so busy that it appears to stop responding, the other nodes could declare it as dead. This declaration may also occur for the nodes that use the hardware that supports a "break" and "resume" function. When a node drops to PROM level with a break and subsequently resumes operations, the other nodes may declare the system dead. They can declare it dead even if the system later returns and begins write operations.

I/O fencing is a feature that prevents data corruption in the event of a communication breakdown in a cluster. SFCFSHA 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 SFCFSHA, you must configure I/O fencing in SFCFSHA to ensure data integrity.

See “About planning to configure I/O fencing” on page 73.

# About I/O fencing for SFCFSHA 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, SFCFSHA attempts to provide reasonable safety for the data disks. SFCFSHA requires you to configure non-SCSI-3 server-based I/O fencing in such environments. Non-SCSI-3 fencing uses CP servers as coordination points with some additional configuration changes to support I/O fencing in such environments.

See "Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsfcfsha" on page 137.

See "Setting up non-SCSI-3 fencing in virtual environments manually" on page 239.

# About I/O fencing components

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

- Data disks—Store shared data
  See "About data disks" on page 28.
- Coordination points—Act as a global lock during membership changes
  See "About coordination points" on page 28.

## About data disks

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

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

## About coordination points

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

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

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

- Coordinator disks

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

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

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

- Coordination point servers

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

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

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

# About preferred fencing

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

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

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

See the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide* for more details.

See "Enabling or disabling the preferred fencing policy" on page 139.

Chapter 2

# System requirements

This chapter includes the following topics:


- Release notes
- Hardware compatibility list (HCL)
- Supported operating systems
- Veritas Storage Foundation Cluster File System High Availability hardware requirements
- I/O fencing requirements
- Veritas File System requirements
- Database requirements
- Disk space requirements
- Synchronizing time on Cluster File Systems
- Discovering product versions and various requirement information
- 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:

https://sort.symantec.com/documents

# Hardware compatibility list (HCL)

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

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

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

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

# Supported operating systems

For information on supported operating systems, see the *Veritas Storage Foundation Cluster File System High Availability Release Notes*.

# Veritas Storage Foundation Cluster File System High Availability hardware requirements

The following hardware requirements apply to Veritas Storage Foundation Cluster File System High Availability.

**Table 2-1** Hardware requirements for Veritas Storage Foundation Cluster File System High Availability

| Requirement | Description |
|---|---|
| Memory | 2 GB of memory. |
| CPU | A minimum of 2 CPUs. |
| Node | Veritas Storage Foundation Cluster File System High Availability supports mixed cluster environments with Solaris 10 SPARC operating systems as long as all the nodes in the cluster have the same CPU architecture. |
| Shared storage | Shared storage can be one or more shared disks or a disk array connected either directly to the nodes of the cluster or through a Fibre Channel Switch. Nodes can also have non-shared or local devices on a local I/O channel. It is advisable to have `/`, `/usr`, `/var` and other system partitions on local devices. |

**Table 2-1** Hardware requirements for Veritas Storage Foundation Cluster File System High Availability *(continued)*

| Requirement | Description |
|---|---|
| Fibre Channel switch | Each node in the cluster must have a Fibre Channel I/O channel to access shared storage devices. The primary component of the Fibre Channel fabric is the Fibre Channel switch. |
| Cluster platforms | There are several hardware platforms that can function as nodes in a Veritas Storage Foundation Cluster File System High Availability (SFCFSHA) cluster.<br>See the *Veritas Storage Foundation Cluster File System High Availability Release Notes*.<br>For a cluster to work correctly, all nodes must have the same time. If you are not running the Network Time Protocol (NTP) daemon, make sure the time on all the systems comprising your cluster is synchronized. |

# 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 33.
- CP servers
  See "CP server requirements" on page 34.

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

See "Non-SCSI-3 I/O fencing requirements" on page 37.

## Coordinator disk requirements for I/O fencing

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

- For disk-based I/O fencing, you must have at least three coordinator disks or there must be odd number of coordinator disks.
- The coordinator disks can be raw devices, DMP devices, or iSCSI devices.
- Each of the coordinator disks must use a physically separate disk or LUN. Symantec recommends using the smallest possible LUNs for coordinator disks.

- Each of the coordinator disks should exist on a different disk array, if possible.
- The coordinator disks must support SCSI-3 persistent reservations.
- Symantec recommends using hardware-based mirroring for coordinator disks.
- Coordinator disks must not be used to store data or must not be included in disk groups that store user data.
- Coordinator disks cannot be the special devices that array vendors use. For example, you cannot use EMC gatekeeper devices as coordinator disks.

## CP server requirements

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

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

---

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

---

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

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

---

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

---

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

- Hardware requirements
- Operating system requirements

- Networking requirements (and recommendations)
- Security requirements

Table 2-2 lists additional requirements for hosting the CP server.

**Table 2-2** 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:<br>■ 550 MB in the /opt directory (additionally, the language pack requires another 15 MB)<br>■ 300 MB in /usr<br>■ 20 MB in /var<br>■ 10 MB in /etc (for the CP server database)<br>See "Disk space requirements" on page 39. |
| Storage | When CP server is hosted on an SFHA cluster, there must be shared storage between the nodes of this SFHA cluster. |
| RAM | Each CP server requires at least 512 MB. |
| Network | Network hardware capable of providing TCP/IP connection between CP servers and SFCFSHA clusters (application clusters). |

Table 2-3 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 2-3** 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 | CP server supports any of the following operating systems:<br>■ AIX 6.1 and 7.1<br>■ HP-UX 11i v3<br>■ Linux:<br>  ■ RHEL 5<br>  ■ RHEL 6<br>  ■ SLES 10<br>  ■ SLES 11<br>■ Oracle Solaris 10<br>■ Oracle Solaris 11<br>Review other details such as supported operating system levels and architecture for the supported operating systems.<br>See the *Veritas Cluster Server Release Notes* or the *Veritas Storage Foundation High Availability Release Notes* for that platform. |

Following are the CP server networking requirements and recommendations:

- Symantec recommends that network access from the application clusters to the CP servers should be made highly-available and redundant. The network connections require either a secure LAN or VPN.
- The CP server uses the TCP/IP protocol to connect to and communicate with the application clusters by these network paths. The CP server listens for messages from the application clusters using TCP port 14250. This is the default port that can be changed during a CP server configuration.
  Symantec recommends that you configure multiple network paths to access a CP server. If a network path fails, CP server does not require a restart and continues to listen on all the other available virtual IP addresses.
- The CP server supports either Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with the application clusters. If the CP server is configured to use an IPv6 virtual IP address, then the application clusters should also be on the IPv6 network where the CP server is hosted.
- When placing the CP servers within a specific network configuration, you must take into consideration the number of hops from the different application cluster nodes to the CP servers. As a best practice, Symantec recommends that the number of hops and network latency from the different application cluster nodes to the CP servers should be equal. This ensures that if an event occurs that

results in an I/O fencing scenario, there is no bias in the race due to difference in number of hops or network latency between the CPS and various nodes.

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

| Communication mode | CP server in secure mode | CP server in non-secure mode |
|---|---|---|
| SFCFSHA cluster in secure mode | Yes | Yes |
| SFCFSHA cluster in non-secure mode | Yes | Yes |

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

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

For information about establishing secure communications between the application cluster and CP server, see the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide*.

## Non-SCSI-3 I/O fencing requirements

Supported virtual environment for non-SCSI-3 fencing:

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

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

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

# Veritas File System requirements

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

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

For Solaris 10:

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

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

For Solaris 11:

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

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

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

---

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

---

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

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

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

# Database requirements

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

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

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

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

## Database configuration requirements

Most relational database management system (RDBMS) software requires operating system parameters to be set prior to operation. In Solaris 10 and later, system parameters are managed through the Resource Controls facility.The most critical settings are normally located in the Shared Memory and Semaphore settings on Solaris. For precise settings, consult your current database installation and configuration documentation.

# Disk space requirements

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

Use the **Perform a Pre-installation Check (P)** menu for the Web-based installer to determine whether there is sufficient space.

Or, go to the installation directory and run the installer with the `-precheck` option.

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

See “About the Veritas installer” on page 44.

# Synchronizing time on Cluster File Systems

SFCFSHA requires that the system clocks on all nodes are synchronized using some external component such as the Network Time Protocol (NTP) daemon. If the nodes are not in sync, timestamps for change (`ctime`) and modification (`mtime`) may not be consistent with the sequence in which operations actually happened.

# Discovering product versions and various requirement information

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

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

The information that the `version` option or the `showversion` script discovers on systems includes the following:

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

**To run the version checker**

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

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

# Number of nodes supported

SFCFSHA supports cluster configurations with up to 64 nodes.

Chapter 3

# Planning to install SFCFSHA

This chapter includes the following topics:


- About planning for SFCFSHA installation
- About installation and configuration methods
- About the Veritas installer
- Downloading the Veritas Storage Foundation Cluster File System High Availability software
- Optimizing LLT media speed settings on private NICs
- Guidelines for setting the media speed of the LLT interconnects
- Prerequisites for installing Veritas Storage Foundation Cluster File System High Availability
- Sample SFCFSHA configuration on a Fibre Channel fabric
- About the VRTSspt package troubleshooting tools


## About planning for SFCFSHA installation

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

https://sort.symantec.com/documents

Document version: 6.0.1 Rev 7.

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 SFCFSHA will be installed.

Follow the preinstallation instructions if you are installing Veritas Storage Foundation Cluster File System High Availability.

# About installation and configuration methods

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

**Table 3-1** Installation and configuration methods

| Method | Description |
|---|---|
| Interactive installation and configuration using the script-based installer<br><br>**Note:** If you obtained SFCFSHA from an electronic download site, you must use the `installsfcfsha` script instead of the `installer` script. | You can use one of the following script-based installers:<br>■ Common product installer script:<br>`installer`<br>The common product installer script provides a menu that simplifies the selection of installation and configuration options.<br>■ Product-specific installation script:<br>`installsfcfsha`<br>■ The product-specific installation script provides command-line interface options. Installing and configuring with the `installsfcfsha` script is identical to specifying SFCFSHA from the `installer` script.<br>Use this method to install or configure only SFCFSHA. |
| Silent installation using the response file | The response file automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. You can use the script-based installers with the response file to install silently on one or more systems.<br><br>See "About response files" on page 43. |
| Web-based installer | The Web-based installer provides an interface to manage the installation and configuration from a remote site using a standard Web browser.<br><br>`webinstaller`<br><br>See "About the Web-based installer" on page 143. |

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

| Method | Description |
|---|---|
| JumpStart<br>(For Solaris 10 systems) | You can use the Veritas product installer of the product-specific installation script to generate a JumpStart script file. Use the generated script to install Veritas packages from your JumpStart server.<br>See "Installing SFCFSHA on Solaris 10 using JumpStart" on page 203. |
| Manual installation and configuration | Manual installation uses the Solaris commands to install SFCFSHA. To retrieve a list of all packages and patches required for all products in the correct installation order, enter:<br>`# installer -allpkgs`<br>Use the Solaris commands to install SFCFSHA. Then use a manual or an interactive method with installsfcfsha or `installer` script to configure the SFCFSHA stack. |
| Automated Installer<br>(For Solaris 11 systems) | You can use the Oracle Solaris Automated Installer (AI) to install the Solaris operating system on multiple client systems in a network. AI performs a hands-free installation (automated installation without manual interactions) of both x86 and SPARC systems. |

# About response files

The installer or product installation script generates a response file during any installation, configuration, upgrade (except rolling upgrade), or uninstall procedure. The response file contains the configuration information that you entered during the procedure. When the procedure completes, the installation script displays the location of the response files.

You can use the response file for future installation procedures by invoking an installation script with the `-responsefile` option. The response file passes arguments to the script to automate the installation of that product. You can edit the file to automate installation and configuration of additional systems.

You can generate a response file using the `-makeresponsefile` option.

See "Installation script options" on page 429.

## 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"];
```

# About the Veritas installer

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

- The general product installer. The general product installer enables you to install and configure the product, verify preinstallation requirements, and view the product's description. You perform the installation from a disc, and you are prompted to choose a product to install.
  See "Installing Storage Foundation Cluster File System High Availability using the product installer" on page 69.
- Product-specific installation scripts. If you obtained a standalone Veritas product from an electronic download site, the single product download files do not contain the general product installer. Use the product installation script to install the individual products. You can find these scripts at the root of the product media in the scripts directory. These scripts are also installed with the product.

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

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

**Table 3-2** Product installation scripts

| Veritas product name | Product installation script (When running the script from the install media) | Product installation script (When running the script from a system on which the SFHA Solutions product is installed) |
|---|---|---|
| Veritas Cluster Server (VCS) | `installvcs` | `installvcs<version>` |

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

| Veritas product name | Product installation script (When running the script from the install media) | Product installation script (When running the script from a system on which the SFHA Solutions product is installed) |
|---|---|---|
| Veritas Storage Foundation (SF) | `installsf` | `installsf<version>` |
| Veritas Storage Foundation and High Availability (SFHA) | `installsfha` | `installsfha<version>` |
| Veritas Storage Foundation Cluster File System High Availability (SFCFSHA) | `installsfcfsha` | `installsfcfsha<version>` |
| Veritas Storage Foundation for Oracle RAC (SF Oracle RAC) | `installsfrac` | `installsfrac<version>` |
| Veritas Storage Foundation for Sybase ASE CE (SF Sybase CE) | `installsfsybasece` | `installsfsybasece<version>` |
| Veritas Dynamic Multi-Pathing | `installdmp` | `installdmp<version>` |
| Symantec VirtualStore | `installsvs` | `installsvs<version>` |

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

For example, for the 6.0.1 version:

```
# /opt/VRTS/install/installsfcfsha601 -configure
```

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

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

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

See "Installation script options" on page 429.

# Downloading the Veritas Storage Foundation Cluster File System High Availability software

One method of obtaining the Veritas Storage Foundation Cluster File System High Availability software is to download it to your local system from the Symantec Web site.

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

**To download the trialware version of the software**

1. Open the following link in your browser:

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

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

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

See "About the Veritas installer" on page 44.

**To download the software**

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

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

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

   See "Disk space requirements" on page 39.

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

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

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

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

# Optimizing LLT media speed settings on private NICs

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

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

# Guidelines for setting the media speed of the LLT interconnects

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

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

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

# Prerequisites for installing Veritas Storage Foundation Cluster File System High Availability

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

Provide the following information when installing SFCFSHA:

- The cluster name, beginning with a letter (a-z, A-Z).
- A unique ID from 0-65535 for the cluster. Within the public subnet, a new cluster using a duplicate cluster ID can cause existing clusters to fail.
- The host names of the cluster nodes.
- The device names of the network interface cards (NICs) used for the private networks among nodes.
- Establishing communication between nodes is required to install Veritas software from a remote system, or to install and configure a cluster. The node from which the installation utility is run must have permissions to run `rsh` (remote shell) or ssh (secure shell) utilities as root on all cluster nodes or remote systems.

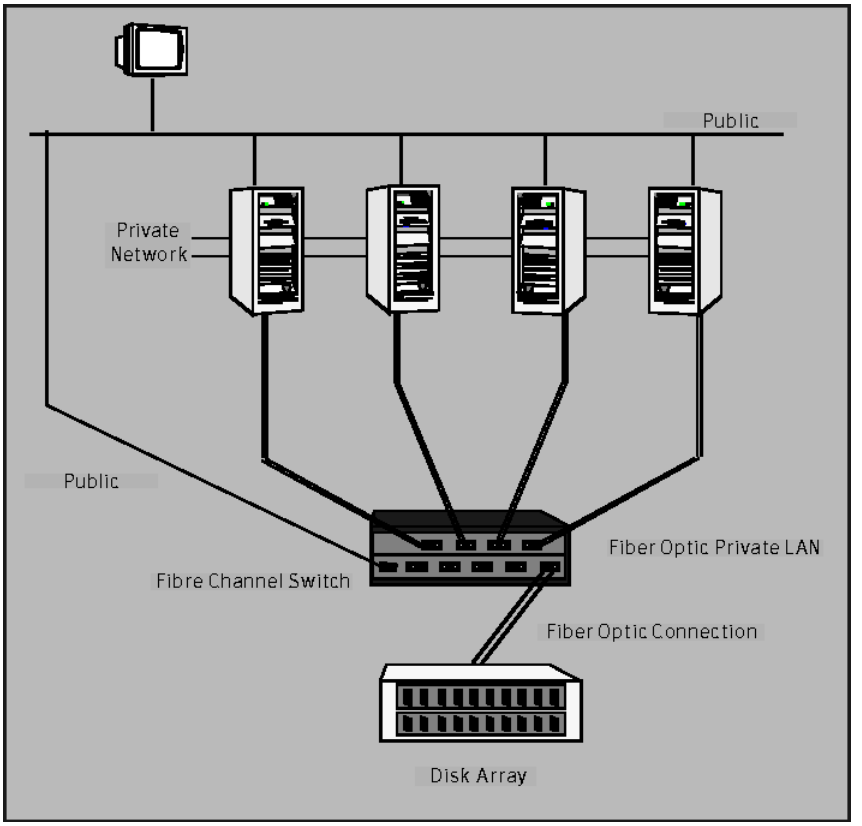
- Symantec recommends configuring the cluster with I/O fencing enabled. I/O fencing requires shared devices to support SCSI-3 Persistent Reservations (PR). Enabling I/O fencing prevents data corruption caused by a split brain scenario.
  The Veritas Storage Foundation Cluster File System High Availability is supported without I/O fencing enabled. However, without I/O fencing enabled, split brain scenarios can result in data corruption.
- In a large cluster environment, make sure the first volume of the volume set is large enough to accommodate all of the metadata. A large cluster environment includes more than 14 nodes, and a volume set with more than 40 volumes. The minimum size of the first volume should be more than 900M.

# Sample SFCFSHA configuration on a Fibre Channel fabric

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

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

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




# About the VRTSspt package troubleshooting tools

The VRTSspt package provides a group of tools for troubleshooting a system and collecting information on its configuration. If you install and use the VRTSspt package, it will be easier for Symantec Support to diagnose any issues you may have.

The tools can gather Veritas File System and Veritas Volume Manager metadata information and establish various benchmarks to measure file system and volume manager performance. Although the tools are not required for the operation of any Veritas product, Symantec recommends installing them should a support case be needed to be opened with Symantec Support. Use caution when you use the VRTSspt package, and always use it in concert with Symantec Support.

Chapter 4

# Licensing SFCFSHA

This chapter includes the following topics:


- About Veritas product licensing
- Setting or changing the product level for keyless licensing
- Installing Veritas product license keys


## About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

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

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

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

http://go.symantec.com/sfhakeyless

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

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See "Setting or changing the product level for keyless licensing" on page 52.
  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 54.
  See the `vxlicinst(1m)` manual page.

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

---

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

---

# Setting or changing the product level for keyless licensing

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

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

http://go.symantec.com/vom

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

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

**To set or change the product level**

1 Change your current working directory:

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

2 View the current setting for the product level.

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

3 View the possible settings for the product level.

```
# ./vxkeyless displayall
```

4 Set the desired product level.

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

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

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

---

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

---

**To clear the product license level**

1 View the current setting for the product license level.

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

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

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

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

# Installing Veritas product license keys

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

| | |
|---|---|
| vxlicinst | Installs a license key for a Symantec product |
| vxlicrep | Displays currently installed licenses |
| vxlictest | Retrieves features and their descriptions encoded in a license key |

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

**To install a new license**

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

```
# cd /opt/VRTS/bin

# ./vxlicinst -k license key
```

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

```
# ./vxkeyless display
```

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

Section 2

# Preinstallation tasks


- Chapter 5. Preparing to install SFCFSHA

Chapter 5

# Preparing to install SFCFSHA

This chapter includes the following topics:


- Installation preparation overview
- About using ssh or rsh with the Veritas installer
- Setting up shared storage
- Creating root user
- Creating the /opt directory
- Setting environment variables
- Mounting the product disc
- Assessing the system for installation readiness
- Making the IPS publisher accessible


## 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 51. |

**Table 5-1** Installation overview *(continued)*

| Installation task | Section |
|---|---|
| Download the software, or insert the product DVD. | See "Downloading the Veritas Storage Foundation Cluster File System High Availability software" on page 46.<br>See "Mounting the product disc" on page 63. |
| Set environment variables. | See "Setting environment variables" on page 63. |
| Create the `/opt` directory, if it does not exist. | See "Creating the /opt directory" on page 63. |
| Configure the secure shell (ssh) or remote shell (rsh) on all nodes. | See "About configuring secure shell or remote shell communication modes before installing products" on page 467. |
| Verify that hardware, software, and operating system requirements are met. | See "Release notes" on page 31. |
| Check that sufficient disk space is available. | See "Disk space requirements" on page 39. |
| Use the installer to install the products. | See "About the Veritas installer" on page 44. |

# About using ssh or rsh with the Veritas installer

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

See "Installation script options" on page 429.

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

- When you perform installer sessions using a response file.

See “About configuring secure shell or remote shell communication modes before installing products” on page 467.

# 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 73.

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

## Setting up shared storage: SCSI disks

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

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

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

**To set up shared storage**

1. Install the required SCSI host adapters on each node that connects to the storage, and make cable connections to the storage.

   Refer to the documentation that is shipped with the host adapters, the storage, and the systems.

2. With both nodes powered off, power on the storage devices.

3. Power on one system, but do not allow it to boot. If necessary, halt the system so that you can use the ok prompt.

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

4 Find the paths to the host adapters:

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

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

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

```
{0} ok nvedit
```

As you edit the script, note the following points:

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

In this example, edit the nvramrc script as follows:

```
0: probe-all
1: cd /sbus@6,0/QLGC,isp@2,10000
2: 5 " scsi-initiator-id" integer-property
3: device-end
4: install-console
5: banner
6: <CTRL-C>
```

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

```
{0} ok nvstore
```

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

```
{0} ok printenv nvramrc
```

You can re-edit the file to make corrections:

```
{0} ok nvedit
```

Or, discard the changes if necessary by entering:

```
{0} ok nvquit
```

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

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

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

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

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

Permit the system to continue booting.

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

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

Permit the system to continue booting.

# Setting up shared storage: Fibre Channel

Perform the following steps to set up Fibre Channel.

**To set up shared storage**

1 Install the required FC-AL controllers.

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

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

3 Boot each system with the reconfigure devices option:

```
ok boot -r
```

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

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

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

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

# Creating root user

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

**To change root role into a user**

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

```
% su  - root
```

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

```
# roles admin

root

# usermod -R " " admin
```

3 Change the root role into a user.

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

4 Verify the change.

- `# getent user_attr root`

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

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

- `# userattr type root`

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

---

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

---

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

See "Changing root user into root role" on page 334.

# 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.

# 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, SFCFSHA commands are in `/opt/VRTS/bin`. SFCFSHA 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 SFCFSHA software.

**To mount the product disc**

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

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

2. Insert the product disc into a DVD drive that is connected to your system.

3. If Solaris volume management software is running on your system, the software disc automatically mounts as /cdrom/cdrom0.

4. If Solaris volume management software is not available to mount the DVD, you must mount it manually. After you insert the software disc, enter:

   ```
   # mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
   ```

   Where c0t6d0s2 is the default address for the disc drive.

# Assessing the system for installation readiness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Veritas Storage Foundation Cluster File System High Availability 6.0.1.

| | |
|---|---|
| Symantec Operations Readiness Tools | Symantec Operations Readiness Tools (SORT) is a Web-based application that is designed to support Symantec enterprise products.<br><br>See "About Symantec Operations Readiness Tools" on page 64. |
| Prechecking your systems using the installer | Performs a pre-installation check on the specified systems. The Veritas product installer reports whether the specified systems meet the minimum requirements for installing Veritas Storage Foundation Cluster File System High Availability 6.0.1.<br><br>See "Prechecking your systems using the Veritas installer" on page 65. |

## About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a Web site that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you

manage your datacenter more efficiently and get the most out of your Symantec products.

Among its broad set of features, SORT lets you do the following:

- Generate server-specific reports that describe how to prepare your servers for installation or upgrade of Symantec enterprise products.
- Access a single site with the latest production information, including patches, agents, and documentation.
- Create automatic email notifications for changes in patches, documentation, and array-specific modules.

To access SORT, go to:

https://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.

   See "Installing SFCFSHA with the Web-based installer" on page 146.

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.

# Making the IPS publisher accessible

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

*CPI ERROR V-9-20-1273 Unable to contact configured publishers on <node_name>.*

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

```
# pkg publisher
```

Example:

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

**To make the IPS publisher accessible**

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

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

2. Repeat the installation of SFCFSHA 6.0.1.
3. Re-enable the original publisher. If the publisher is still inaccessible (private network), then the `no-refresh` option can be used to re-enable it.

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

   or

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

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

Section 3

# Installation using the script-based installer


- Chapter 6. Installing SFCFSHA
- Chapter 7. Preparing to configure SFCFSHA clusters for data integrity
- Chapter 8. Configuring SFCFSHA
- Chapter 9. Configuring SFCFSHA clusters for data integrity

Chapter 6

# Installing SFCFSHA

This chapter includes the following topics:


- Installing Storage Foundation Cluster File System High Availability using the product installer
- Installing language packages


## Installing Storage Foundation Cluster File System High Availability using the product installer

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

The following sample procedure is based on the installation of a Veritas Storage Foundation Cluster File System High Availability cluster with two nodes: "sys1" and "sys2" If you are installing on standalone systems only, some steps are unnecessary, and these are indicated.

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

---

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

---

**To install Veritas Storage Foundation Cluster File System High Availability**

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 467.

2. Load and mount the software disc.

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

   ```
   # cd /dvd_mount
   ```

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

   ```
   # ./installer
   ```

5. Enter I to install and press Return.

6. From the Installation menu, choose the I option for Install and enter the number for Storage Foundation Cluster File System High Availability. 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_cluster_file_system_ha/EULA/lang/EULA_CFSHA_Ux_6.0.1.pdf
   file present

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

8. Select from one of the following install options:

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

   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, "sys1" and "sys2") on which the software is to be installed. Enter the system name or names and then press Return.

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

10 During the initial system check, the installer verifies that communication between systems has been set up. The installer prompts you to allow it to set up ssh or rsh. After the installation, the installer cleans up the ssh or rsh as needed.

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

12 You are prompted to choose your licensing method.

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

* Enter a valid license key matching the functionality in use on
the systems
* Enable keyless licensing and manage the systems with a
Management Server.

For more details visit http://go.symantec.com/sfhakeyless. The
product is fully functional during these 60 days.

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

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

If you have a valid license key, select 1 and enter the license key at the prompt. Skip to step 16.

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

---

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

---

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

http://go.symantec.com/vom

13 Select **yes** to enable replication.

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

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 product installation completes.

Review the output and summary files. Reboot nodes as requested. Run the following command to configure SFCFSHA.

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

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

See "About the Veritas installer" on page 44.

# Installing language packages

To install SFCFSHA in a language other than English, install the required language packages after installing the English packages.

**To install the language packages on the server**

1 Insert the "Language" disc into the DVD-ROM or CD-ROM drive. With Solaris volume management software, the disc is automatically mounted as `/cdrom/cdrom0`.

2 Install the language packages using the `install_lp` command.

```
# cd /cdrom/cdrom0
# ./install_lp
```

Chapter 7

# Preparing to configure SFCFSHA clusters for data integrity

This chapter includes the following topics:


- About planning to configure I/O fencing
- Setting up the CP server


## About planning to configure I/O fencing

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

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

The coordination points in server-based fencing can include only CP servers or a mix of CP servers and coordinator disks.

Symantec also supports server-based fencing with a single coordination point which is a single highly available CP server that is hosted on an SFHA cluster.

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

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

See Figure 7-2 on page 76.

Figure 7-1 illustrates a high-level flowchart to configure I/O fencing for the SFCFSHA cluster.

**Figure 7-1** Workflow to configure I/O fencing

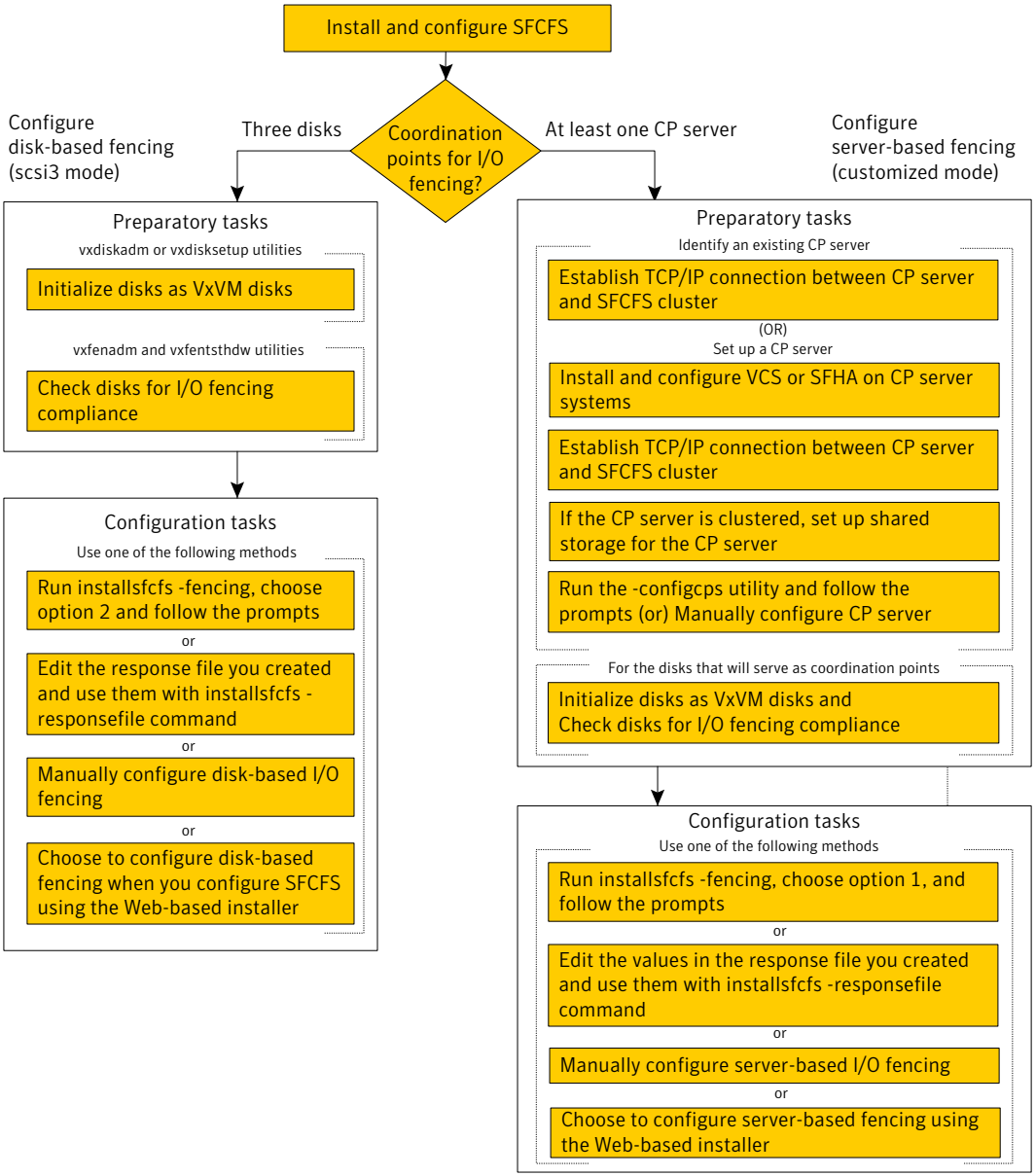
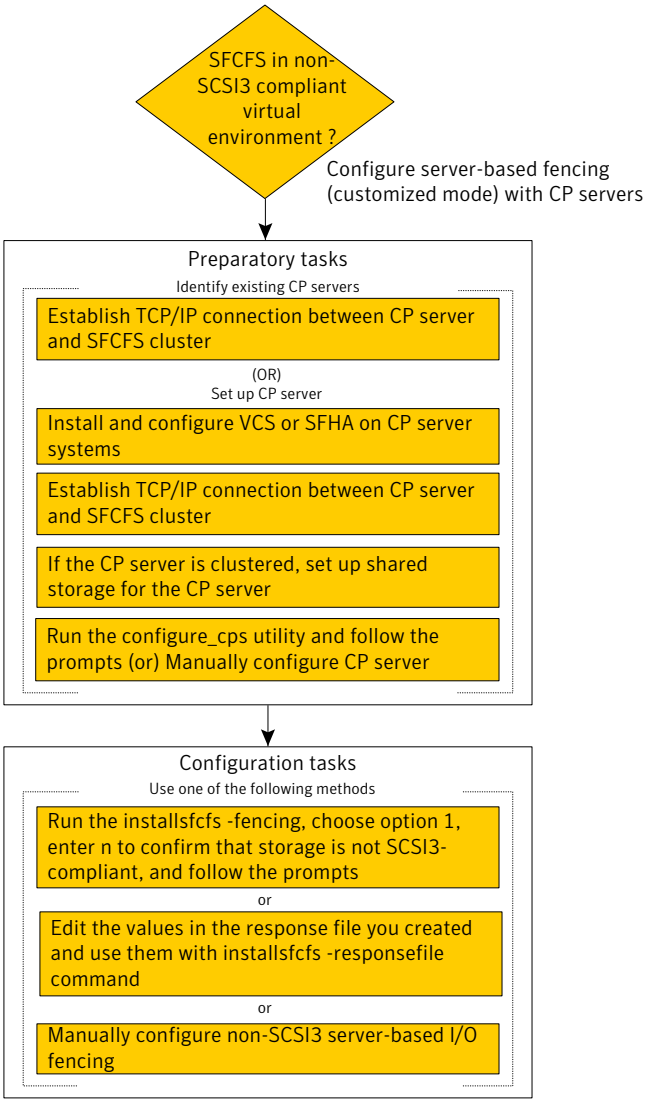



Figure 7-2 illustrates a high-level flowchart to configure non-SCSI-3 server-based I/O fencing for the SFCFSHA cluster in virtual environments that do not support SCSI-3 PR.

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




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

| | |
|---|---|
| Using the installsfcfsha | See "Setting up disk-based I/O fencing using installsfcfsha" on page 121.<br>See "Setting up server-based I/O fencing using installsfcfsha" on page 129.<br>See "Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsfcfsha" on page 137. |
| Using the Web-based installer | See "Configuring SFCFSHA for data integrity using the Web-based installer" on page 154. |
| Using response files | See "Response file variables to configure disk-based I/O fencing" on page 181.<br>See "Response file variables to configure server-based I/O fencing" on page 189.<br>See "Response file variables to configure non-SCSI-3 server-based I/O fencing" on page 191.<br>See "Configuring I/O fencing using response files" on page 180. |
| Manually editing configuration files | See "Setting up disk-based I/O fencing manually" on page 221.<br>See "Setting up server-based I/O fencing manually" on page 226.<br>See "Setting up non-SCSI-3 fencing in virtual environments manually" on page 239. |

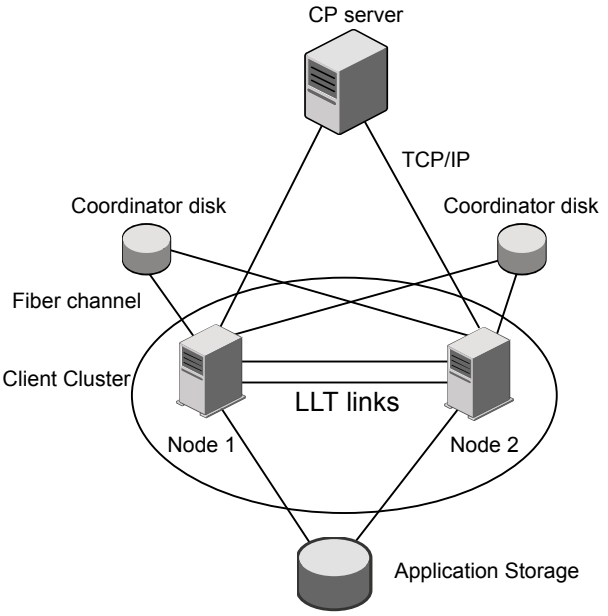
You can also migrate from one I/O fencing configuration to another.

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

## Typical SFCFSHA cluster configuration with server-based I/O fencing

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

**Figure 7-3** CP server, SFCFSHA cluster, and coordinator disks




## Recommended CP server configurations

Following are the recommended CP server configurations:

- Multiple application clusters use three CP servers as their coordination points
  See Figure 7-4 on page 79.
- Multiple application clusters use a single CP server and single or multiple pairs of coordinator disks (two) as their coordination points
  See Figure 7-5 on page 80.
- Multiple application clusters use a single CP server as their coordination point
  This single coordination point fencing configuration must use a highly available CP server that is configured on an SFHA cluster as its coordination point.
  See Figure 7-6 on page 80.

---

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

---

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

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

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

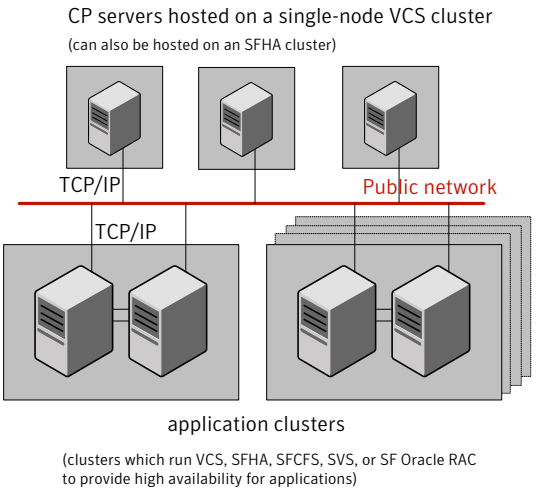



Figure 7-5 displays a configuration using a single CP server that is connected to multiple application clusters with each application cluster also using two coordinator disks.

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

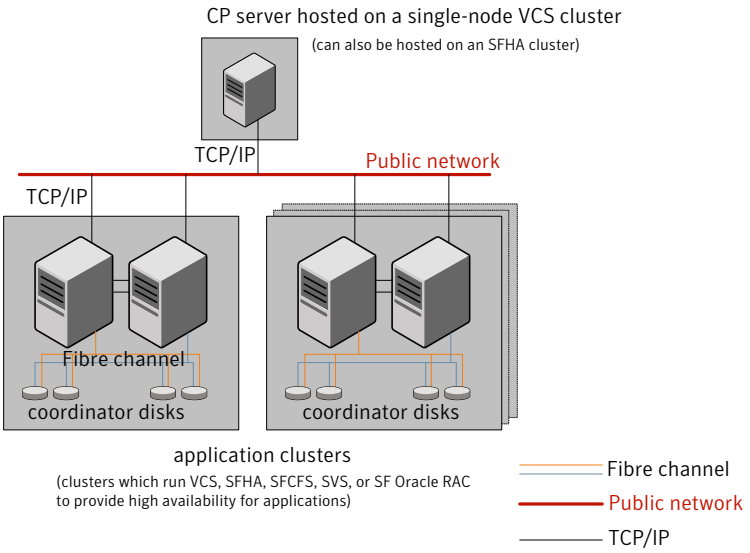
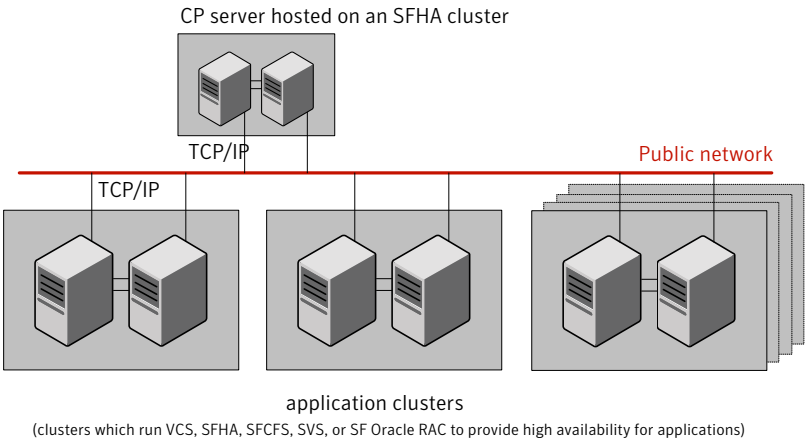



Figure 7-6 displays a configuration using a single CP server that is connected to multiple application clusters.

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




See "Configuration diagrams for setting up server-based I/O fencing" on page 517.

# Setting up the CP server

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

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

| Task | Reference |
|---|---|
| Plan your CP server setup | See "Planning your CP server setup" on page 81. |
| Install the CP server | See "Installing the CP server using the installer" on page 82. |
| Configure the CP server cluster in secure mode | See "Configuring the CP server cluster in secure mode" on page 83. |
| Set up shared storage for the CP server database | See "Setting up shared storage for the CP server database" on page 84. |
| Configure the CP server | See " Configuring the CP server using the installer program" on page 85.<br>See "Configuring the CP server using the Web-based installer" on page 96.<br>See "Configuring the CP server manually" on page 94.<br>See "Configuring CP server using response files" on page 185. |
| Verify the CP server configuration | See "Verifying the CP server configuration" on page 96. |

## Planning your CP server setup

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

**To plan your CP server setup**

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

   Symantec recommends hosting the CP server on an SFHA cluster to make the CP server highly available.

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

- You must set up shared storage for the CP server database during your CP server setup.
- Decide whether you want to configure server-based fencing for the SFCFSHA cluster (application cluster) with a single CP server as coordination point or with at least three coordination points.
  Symantec recommends using at least three coordination points.

3 Decide whether you want to configure the CP server cluster in secure mode.

  Symantec recommends configuring the CP server cluster in secure mode to secure the communication between the CP server and its clients (SFCFSHA clusters). It also secures the HAD communication on the CP server cluster.

4 Set up the hardware and network for your CP server.

  See "CP server requirements" on page 34.

5 Have the following information handy for CP server configuration:

- Name for the CP server
  The CP server name should not contain any special characters. CP server name can include alphanumeric characters, underscore, and hyphen.
- Port number for the CP server
  Allocate a TCP/IP port for use by the CP server.
  Valid port range is between 49152 and 65535. The default port number is 14250.
- Virtual IP address, network interface, netmask, and networkhosts for the CP server
  You can configure multiple virtual IP addresses for the CP server.

## Installing the CP server using the installer

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

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

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

| | |
|---|---|
| CP server setup uses a single system | Install and configure VCS to create a single-node VCS cluster.<br>During installation, make sure to select all packages for installation. The VRTScps package is installed only if you select to install all packages.<br>See the *Veritas Cluster Server Installation Guide* for instructions on installing and configuring VCS.<br>Proceed to configure the CP server.<br>See " Configuring the CP server using the installer program" on page 85.<br>See "Configuring the CP server manually" on page 94. |
| CP server setup uses multiple systems | Install and configure SFHA to create an SFHA cluster. This makes the CP server highly available.<br>Meet the following requirements for CP server:<br>■ During installation, make sure to select all packages for installation. The VRTScps package is installed only if you select to install all packages.<br>■ During configuration, configure disk-based fencing (scsi3 mode).<br>See the *Veritas Storage Foundation and High Availability Installation Guide* for instructions on installing and configuring SFHA.<br>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 SFCFSHA cluster (CP client).

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

---

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

---

**To configure the CP server cluster in secure mode**

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

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

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

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

  See "About the Veritas installer" on page 44.

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

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

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

  See "About the Veritas installer" on page 44.

## Setting up shared storage for the CP server database

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

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

**To set up shared storage for the CP server database**

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

For example:

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

2 Create a mirrored volume over the disk group.

For example:

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

3 Create a file system over the volume.

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

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

| | |
|---|---|
| AIX | `# mkfs -V vxfs /dev/vx/rdsk/cps_dg/cps_volume` |
| HP-UX | `# mkfs -F vxfs /dev/vx/rdsk/cps_dg/cps_volume` |
| Linux | `# mkfs -t vxfs /dev/vx/rdsk/cps_dg/cps_volume` |
| Solaris | `# mkfs -F vxfs /dev/vx/rdsk/cps_dg/cps_volume` |

# Configuring the CP server using the installer program

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

Perform one of the following procedures:

| | |
|---|---|
| For CP servers on single-node VCS cluster: | See "To configure the CP server on a single-node VCS cluster" on page 86. |
| For CP servers on an SFHA cluster: | See "To configure the CP server on an SFHA cluster" on page 90. |

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

1 Verify that the `VRTScps` package is installed on the node.

2 Run the installvcs<*version*> program with the configcps option.

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

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

See "About the Veritas installer" on page 44.

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

Enter **y** to confirm.

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

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

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

The installer then runs the following preconfiguration checks:

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

6 Enter the name of the CP Server.

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

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

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

---

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

---

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

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

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

---

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

---

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

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

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

11 Verify and confirm the CP server configuration information.

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

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

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

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

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

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

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

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

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

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

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

16 Enter the networkhosts information for each NIC resource.

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

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

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

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

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

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

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

The Veritas Coordination Point Server is ONLINE

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

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

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

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

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

**To configure the CP server on an SFHA cluster**

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

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

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

   See "About the Veritas installer" on page 44.

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

   Enter **y** to confirm.

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

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

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

   The installer then runs the following preconfiguration checks:

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

7. Enter the name of the CP server.

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

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

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

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

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

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

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

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

11 Enter absolute path of the database.

```
CP Server uses an internal database to store the client information.
As the CP Server is being configured on SFHA cluster, the database should reside
on shared storage with vxfs file system. Please refer to documentation for
information on setting up of shared storage for CP server database.
Enter absolute path of the database: [b] /cpsdb
```

12 Verify and confirm the CP server configuration information.

```
CP Server configuration verification:

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

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

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

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

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

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

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

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

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

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

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

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

17 Enter the networkhosts information for each NIC resource.

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

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


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

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

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

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

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

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

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

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

```
Select one disk group as CP Server database disk group: [1-3,q] 3
1)  mycpsdg
2)  cpsdg1
3)  newcpsdg
```

21 Select the CP Server database volume.

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

```
Select one of the options below for CP Server database volume:
 1)  Create a new volume on disk group newcpsdg
 2)  Using an existing volume on disk group newcpsdg
```

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

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

```
1) newcpsvol
```

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

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

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

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

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

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

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

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

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

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

## Configuring the CP server 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 sample main.cf as an example:

See "Sample configuration files for CP server" on page 454.

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

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

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

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

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

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

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

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

5 Start VCS on all the cluster nodes.

```
# hastart
```

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

```
# hagrp -state CPSSG
```

Output similar to the following appears:

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

# Verifying the CP server configuration

Perform the following steps to verify the CP server configuration.

**To verify the CP server configuration**

1. Verify that the following configuration files are updated with the information you provided during the CP server configuration process:
   - `/etc/vxcps.conf` (CP server configuration file)
   - `/etc/VRTSvcs/conf/config/main.cf` (VCS configuration file)
   - `/etc/VRTScps/db` (default location for CP server database)
2. Run the `cpsadm` command to check if the vxcpserv process is listening on the configured Virtual IP.

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

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

# Configuring the CP server using the Web-based installer

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

**To configure SFCFSHA on a cluster**

1. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 144.
2. On the Select a task and a product page, select the task and the product as follows:

   | | |
   |---|---|
   | Task | I/O fencing configuration |
   | Product | Storage Foundation Cluster File System/HA |

   Click **Next**.
3. On the Select Cluster page, enter the system names where you want to configure SFCFSHA and click **Next**.
4. In the Confirmation dialog box, verify cluster information is correct and choose whether or not to configure I/O fencing.
   - To configure I/O fencing, click **Yes**.
   - To configure I/O fencing later, click **No**.
5. On the Select Option page, select Configure CP Server on VCS and click **Next**.

6 On the Configure CP Server page, provide CP server information, such as, name, virtual IPs, port numbers, and absolute path of the database to store the configuration details.

Click **Next**.

7 Configure the CP Server Service Group (CPSSG), select the number of NIC resources, and associate NIC resources to virtual IPs that are going to be used to configure the CP Server.

Click **Next**.

8 Configure network hosts for the CP server.

Click **Next**.

9 Configure disk group for the CP server.

Click **Next**.

---

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

---

10 Configure volume for the disk group associated to the CP server.

Click **Next**.

---

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

---

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

Chapter 8

# Configuring SFCFSHA

This chapter includes the following topics:


- Overview of tasks to configure SFCFSHA using the script-based installer
- Starting the software configuration
- Specifying systems for configuration
- Configuring the cluster name
- Configuring private heartbeat links
- Configuring the virtual IP of the cluster
- Configuring Veritas Storage Foundation Cluster File System High Availability in secure mode
- Configuring a secure cluster node by node
- Adding VCS users
- Configuring SMTP email notification
- Configuring SNMP trap notification
- Configuring global clusters
- Completing the SFCFSHA configuration
- Verifying and updating licenses on the system
- Configuring the Storage Foundation for Databases repository database after installation

# Overview of tasks to configure SFCFSHA using the script-based installer

Table 8-1 lists the tasks that are involved in configuring SFCFSHA using the script-based installer.

**Table 8-1** Tasks to configure SFCFSHA using the script-based installer

| Task | Reference |
|---|---|
| Start the software configuration | See "Starting the software configuration" on page 100. |
| Specify the systems where you want to configure SFCFSHA | See "Specifying systems for configuration" on page 100. |
| Configure the basic cluster | See "Configuring the cluster name" on page 101.<br>See "Configuring private heartbeat links" on page 102. |
| Configure virtual IP address of the cluster (optional) | See "Configuring the virtual IP of the cluster" on page 105. |
| Configure the cluster in secure mode (optional) | See " Configuring Veritas Storage Foundation Cluster File System High Availability in secure mode" on page 107. |
| Add VCS users (required if you did not configure the cluster in secure mode) | See "Adding VCS users" on page 112. |
| Configure SMTP email notification (optional) | See "Configuring SMTP email notification" on page 113. |
| Configure SNMP email notification (optional) | See "Configuring SNMP trap notification" on page 114. |
| Configure global clusters (optional)<br>**Note:** You must have enabled Global Cluster Option when you installed SFCFSHA. | See "Configuring global clusters" on page 116. |
| Complete the software configuration | See "Completing the SFCFSHA configuration" on page 117. |

# Starting the software configuration

You can configure SFCFSHA using the Veritas product installer or the installsfcfsha command.

---

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

---

**To configure SFCFSHA using the product installer**

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

   ```
   # ./installer
   ```

   The installer starts the product installation program with a copyright message and specifies the directory where the logs are created.
3. From the opening Selection Menu, choose: `C` for "Configure an Installed Product."
4. From the displayed list of products to configure, choose the corresponding number for your product:

   Storage Foundation Cluster File System High Availability

**To configure SFCFSHA using the installsfcfsha program**

1. Confirm that you are logged in as the superuser.
2. Start the `installsfcfsha` program, with the configure option.

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

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

   See “About the Veritas installer” on page 44.

   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 SFCFSHA. 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 SFCFSHA.

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

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

The installer does the following tasks:

- Checks that the local node running the installer can communicate with remote nodes
  If the installer finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases. If ssh binaries cannot communicate with remote nodes, the installer tries remsh binaries. And if both ssh and rsh binaries fail, the installer prompts to help the user to setup ssh or rsh binaries.
- Makes sure that the systems are running with the supported operating system
- Makes sure the installer started from the global zone
- Verifies that SFCFSHA is installed
- Exits if Veritas Storage Foundation Cluster File System High Availability 6.0.1 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 73.

# Configuring the cluster name

Enter the cluster information when the installer prompts you.

**To configure the cluster**

1 Review the configuration instructions that the installer presents.

2 Enter a unique cluster name.

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

# Configuring private heartbeat links

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

See "Using the UDP layer for LLT" on page 531.

The following procedure helps you configure LLT over Ethernet.

**To configure private heartbeat links**

1 Choose one of the following options at the installer prompt based on whether you want to configure LLT over Ethernet or UDP.

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

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

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

  The installer discovers and lists the network interface cards.

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

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

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

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

- For Solaris x64:
  You must not enter the network interface card that is used for the public network (typically e1000g0.)

```
Enter the NIC for the first private heartbeat link on sys1:
[b,q,?] e1000g1
Would you like to configure a second private heartbeat link?
[y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat link on sys1:
[b,q,?] e1000g2
Would you like to configure a third private heartbeat link?
[y,n,q,b,?](n)
```

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

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

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

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

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

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

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

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

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

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

6 Enter a unique cluster ID:

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

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

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

7 Verify and confirm the information that the installer summarizes.

# Configuring the virtual IP of the cluster

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

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

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

**To configure the virtual IP of the cluster**

1 Review the required information to configure the virtual IP of the cluster.

2 When the system prompts whether you want to configure the virtual IP, enter `y`.

3 Confirm whether you want to use the discovered public NIC on the first system.

Do one of the following:

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

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

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

Do one of the following:

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

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

5 Enter the virtual IP address for the cluster.

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

For IPv4:

- Enter the virtual IP address.

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

- Confirm the default netmask or enter another one:

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

- Verify and confirm the Cluster Virtual IP information.

  ```
  Cluster Virtual IP verification:

        NIC: bge0
        IP: 192.168.1.16
        Netmask: 255.255.240.0

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

For IPv6

- Enter the virtual IP address.

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

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

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

- Verify and confirm the Cluster Virtual IP information.

  ```
  Cluster Virtual IP verification:

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

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

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

See "Configuring a secure cluster node by node" on page 108.

# Configuring Veritas Storage Foundation Cluster File System High Availability in secure mode

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

**To configure SFCFSHA in secure mode**

1 Enter appropriate choices when the installer prompts you:

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

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

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

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

# Configuring a secure cluster node by node

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

Table 8-2 lists the tasks that you must perform to configure a secure cluster.

**Table 8-2** Configuring a secure cluster node by node

| Task | Reference |
|---|---|
| Configure security on one node | See "Configuring the first node" on page 108. |
| Configure security on the remaining nodes | See "Configuring the remaining nodes" on page 109. |
| Complete the manual configuration steps | See "Completing the secure cluster configuration" on page 110. |

## Configuring the first node

Perform the following steps on one node in your cluster.

**To configure security on the first node**

1 Ensure that you are logged in as superuser.

2 Enter the following command:

```
# /opt/VRTS/install/installsfcfsha<version> -securityonenode
```

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

See "About the Veritas installer" on page 44.

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

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

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

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

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

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

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

4 Copy the security configuration files from the location specified by the installer to temporary directories on the other nodes in the cluster.

## Configuring the remaining nodes

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

**To configure security on each remaining node**

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

   ```
   # /opt/VRTS/install/installsfcfsha<version> -securityonenode
   ```

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

   See "About the Veritas installer" on page 44.

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

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

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

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

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

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

# Completing the secure cluster configuration

Perform the following manual steps to complete the configuration.

**To complete the secure cluster configuration**

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

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

   # /opt/VRTSvcs/bin/hagrp -list Frozen=0

   # /opt/VRTSvcs/bin/hagrp -freeze groupname -persistent

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

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

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

3. On all nodes, stop the CmdServer.

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

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

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

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

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

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

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

7 On all nodes, start CmdServer.

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

8 On the first node, unfreeze the service groups.

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

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

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

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

# Adding VCS users

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

**To add VCS users**

1 Review the required information to add VCS users.

2 Reset the password for the Admin user, if necessary.

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

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

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

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

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

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

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

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

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

# Configuring SMTP email notification

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

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

**To configure SMTP email notification**

1 Review the required information to configure the SMTP email notification.

2 Specify whether you want to configure the SMTP notification.

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

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

See "Configuring SNMP trap notification" on page 114.

3 Provide information to configure SMTP notification.

Provide the following information:

- Enter the NIC information.

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

- Enter the SMTP server's host name.

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

- Enter the email address of each recipient.

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

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

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

4 Add more SMTP recipients, if necessary.

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

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

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

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

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

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

5 Verify and confirm the SMTP notification information.

```
NIC: bge0

SMTP Address: smtp.example.com
Recipient: ozzie@example.com receives email for Warning or
higher events
Recipient: harriet@example.com receives email for Error or
higher events

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

# Configuring SNMP trap notification

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

Note that you can also configure the notification after installation.

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

**To configure the SNMP trap notification**

1. Review the required information to configure the SNMP notification feature of VCS.
2. Specify whether you want to configure the SNMP notification.

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

   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 SFCFSHA based on the configuration details you provided.

   See "Configuring global clusters" on page 116.
3. Provide information to configure SNMP trap notification.

   Provide the following information:

   - Enter the NIC information.

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

   - Enter the SNMP trap daemon port.

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

   - Enter the SNMP console system name.

     ```
     Enter the SNMP console system name: [b,q,?] sys5
     ```

   - 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 sys5 [I=Information, W=Warning, E=Error,
     S=SevereError]: [b,q,?] E
     ```
4. Add more SNMP consoles, if necessary.

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

     ```
     Would you like to add another SNMP console? [y,n,q,b] (n) y
     Enter the SNMP console system name: [b,q,?] sys4
     ```

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

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

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

5 Verify and confirm the SNMP notification information.

```
NIC: bge0

SNMP Port: 162
Console: sys5 receives SNMP traps for Error or
higher events
Console: sys4 receives SNMP traps for SevereError or
higher events

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

# Configuring global clusters

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

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

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

---

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

---

**To configure the global cluster option**

1 Review the required information to configure the global cluster option.

2 Specify whether you want to configure the global cluster option.

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

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

3 Provide information to configure this cluster as global cluster.

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

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

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

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

For IPv4:

```
Global Cluster Option configuration verification:

      NIC: bge0
      IP: 10.198.89.22
      Netmask: 255.255.240.0

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

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

For IPv6

```
Global Cluster Option configuration verification:

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

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

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

# Completing the SFCFSHA configuration

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

**To complete the SFCFSHA configuration**

1 If prompted, press Enter at the following prompt.

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

2 Review the output as the installer stops various processes and performs the configuration. The installer then restarts SFCFSHA 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 SFCFSHA 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.<br>See "Configuring SFCFSHA using response files" on page 168. |

# Verifying and updating licenses on the system

After you install SFCFSHA, 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 118.

See "Updating product licenses" on page 119.

## 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 output to determine the following information:

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

# Updating product licenses

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

See "Replacing a SFCFSHA demo license with a permanent license" on page 119.

**To update product licenses using the installer command**

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

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

2 At the prompt, enter your license number.

**To update product licenses using the vxlicinst command**

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

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

## Replacing a SFCFSHA demo license with a permanent license

When a SFCFSHA 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 SFCFSHA on all nodes in the cluster:

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

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

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

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

   ```
   # vxlicrep
   ```

5. Start SFCFSHA on each node:

   ```
   # hastart
   ```

# Configuring the Storage Foundation for Databases repository database after installation

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

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

Chapter 9

# Configuring SFCFSHA clusters for data integrity

This chapter includes the following topics:


- Setting up disk-based I/O fencing using installsfcfsha
- Setting up server-based I/O fencing using installsfcfsha
- Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsfcfsha
- Enabling or disabling the preferred fencing policy


## Setting up disk-based I/O fencing using installsfcfsha

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

### Configuring disk-based I/O fencing using installsfcfsha

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

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

1 Start the installsfcfsha with `-fencing` option.

```
# /opt/VRTS/install/installsfcfsha<version> -fencing
```

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

See "About the Veritas installer" on page 44.

The installsfcfsha 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 SFCFSHA 6.0.1 is configured properly.

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

```
Select the fencing mechanism to be configured in this
Application Cluster [1-4,b,q] 2
```

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

- If the check fails, configure and enable VxVM before you repeat this procedure.
- If the check passes, then the program prompts you for the coordinator disk group information.

5 Choose whether to use an existing disk group or create a new disk group to configure as the coordinator disk group.

The program lists the available disk group names and provides an option to create a new disk group. Perform one of the following:

- To use an existing disk group, enter the number corresponding to the disk group at the prompt.
  The program verifies whether the disk group you chose has an odd number of disks and that the disk group has a minimum of three disks.
- To create a new disk group, perform the following steps:
  - Enter the number corresponding to the **Create a new disk group** option.

The program lists the available disks that are in the CDS disk format in the cluster and asks you to choose an odd number of disks with at least three disks to be used as coordinator disks.

Symantec recommends that you use three disks as coordination points for disk-based I/O fencing.

If the available VxVM CDS disks are less than the required, installer asks whether you want to initialize more disks as VxVM disks. Choose the disks you want to initialize as VxVM disks and then use them to create new disk group.

- Enter the numbers corresponding to the disks that you want to use as coordinator disks.
- Enter the disk group name.

6 Verify that the coordinator disks you chose meet the I/O fencing requirements.

You must verify that the disks are SCSI-3 PR compatible using the vxfentsthdw utility and then return to this configuration program.

See "Checking shared disks for I/O fencing" on page 125.

7 After you confirm the requirements, the program creates the coordinator disk group with the information you provided.

8 Enter the I/O fencing disk policy that you chose to use. For example:

```
Enter disk policy for the disk(s) (raw/dmp): [b,q,?] raw
```

The program also does the following:

- Populates the /etc/vxfendg file with this disk group information
- Populates the /etc/vxfenmode file on each cluster node with the I/O fencing mode information and with the SCSI-3 disk policy information

9 Verify and confirm the I/O fencing configuration information that the installer summarizes.

10 Review the output as the configuration program does the following:

- Stops VCS and I/O fencing on each node.
- Configures disk-based I/O fencing and starts the I/O fencing process.
- Updates the VCS configuration file main.cf if necessary.
- Copies the /etc/vxfenmode file to a date and time suffixed file /etc/vxfenmode-*date-time*. This backup file is useful if any future fencing configuration fails.
- Updates the I/O fencing configuration file /etc/vxfenmode.

- Starts VCS on each node to make sure that the SFCFSHA is cleanly configured to use the I/O fencing feature.

11 Review the output as the configuration program displays the location of the log files, the summary files, and the response files.

12 Configure the Coordination Point Agent.

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

13 Enter a name for the service group for the Coordination Point Agent.

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

14 Set the level two monitor frequency.

```
Do you want to set LevelTwoMonitorFreq? [y,n,q] (y)
```

15 Decide the value of the level two monitor frequency.

```
Enter the value of the LevelTwoMonitorFreq attribute: [b,q,?] (5)
```

Installer adds Coordination Point Agent and updates the main configuration file.

See "Configuring CoordPoint agent to monitor coordination points" on page 236.

# Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

**To initialize disks as VxVM disks**

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

```
# vxdisk list
```

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

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

```
# vxdisksetup -i device_name
```

The example specifies the CDS format:

```
# vxdisksetup -i c2t13d0
```

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

# Checking shared disks for I/O fencing

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

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

The vxfentsthdw utility has additional options suitable for testing many disks. Review the options for testing the disk groups (`-g`) and the disks that are listed in a file (`-f`). You can also test disks without destroying data using the `-r` option.

See the *Veritas Storage Foundation Cluster File System High Availability 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 125.
- Verifying that nodes have access to the same disk
  See "Verifying that the nodes have access to the same disk" on page 126.
- Testing the shared disks for SCSI-3
  See "Testing the disks using vxfentsthdw utility" on page 127.

## Verifying Array Support Library (ASL)

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

**To verify Array Support Library (ASL)**

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

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

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

The following output is a sample:

```
# vxddladm listsupport all


LIBNAME             VID                 PID
============================================================
libvx3par.so        3PARdata            VV
libvxCLARiiON.so    DGC                 All
libvxFJTSYe6k.so    FUJITSU             E6000
libvxFJTSYe8k.so    FUJITSU             All
libvxap.so          SUN                 All
libvxatf.so         VERITAS             ATFNODES
libvxcompellent.so  COMPELNT            Compellent Vol
libvxcopan.so       COPANSYS            8814, 8818
```

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

```
# vxdisk scandisks
```

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

## Verifying that the nodes have access to the same disk

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

**To verify that the nodes have access to the same disk**

1 Verify the connection of the shared storage for data to two of the nodes on which you installed SFCFSHA.

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/rdsk/c1t1d0s2 path on node A and the /dev/rdsk/c2t1d0s2 path on node B.

From node A, enter:

```
# vxfenadm -i /dev/rdsk/c1t1d0s2

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

The same serial number information should appear when you enter the equivalent command on node B using the /dev/rdsk/c2t1d0s2 path.

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

```
# vxfenadm -i /dev/rdsk/c3t1d2s2

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

## Testing the disks using vxfentsthdw utility

This procedure uses the /dev/rdsk/c1t1d0s2 disk in the steps.

If the utility does not show a message that states a disk is ready, the verification has failed. Failure of verification can be the result of an improperly configured disk array. The failure can also be due to a bad disk.

If the failure is due to a bad disk, remove and replace it. The vxfentsthdw utility indicates a disk can be used for I/O fencing with a message resembling:

```
The disk /dev/rdsk/c1t1d0s2 is ready to be configured for I/O Fencing on
node sys1
```

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

**To test the disks using vxfentsthdw utility**

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

2 From one node, start the utility.

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

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

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

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

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

Do you still want to continue : [y/n] (default: n) y
Enter the first node of the cluster: sys1
Enter the second node of the cluster: sys2
```

4 Enter the names of the disks that you want to check. Each node may know the same disk by a different name:

```
Enter the disk name to be checked for SCSI-3 PGR on node
IP_adrs_of_sys1 in the format:
for dmp: /dev/vx/rdmp/cxtxdxsx
for raw: /dev/rdsk/cxtxdxsx
Make sure it's the same disk as seen by nodes
IP_adrs_ofsys1 and IP_adrs_of_sys2
  /dev/rdsk/c2t13d0s2

Enter the disk name to be checked for SCSI-3 PGR on node
IP_adrs_of_sys2 in the format:
for dmp: /dev/vx/rdmp/cxtxdxsx
for raw: /dev/rdsk/cxtxdxsx
Make sure it's the same disk as seen by nodes
IP_adrs_ofsys1 and IP_adrs_of_sys2
  /dev/rdsk/c2t13d0s2
```

If the serial numbers of the disks are not identical, then the test terminates.

5 Review the output as the utility performs the checks and reports its activities.

6 If a disk is ready for I/O fencing on each node, the utility reports success for each node. For example, the utility displays the following message for the node sys1.

```
The disk is now ready to be configured for I/O Fencing on node
sys1

ALL tests on the disk /dev/rdsk/c1t1d0s2 have PASSED
The disk is now ready to be configured for I/O Fencing on node
sys1
```

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

# Setting up server-based I/O fencing using installsfcfsha

You can configure server-based I/O fencing for the SFCFSHA cluster using the installsfcfsha.

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 73.

See "Recommended CP server configurations" on page 78.

This section covers the following example procedures:

| | |
|---|---|
| Mix of CP servers and coordinator disks | See "To configure server-based fencing for the SFCFSHA cluster (one CP server and two coordinator disks)" on page 129. |
| Single CP server | See "To configure server-based fencing for the SFCFSHA cluster (single CP server)" on page 134. |

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

1 Depending on the server-based configuration model in your setup, make sure of the following:

- CP servers are configured and are reachable from the SFCFSHA cluster. The SFCFSHA cluster is also referred to as the application cluster or the client cluster.
  See "Setting up the CP server" on page 81.
- The coordination disks are verified for SCSI3-PR compliance.
  See "Checking shared disks for I/O fencing" on page 125.

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

```
# /opt/VRTS/install/installsfcfsha<version> -fencing
```

Where <version> is the specific release version. The installsfcfsha starts with a copyright message and verifies the cluster information.

See "About the Veritas installer" on page 44.

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 SFCFSHA 6.0.1 is configured properly.

4 Review the I/O fencing configuration options that the program presents. Type **1** to configure server-based I/O fencing.

```
Select the fencing mechanism to be configured in this
Application Cluster [1-4,b,q] 1
```

5 Make sure that the storage supports SCSI3-PR, and answer y at the following prompt.

```
Does your storage environment support SCSI3 PR? [y,n,q] (y)
```

6 Provide the following details about the coordination points at the installer prompt:

- Enter the total number of coordination points including both servers and disks. This number should be at least 3.

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

- Enter the total number of coordinator disks among the coordination points.

```
Enter the total number of disks among these:
[b] (0) 2
```

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

- Enter the total number of virtual IP addresses or the total number of fully qualified host names for each of the CP servers.

```
Enter the total number of Virtual IP addresses or fully
qualified host name for the
Coordination Point Server #1: [b,q,?] (1) 2
```

- Enter the virtual IP addresses or the fully qualified host name for each of the CP servers. The installer assumes these values to be identical as viewed from all the application cluster nodes.

```
Enter the Virtual IP address or fully qualified host name
#1 for the Coordination Point Server #1:
[b] 10.209.80.197
```

  The installer prompts for this information for the number of virtual IP addresses you want to configure for each CP server.

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

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

8 Provide the following coordinator disks-related details at the installer prompt:

- Enter the I/O fencing disk policy for the coordinator disks.

```
Enter disk policy for the disk(s) (raw/dmp):
[b,q,?] raw
```

- Choose the coordinator disks from the list of available disks that the installer displays. Ensure that the disk you choose is available from all the SFCFSHA (application cluster) nodes.
  The number of times that the installer asks you to choose the disks depends on the information that you provided in step 6. For example, if you had chosen to configure two coordinator disks, the installer asks you to choose the first disk and then the second disk:

```
Select disk number 1 for co-ordination point

1) c1t1d0s2
2) c2t1d0s2
```

```
3) c3t1d0s2

Please enter a valid disk which is available from all the
cluster nodes for co-ordination point [1-3,q] 1
```

- If you have not already checked the disks for SCSI-3 PR compliance in step 1, check the disks now.
  The installer displays a message that recommends you to verify the disks in another window and then return to this configuration procedure.
  Press Enter to continue, and confirm your disk selection at the installer prompt.
- Enter a disk group name for the coordinator disks or accept the default.

```
Enter the disk group name for coordinating disk(s):
[b] (vxfencoorddg)
```

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

For example:

```
Total number of coordination points being used: 3
Coordination Point Server ([VIP or FQHN]:Port):
    1. 10.109.80.197 ([10.109.80.197]:14250)
SCSI-3 disks:
    1. c1t1d0s2
    2. c2t1d0s2
Disk Group name for the disks in customized fencing: vxfencoorddg
Disk policy used for customized fencing: raw
```

The installer initializes the disks and the disk group and deports the disk group on the SFCFSHA (application cluster) node.

10 If the CP server is configured for security, the installer sets up secure communication between the CP server and the SFCFSHA (application cluster).

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

11 Verify and confirm the I/O fencing configuration information.

```
CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: clus1
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
```

12 Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the `/etc/vxfenmode` file with the appropriate details in each of the application cluster nodes.

```
Updating client cluster information on Coordination Point Server 10.210.80.197

Adding the client cluster to the Coordination Point Server 10.210.80.197 .......... Done

Registering client node sys1 with Coordination Point Server 10.210.80.197...... Done
Adding CPClient user for communicating to Coordination Point Server 10.210.80.197 .... Done
Adding cluster clus1 to the CPClient user on Coordination Point Server 10.210.80.197 .. Done

Registering client node sys2 with Coordination Point Server 10.210.80.197 ..... Done
Adding CPClient user for communicating to Coordination Point Server 10.210.80.197 .... Done
Adding cluster clus1 to the CPClient user on Coordination Point Server 10.210.80.197 ..Done

Updating /etc/vxfenmode file on sys1 ................................. Done
Updating /etc/vxfenmode file on sys2 ......... ....................... Done
```

See “About I/O fencing configuration files” on page 452.

13 Review the output as the installer stops and restarts the VCS and the fencing processes on each application cluster node, and completes the I/O fencing configuration.

14 Configure the CP agent on the SFCFSHA (application cluster). The Coordination Point Agent monitors the registrations on the coordination points.

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

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

15 Additionally the coordination point agent can also monitor changes to the Coordinator Disk Group constitution such as a disk being accidently deleted from the Coordinator Disk Group. The frequency of this detailed monitoring can be tuned with the LevelTwoMonitorFreq attribute. For example, if you set this attribute to 5, the agent will monitor the Coordinator Disk Group constitution every five monitor cycles.

Note that for the LevelTwoMonitorFreq attribute to be applicable there must be disks as part of the Coordinator Disk Group.

```
Enter the value of the LevelTwoMonitorFreq attribute: (5)

Adding Coordination Point Agent via sys1 .... Done
```

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

**To configure server-based fencing for the SFCFSHA cluster (single CP server)**

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

2 See "Setting up the CP server" on page 81.

3 Start the installsfcfsha with `-fencing` option.

```
# /opt/VRTS/install/installsfcfsha<version>  -fencing
```

Where <version> is the specific release version. The installsfcfsha starts with a copyright message and verifies the cluster information.

See "About the Veritas installer" on page 44.

Note the location of log files which you can access in the event of any problem with the configuration process.

4 Confirm that you want to proceed with the I/O fencing configuration at the prompt.

The program checks that the local node running the script can communicate with remote nodes and checks whether SFCFSHA 6.0.1 is configured properly.

5 Review the I/O fencing configuration options that the program presents. Type **1** to configure server-based I/O fencing.

```
Select the fencing mechanism to be configured in this
Application Cluster [1-4,b,q] 1
```

6 Make sure that the storage supports SCSI3-PR, and answer y at the following prompt.

```
Does your storage environment support SCSI3 PR? [y,n,q] (y)
```

7 Enter the total number of coordination points as **1**.

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

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

8 Provide the following CP server details at the installer prompt:

- Enter the total number of virtual IP addresses or the total numner of fully qualified host names for each of the CP servers.

```
Enter the total number of Virtual IP addresses or fully
qualified host name for the
Coordination Point Server #1: [b,q,?] (1) 2
```

- Enter the virtual IP address or the fully qualified host name for the CP server. The installer assumes these values to be identical as viewed from all the application cluster nodes.

```
Enter the Virtual IP address or fully qualified host name
#1 for the Coordination Point Server #1:
[b] 10.209.80.197
```

The installer prompts for this information for the number of virtual IP addresses you want to configure for each CP server.

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

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

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

For example:

```
Total number of coordination points being used: 1
Coordination Point Server ([VIP or FQHN]:Port):
    1. 10.209.80.197 ([10.209.80.197]:14250)
```

10 If the CP server is configured for security, the installer sets up secure communication between the CP server and the SFCFSHA (application cluster).

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

11 Verify and confirm the I/O fencing configuration information.

```
CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: clus1
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
```

12 Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the `/etc/vxfenmode` file with the appropriate details in each of the application cluster nodes.

The installer also populates the `/etc/vxfenmode` file with the entry `single_cp=1` for such single CP server fencing configuration.

```
Updating client cluster information on Coordination Point Server 10.210.80.197

Adding the client cluster to the Coordination Point Server 10.210.80.197 .......... Done

Registering client node sys1 with Coordination Point Server 10.210.80.197...... Done
Adding CPClient user for communicating to Coordination Point Server 10.210.80.197 .... Done
Adding cluster clus1 to the CPClient user on Coordination Point Server 10.210.80.197 .. Done

Registering client node sys2 with Coordination Point Server 10.210.80.197 ..... Done
Adding CPClient user for communicating to Coordination Point Server 10.210.80.197 .... Done
Adding cluster clus1 to the CPClient user on Coordination Point Server 10.210.80.197 .. Done

Updating /etc/vxfenmode file on sys1 ................................. Done
Updating /etc/vxfenmode file on sys2 ......... ....................... Done
```

See “About I/O fencing configuration files” on page 452.

13 Review the output as the installer stops and restarts the VCS and the fencing processes on each application cluster node, and completes the I/O fencing configuration.

14 Configure the CP agent on the SFCFSHA (application cluster).

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

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

Adding Coordination Point Agent via sys1 ... Done
```

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

# Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installsfcfsha

If you have installed VCS in virtual environments that do not support SCSI-3 PR-compliant storage, you can configure non-SCSI-3 fencing.

**To configure I/O fencing using the installsfcfsha in a non-SCSI-3 PR-compliant setup**

1 Start the installsfcfsha with `-fencing` option.

```
# /opt/VRTS/install/installsfcfsha<version> -fencing
```

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

See "About the Veritas installer" on page 44.

The installsfcfsha starts with a copyright message and verifies the cluster information.

2 Confirm that you want to proceed with the I/O fencing configuration at the prompt.

The program checks that the local node running the script can communicate with remote nodes and checks whether SFCFSHA 6.0.1 is configured properly.

3 Review the I/O fencing configuration options that the program presents. Type **1** to configure server-based I/O fencing.

```
Select the fencing mechanism to be configured in this
Application Cluster
[1-4,b,q] 1
```

4 Enter **n** to confirm that your storage environment does not support SCSI-3 PR.

```
Does your storage environment support SCSI3 PR?
[y,n,q] (y) n
```

5 Confirm that you want to proceed with the non-SCSI-3 I/O fencing configuration at the prompt.

6 Enter the number of CP server coordination points you want to use in your setup.

7 Enter the following details for each CP server:

- Enter the virtual IP address or the fully qualified host name.
- Enter the port address on which the CP server listens for connections. The default value is 14250. You can enter a different port address. Valid values are between 49152 and 65535.

The installer assumes that these values are identical from the view of the SFCFSHA cluster nodes that host the applications for high availability.

8 Verify and confirm the CP server information that you provided.

9 Verify and confirm the SFCFSHA cluster configuration information.

Review the output as the installer performs the following tasks:

- Updates the CP server configuration files on each CP server with the following details:
  - Registers each node of the SFCFSHA cluster with the CP server.
  - Adds CP server user to the CP server.
  - Adds SFCFSHA cluster to the CP server user.
- Updates the following configuration files on each node of the SFCFSHA cluster
  - `/etc/vxfenmode` file
  - `/etc/default/vxfen` file
  - `/etc/vxenviron` file
  - `/etc/llttab` file
  - `/etc/vxfentab` file

10 Review the output as the installer stops SFCFSHA on each node, starts I/O fencing on each node, updates the VCS configuration file main.cf, and restarts SFCFSHA with non-SCSI-3 server-based fencing.

   Confirm to configure the CP agent on the SFCFSHA cluster.

11 Confirm whether you want to send the installation information to Symantec.

12 After the installer configures I/O fencing successfully, note the location of summary, log, and response files that installer creates.

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

# 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 30.

**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 Veritas Cluster Server (VCS) configuration writable.

  ```
  # haconf -makerw
  ```

- Set the value of the cluster-level attribute `PreferredFencingPolicy` as **System**.

  ```
  # haclus -modify PreferredFencingPolicy System
  ```

- Set the value of the system-level attribute `FencingWeight` for each node in the cluster.

For example, in a two-node cluster, where you want to assign sys1 five times more weight compared to sys2, run the following commands:

```
# hasys -modify sys1 FencingWeight 50
# hasys -modify sys2 FencingWeight 10
```

- Save the VCS configuration.

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

4 To enable group-based race policy, perform the following steps:

- Make the VCS configuration writable.

```
# haconf -makerw
```

- Set the value of the cluster-level attribute `PreferredFencingPolicy` as **Group**.

```
# haclus -modify PreferredFencingPolicy Group
```

- Set the value of the group-level attribute `Priority` for each service group. For example, run the following command:

```
# hagrp -modify service_group Priority 1
```

Make sure that you assign a parent service group an equal or lower priority than its child service group. In case the parent and the child service groups are hosted in different subclusters, then the subcluster that hosts the child service group gets higher preference.

- Save the VCS configuration.

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

5 To view the fencing node weights that are currently set in the fencing driver, run the following command:

```
# vxfenconfig -a
```

**To disable preferred fencing for the I/O fencing configuration**

1 Make sure that the cluster is running with I/O fencing set up.

```
# vxfenadm -d
```

2 Make sure that the cluster-level attribute `UseFence` has the value set to **SCSI3**.

```
# haclus -value UseFence
```

3 To disable preferred fencing and use the default race policy, set the value of the cluster-level attribute `PreferredFencingPolicy` as **Disabled**.

```
# haconf -makerw
# haclus -modify PreferredFencingPolicy Disabled
# haconf -dump -makero
```

Section 4

# Installation using the Web-based installer


- Chapter 10. Installing SFCFSHA
- Chapter 11. Configuring SFCFSHA

Chapter 10

# Installing SFCFSHA

This chapter includes the following topics:


- About the Web-based installer
- Before using the Veritas Web-based installer
- Starting the Veritas Web-based installer
- Obtaining a security exception on Mozilla Firefox
- Performing a pre-installation check with the Veritas Web-based installer
- Installing SFCFSHA with the Web-based installer


## About the Web-based installer

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

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

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

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

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

See “Before using the Veritas Web-based installer” on page 144.

See “Starting the Veritas Web-based installer” on page 144.

# Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

**Table 10-1** Web-based installer requirements

| System | Function | Requirements |
|---|---|---|
| Target system | The systems where you plan to install the Veritas products. | Must be a supported platform for Veritas Storage Foundation Cluster File System High Availability 6.0.1. |
| Installation server | The server where you start the installation. The installation media is accessible from the installation server. | Must use the same operating system as the target systems and must be at one of the supported operating system update levels. |
| Administrative system | The system where you run the Web browser to perform the installation. | Must have a Web browser.<br>Supported browsers:<br>■ Internet Explorer 6, 7, and 8<br>■ Firefox 3.x and later |

# Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

**To start the Web-based installer**

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

```
# ./webinstaller start
```

The webinstaller script displays a URL. Note this URL.

---

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

The default listening port is 14172. If you have a firewall that blocks port 14172, use the `-port` option to use a free port instead.

---

2 On the administrative server, start the Web browser.

3 Navigate to the URL that the script displayed.

4 Certain browsers may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

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

5 Log in as superuser.

# Obtaining a security exception on Mozilla Firefox

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

The following instructions are general. They may change because of the rapid release cycle of Mozilla browsers.

**To obtain a security exception**

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

2 Click **I Understand the Risks**, or **You can add an exception**.

3 Click **Get Certificate** button.

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

5 Click **Confirm Security Exception** button.

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

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

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

**To perform a pre-installation check**

1. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 144.

2. On the Select a task and a product page, select **Perform a Pre-installation Check** from the **Task** drop-down list. Select **Veritas Storage Foundation and High Availability** from the **Product** drop-down list and click **Next**.
3. Select the Veritas Storage Foundation Cluster File System High Availability from the **Product** drop-down list, and click **Next**.
4. Indicate the systems on which to perform the precheck. Enter one or more system names, separated by spaces. Click **Next**.
5. The installer performs the precheck and displays the results.
6. If the validation completes successfully, click **Next**. The installer prompts you to begin the installation. Click **Yes** to install on the selected system. Click **No** to install later.
7. Click **Finish**. The installer prompts you for another task.

# Installing SFCFSHA with the Web-based installer

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

**To install SFCFSHA using the Web-based installer**

1. Perform preliminary steps.

   See "Performing a pre-installation check with the Veritas Web-based installer" on page 146.

2. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 144.

3. Select **Install a Product** from the **Task** drop-down list.
4. Select **Veritas Storage Foundation Cluster File System HA** 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 packages. Click **Next**.

7 Indicate the systems where you want to install. Separate multiple system names with spaces. Click **Next**.

8 If you have not yet configured a communication mode among systems, you have the option to let the installer configure ssh or rsh. If you choose to allow this configuration, select the communication mode and provide the superuser passwords for the systems.

9 After the validation completes successfully, click **Next** to install SFCFSHA 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 enable Veritas Replicator.
  - Choose whether you want to enable Global Cluster option.

  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 The product installation completes.

Review the output. Reboot nodes as requested. The installer may prompt you to perform other tasks.

12 If prompted, select the checkbox to specify whether you want to send your installation information to Symantec.

```
Would you like to send the information about this installation
to Symantec to help improve installation in the future?
```

Click **Finish**. The installer asks if you would like to read the summary file. Select **Yes** to read the summary file. If you select **No**, the installer prompts you for another task.

Chapter 11

# Configuring SFCFSHA

This chapter includes the following topics:


- Configuring SFCFSHA using the Web-based installer


## Configuring SFCFSHA using the Web-based installer

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

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

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

**To configure SFCFSHA on a cluster**

1. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 144.

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 Cluster File System/HA |

   Click **Next**.

3 On the Select Systems page, enter the system names where you want to configure SFCFSHA, and click **Next**.

Example: **sys1 sys2**

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

Click **Next** after the installer completes the system verification successfully.

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

To configure I/O fencing, click **Yes**.

To configure I/O fencing later, click **No**. You can configure I/O fencing later using the Web-based installer.

See "Configuring SFCFSHA for data integrity using the Web-based installer" on page 154.

You can also configure I/O fencing later using the `installsfcfsha<version> -fencing` command, the response files, or manually configure.

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

See "About the Veritas installer" on page 44.

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.<br>Note that you can have the installer check to see if the cluster ID is unique. Symantec recommends that you use the installer to check for duplicate cluster IDs in multi-cluster environments. |
| **Check duplicate cluster ID** | Select the check box if you want the installer to verify if the given cluster ID is unique in your private network. The verification is performed after you specify the heartbeat details in the following pages. The verification takes some time to complete. |
| **LLT Type** | Select an LLT type from the list. You can choose to configure LLT over UDP or over Ethernet. |
| **Number of Heartbeats** | Choose the number of heartbeat links you want to configure. |
| **Additional Low Priority Heartbeat NIC** | Select the check box if you want to configure a low priority link. The installer configures one heartbeat link as low priority link. |
| **Unique Heartbeat NICs per system** | For LLT over Ethernet, select the check box if you do not want to use the same NIC details to configure private heartbeat links on other systems.<br>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 On the Optional Configuration page, decide the optional VCS features that you want to configure. Click the corresponding tab to specify the details for each option:

**Security**

To configure a secure SFCFSHA cluster, select the **Configure secure cluster** check box.

If you want to perform this task later, do not select the **Configure secure cluster** check box. You can use the `-security` option of the installsfcfsha.

**Virtual IP**

- Select the **Configure Virtual IP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- Select the interface on which you want to configure the virtual IP.
- Enter a virtual IP address and value for the netmask.
  You can use an IPv4 or an IPv6 address.

**VCS Users**

- Reset the password for the Admin user, if necessary.
- Select the **Configure VCS users** option.
- Click **Add** to add a new user.
  Specify the user name, password, and user privileges for this user.

**SMTP**

- Select the **Configure SMTP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- If all the systems use the same NIC, select the NIC for the VCS Notifier to be used on all systems. If not, select the NIC to be used by each system.
- In the **SMTP Server** box, enter the domain-based hostname of the SMTP server. Example: smtp.yourcompany.com
- In the **Recipient** box, enter the full email address of the SMTP recipient. Example: user@yourcompany.com.
- In the **Event** list box, select the minimum security level of messages to be sent to each recipient.
- Click **Add** to add more SMTP recipients, if necessary.

**SNMP**

- Select the **Configure SNMP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- If all the systems use the same NIC, select the NIC for the VCS Notifier to be used on all systems. If not, select the NIC to be used by each system.
- In the **SNMP Port** box, enter the SNMP trap daemon port: (162).
- In the **Console System Name** box, enter the SNMP console system name.
- In the **Event** list box, select the minimum security level of messages to be sent to each console.
- Click **Add** to add more SNMP consoles, if necessary.

**GCO**

If you installed a valid HA/DR license, you can now enter the wide-area heartbeat link details for the global cluster that you would set up later.

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

- Select the **Configure GCO** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- Select a NIC.
- Enter a virtual IP address and value for the netmask. You can use an IPv4 or an IPv6 address.

Click **Next**.

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

9 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 11. Go to step 10 to configure fencing.

10 On the Select Fencing Type page, choose the type of fencing configuration:

| | |
|---|---|
| **Configure Coordination Point client based fencing** | Choose this option to configure server-based I/O fencing. |
| **Configure disk based fencing** | Choose this option to configure disk-based I/O fencing. |

Based on the fencing type you choose to configure, follow the installer prompts.

See "Configuring SFCFSHA for data integrity using the Web-based installer" on page 154.

11 Click **Next** to complete the process of configuring SFCFSHA.

On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

12 Select the checkbox to specify whether you want to send your installation information to Symantec.

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

# Configuring SFCFSHA for data integrity using the Web-based installer

After you configure SFCFSHA, you must configure the cluster for data integrity. Review the configuration requirements.

See "Configuring SFCFSHA using the Web-based installer" on page 149.

See "About planning to configure I/O fencing" on page 73.

Ways to configure I/O fencing using the Web-based installer:

- See "Configuring disk-based fencing for data integrity using the Web-based installer" on page 154.
- See "Configuring server-based fencing for data integrity using the Web-based installer" on page 157.
- See "Configuring fencing in disabled mode using the Web-based installer" on page 159.
- See "Online fencing migration mode using the Web-based installer" on page 160.

## Configuring disk-based fencing for data integrity using the Web-based installer

After you configure SFCFSHA, you must configure the cluster for data integrity. Review the configuration requirements.

See “Configuring SFCFSHA using the Web-based installer” on page 149.

See “About planning to configure I/O fencing” on page 73.

**To configure SFCFSHA for data integrity**

1 Start the Web-based installer.

See “Starting the Veritas Web-based installer” on page 144.

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

| | |
|---|---|
| **Task** | I/O fencing configuration |
| **Product** | Storage Foundation Cluster File System/HA |

Click **Next**.

3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.

4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

5 On the Select Fencing Type page, select the `Configure disk-based fencing` option.

6 In the Confirmation dialog box that appears, confirm whether your storage environment supports SCSI-3 PR.

You can configure non-SCSI-3 server-based fencing in a virtual environment that is not SCSI-3 PR compliant.

7 On the Configure Fencing page, the installer prompts for details based on the fencing type you chose to configure. Specify the coordination points details.

Click **Next**.

8 On the Configure Fencing page, specify the following information:

**Select a Disk Group** Select the **Create a new disk group** option or select one of the disk groups from the list.

- If you selected one of the disk groups that is listed, choose the fencing disk policy for the disk group.
- If you selected the **Create a new disk group** option, make sure you have SCSI-3 PR enabled disks, and click **Yes** in the confirmation dialog box.

  Click **Next**.

9 On the Create New DG page, specify the following information:

**New Disk Group Name** Enter a name for the new coordinator disk group you want to create.

**Select Disks** Select at least three disks to create the coordinator disk group.

If you want to select more than three disks, make sure to select an odd number of disks.

**Fencing Disk Policy** Choose the fencing disk policy for the disk group.

10 If you want to configure the Coordination Point agent on the client cluster, do the following:

- At the prompt for configuring the Coordination Point agent on the client cluster, click **Yes** and enter the Coordination Point agent service group name.
- If you want to set the LevelTwoMonitorFreq attribute, click Yes at the prompt and enter a value (0 to 65535).
- Follow the rest of the prompts to complete the Coordination Point agent configuration.

11 Click **Next** to complete the process of configuring I/O fencing.

On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

12 Select the checkbox to specify whether you want to send your installation information to Symantec.

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

## Configuring server-based fencing for data integrity using the Web-based installer

After you configure SFCFSHA, you must configure the cluster for data integrity. Review the configuration requirements.

See "Configuring SFCFSHA using the Web-based installer" on page 149.

See "About planning to configure I/O fencing" on page 73.

**To configure SFCFSHA for data integrity**

1 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 144.

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

| | |
|---|---|
| **Task** | I/O fencing configuration |
| **Product** | Storage Foundation Cluster File System/HA |

Click **Next**.

3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.

4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

5 On the Select Fencing Type page, select the `Configure server-based fencing` option.

6 In the Confirmation dialog box that appears, confirm whether your storage environment supports SCSI-3 PR.

You can configure non-SCSI-3 server-based fencing in a virtual environment that is not SCSI-3 PR compliant.

7 On the Configure Fencing page, the installer prompts for details based on the fencing type you chose to configure. Specify the coordination points details.

Click **Next**.

8 Provide the following details for each of the CP servers:

- Enter the virtual IP addresses or host names of the virtual IP address. The installer assumes these values to be identical as viewed from all the application cluster nodes.
- Enter the port that the CP server must listen on.
- Click **Next**.

9 If your server-based fencing configuration also uses disks as coordination points, perform the following steps:

- If you have not already checked the disks for SCSI-3 PR compliance, check the disks now, and click OK in the dialog box.
- If you do not want to use the default coordinator disk group name, enter a name for the new coordinator disk group you want to create.
- Select the disks to create the coordinator disk group.
- Choose the fencing disk policy for the disk group.
  The default fencing disk policy for the disk group is dmp.

10 In the Confirmation dialog box that appears, confirm whether the coordination points information you provided is correct, and click **Yes**.

11 Verify and confirm the I/O fencing configuration information.

The installer stops and restarts the VCS and the fencing processes on each application cluster node, and completes the I/O fencing configuration.

12 If you want to configure the Coordination Point agent on the client cluster, do the following:

- At the prompt for configuring the Coordination Point agent on the client cluster, click **Yes** and enter the Coordination Point agent service group name.
- Follow the rest of the prompts to complete the Coordination Point agent configuration.

13 Click **Next** to complete the process of configuring I/O fencing.

On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

14 Select the checkbox to specify whether you want to send your installation information to Symantec.

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

## Configuring fencing in disabled mode using the Web-based installer

After you configure SFCFSHA, you must configure the cluster for data integrity. Review the configuration requirements.

See "Configuring SFCFSHA using the Web-based installer" on page 149.

See "About planning to configure I/O fencing" on page 73.

**To configure SFCFSHA for data integrity**

1 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 144.

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

| | |
|---|---|
| **Task** | I/O fencing configuration |
| **Product** | Storage Foundation Cluster File System/HA |

Click **Next**.

3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.

4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

5 Fencing may be enabled, installer may prompt whether you want to reconfigure it.

Click **Yes**.

6 On the Select Fencing Type page, select the `Configure fencing in disabled mode` option.

7 Installer stops VCS before applying the selected fencing mode to the cluster.

---

**Note:** Unfreeze any frozen service group and unmount any file system that is mounted in the cluster.

---

Click **Yes**.

8 Installer restarts VCS on all systems of the cluster. I/O fencing is disabled.

9 Verify and confirm the I/O fencing configuration information.

On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

10 Select the checkbox to specify whether you want to send your installation information to Symantec.

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

## Online fencing migration mode using the Web-based installer

After you configure SFCFSHA, you must configure the cluster for data integrity. Review the configuration requirements.

See "Configuring SFCFSHA using the Web-based installer" on page 149.

See "About planning to configure I/O fencing" on page 73.

**To configure SFCFSHA for data integrity**

1 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 144.

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

| | |
|---|---|
| **Task** | I/O fencing configuration |
| **Product** | Storage Foundation Cluster File System/HA |

Click **Next**.

3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.

4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

5 Fencing may be enabled, installer may prompt whether you want to reconfigure it.

Click **Yes**.

6 On the Select Fencing Type page, select the `Online fencing migration` option.

7 The installer prompts to select the coordination points you want to remove from the currently configured coordination points.

Click **Next**.

8 Provide the number of Coordination point server and disk coordination points to be added to the configuration.

Click **Next**.

9 Provide the number of virtual IP addresses or Fully Qualified Host Name (FQHN) used for each coordination point server.

Click **Next**.

10 Provide the IP or FQHN and port number for each coordination point server.

Click **Next**.

11 Installer prompts to confirm the online migration coordination point servers.

Click **Yes**.

---

**Note:** If the coordination point servers are configured in secure mode, then the communication between coordination point servers and client servers happen in secure mode.

---

12 Installer proceeds with migration of the new coordination point servers. VCS is restarted during configuration.

Click **Next**.

13 You can add a Coordination Point agent to the client cluster and also provide name to the agent.

14 Click **Next**.

15 On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

16 Select the checkbox to specify whether you want to send your installation information to Symantec.

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

Section 5

# Automated installation using response files


- Chapter 12. Performing an automated SFCFSHA installation
- Chapter 13. Performing an automated SFCFSHA configuration
- Chapter 14. Performing an automated I/O fencing configuration using response files

Chapter 12

# Performing an automated SFCFSHA installation

This chapter includes the following topics:


- Installing SFCFSHA using response files
- Response file variables to install Veritas Storage Foundation Cluster File System High Availability
- Sample response file for Veritas Storage Foundation Cluster File System High Availability installation


## Installing SFCFSHA using response files

Typically, you can use the response file that the installer generates after you perform SFCFSHA installation on one cluster to install SFCFSHA on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

**To install SFCFSHA using response files**

1. Make sure the systems where you want to install SFCFSHA 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 SFCFSHA.
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

# ./installsfcfsha -responsefile /tmp/response_file
```

Where `/tmp/response_file` is the response file's full path name.

See "About the Veritas installer" on page 44.

# Response file variables to install Veritas Storage Foundation Cluster File System High Availability

Table 12-1 lists the response file variables that you can define to install SFCFSHA.

**Table 12-1** Response file variables for installing SFCFSHA

| Variable | Description |
|---|---|
| CFG{opt}{install} | Installs SFCFSHA packages. Configuration can be performed at a later time using the `-configure` option.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{installallpkgs}<br>or<br>CFG{opt}{installrecpkgs}<br>or<br>CFG{opt}{installminpkgs} | Instructs the installer to install SFCFSHA packages based on the variable that has the value set to 1:<br>■ installallpkgs: Installs all packages<br>■ installrecpkgs: Installs recommended packages<br>■ installminpkgs: Installs minimum packages<br>**Note:** Set only one of these variable values to 1. In addition to setting the value of one of these variables, you must set the variable `$CFG{opt}{install}` to 1.<br>List or scalar: scalar<br>Optional or required: required |

**Table 12-1** Response file variables for installing SFCFSHA *(continued)*

| Variable | Description |
|---|---|
| CFG{accepteula} | Specifies whether you agree with the EULA.pdf file on the media.<br>List or scalar: scalar<br>Optional or required: required |
| CFG{opt}{vxkeyless} | Installs the product with keyless license.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{license} | Installs the product with permanent license.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{keys}{hostname} | List of keys to be registered on the system if the variable `CFG{opt}{vxkeyless}` is set to 0 or if the variable `$CFG{opt}{licence}` is set to 1.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{systems} | List of systems on which the product is to be installed or uninstalled.<br>List or scalar: list<br>Optional or required: required |
| CFG{prod} | Defines the product to be installed or uninstalled.<br>List or scalar: scalar<br>Optional or required: required |
| CFG{opt}{keyfile} | Defines the location of an ssh keyfile that is used to communicate with all remote systems.<br>List or scalar: scalar<br>Optional or required: optional |

**Table 12-1** Response file variables for installing SFCFSHA *(continued)*

| Variable | Description |
|---|---|
| CFG{opt}{pkgpath} | Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{tmppath} | Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{rsh} | Defines that *rsh* must be used instead of ssh as the communication method between systems.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{logpath} | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{prodmode} | List of modes for product<br>List or scalar: list<br>Optional or required: optional |

# Sample response file for Veritas Storage Foundation Cluster File System High Availability installation

The following example shows a response file for installing Veritas Storage Foundation Cluster File System High Availability.

```
##############################################
#Auto generated sfcfsha responsefile #
##############################################
```

```
our %CFG;
$CFG{accepteula}=1;
$CFG{opt}{rsh}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vr}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{prod}="SFCFSHA60";
$CFG{systems}=[ qw( sys1 sys2 ) ];
$CFG{opt}{logpath}="/opt/VRTS/install/logs/installsfcfs-xxxxxx/
installsfcfs-xxxxxx.response";

1;
```

Chapter 13

# Performing an automated SFCFSHA configuration

This chapter includes the following topics:


- Configuring SFCFSHA using response files
- Response file variables to configure Veritas Storage Foundation Cluster File System High Availability
- Sample response file for Veritas Storage Foundation Cluster File System High Availability configuration


## Configuring SFCFSHA using response files

Typically, you can use the response file that the installer generates after you perform SFCFSHA configuration on one cluster to configure SFCFSHA on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

**To configure SFCFSHA using response files**

1. Make sure the SFCFSHA packages are installed on the systems where you want to configure SFCFSHA.
2. Copy the response file to one of the cluster systems where you want to configure SFCFSHA.

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 Veritas Storage Foundation Cluster File System High Availability" on page 169.

4 Start the configuration from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/installsfcfsha<version>
-responsefile /tmp/response_file
```

Where *<version>* is the specific release version, and */tmp/response_file* is the response file's full path name.

See "About the Veritas installer" on page 44.

# Response file variables to configure Veritas Storage Foundation Cluster File System High Availability

Table 13-1 lists the response file variables that you can define to configure SFCFSHA.

**Table 13-1** Response file variables specific to configuring Veritas Storage Foundation Cluster File System High Availability

| Variable | List or Scalar | Description |
|---|---|---|
| $CFG{config_cfs} | Scalar | Performs the Cluster File System configuration for SFCFSHA.<br>(Required)<br>Set the value to 1 to configure Cluster File System for SFCFSHA. |
| CFG{opt}{configure} | Scalar | Performs the configuration if the packages are already installed.<br>(Required)<br>Set the value to 1 to configure SFCFSHA. |
| CFG{accepteula} | Scalar | Specifies whether you agree with EULA.pdf on the media.<br>(Required) |

**Table 13-1** Response file variables specific to configuring Veritas Storage Foundation Cluster File System High Availability *(continued)*

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{systems} | List | List of systems on which the product is to be configured.<br>(Required) |
| CFG{prod} | Scalar | Defines the product to be configured.<br>The value is SFCFSHA60 for SFCFSHA<br>(Required) |
| CFG{opt}{keyfile} | Scalar | Defines the location of an ssh keyfile that is used to communicate with all remote systems.<br>(Optional) |
| CFG{opt}{rsh} | Scalar | Defines that *rsh* must be used instead of ssh as the communication method between systems.<br>(Optional) |
| CFG{opt}{logpath} | Scalar | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.<br>**Note:** The installer copies the response files and summary files also to the specified *logpath* location.<br>(Optional) |
| CFG{uploadlogs} | Scalar | Defines a Boolean value 0 or 1.<br>The value 1 indicates that the installation logs are uploaded to the Symantec Web site.<br>The value 0 indicates that the installation logs are not uploaded to the Symantec Web site.<br>(Optional) |

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (csgnic, csgvip, and csgnetmask) must be defined if any are defined. The same is true for the SMTP notification (smtpserver, smtprecp, and smtprsev), the SNMP trap notification (snmpport, snmpcons, and snmpcsev), and the Global Cluster Option (gconic, gcovip, and gconetmask).

Table 13-2 lists the response file variables that specify the required information to configure a basic SFCFSHA cluster.

**Table 13-2** Response file variables specific to configuring a basic SFCFSHA cluster

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_clusterid} | Scalar | An integer between 0 and 65535 that uniquely identifies the cluster.<br>(Required) |
| CFG{vcs_clustername} | Scalar | Defines the name of the cluster.<br>(Required) |
| CFG{vcs_allowcomms} | Scalar | Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start).<br>(Required) |
| CFG{fencingenabled} | Scalar | In a SFCFSHA configuration, defines if fencing is enabled.<br>Valid values are 0 or 1.<br>(Required) |

Table 13-3 lists the response file variables that specify the required information to configure LLT over Ethernet.

**Table 13-3** Response file variables specific to configuring private LLT over Ethernet

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_lltlink#}<br>{"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.<br>You must enclose the system name within double quotes.<br>(Required) |
| CFG{vcs_lltlinklowpri#}<br>{"system"} | Scalar | Defines a low priority heartbeat link. Typically, lltlinklowpri is used on a public network link to provide an additional layer of communication.<br>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.<br>You must enclose the system name within double quotes.<br>(Optional) |

Table 13-4 lists the response file variables that specify the required information to configure LLT over UDP.

**Table 13-4** Response file variables specific to configuring LLT over UDP

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{lltoverudp}=1 | Scalar | Indicates whether to configure heartbeat link using LLT over UDP.<br>(Required) |

**Table 13-4** Response file variables specific to configuring LLT over UDP *(continued)*

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_udplink<n>_address}<br>{<system1>} | Scalar | Stores the IP address (IPv4 or IPv6) that the heartbeat link uses on node1.<br>You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links.<br>(Required) |
| CFG<br>{vcs_udplinklowpri<n>_address}<br>{<system1>} | Scalar | Stores the IP address (IPv4 or IPv6) that the low priority heartbeat link uses on node1.<br>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.<br>(Required) |
| CFG{vcs_udplink<n>_port}<br>{<system1>} | Scalar | Stores the UDP port (16-bit integer value) that the heartbeat link uses on node1.<br>You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links.<br>(Required) |
| CFG{vcs_udplinklowpri<n>_port}<br>{<system1>} | Scalar | Stores the UDP port (16-bit integer value) that the low priority heartbeat link uses on node1.<br>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.<br>(Required) |

**Table 13-4** Response file variables specific to configuring LLT over UDP *(continued)*

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_udplink<n>_netmask}<br>{<system1>} | Scalar | Stores the netmask (prefix for IPv6) that the heartbeat link uses on node1.<br>You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links.<br>(Required) |
| CFG{vcs_udplinklowpri<n>_netmask}<br>{<system1>} | Scalar | Stores the netmask (prefix for IPv6) that the low priority heartbeat link uses on node1.<br>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.<br>(Required) |

Table 13-5 lists the response file variables that specify the required information to configure virtual IP for SFCFSHA cluster.

**Table 13-5** Response file variables specific to configuring virtual IP for SFCFSHA cluster

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_csgnic}<br>{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.<br>(Optional) |
| CFG{vcs_csgvip} | Scalar | Defines the virtual IP address for the cluster.<br>(Optional) |
| CFG{vcs_csgnetmask} | Scalar | Defines the Netmask of the virtual IP address for the cluster.<br>(Optional) |

Table 13-6 lists the response file variables that specify the required information to configure the SFCFSHA cluster in secure mode.

**Table 13-6** Response file variables specific to configuring SFCFSHA cluster in secure mode

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_eat_security} | Scalar | Specifies if the cluster is in secure enabled mode or not. |
| CFG{opt}{securityonenode} | Scalar | Specifies that the securityonenode option is being used. |
| CFG{securityonenode_menu} | Scalar | Specifies the menu option to choose to configure the secure cluster one at a time.<br>■ 1—Configure the first node<br>■ 2—Configure the other node |
| CFG{security_conf_dir} | Scalar | Specifies the directory where the configuration files are placed. |
| CFG{opt}{security} | Scalar | Specifies that the security option is being used. |
| CFG{opt}{fips} | Scalar | Specifies that the FIPS option is being used. |
| CFG{vcs_eat_security_fips} | Scalar | Specifies that the enabled security is FIPS compliant. |

Table 13-7 lists the response file variables that specify the required information to configure VCS users.

**Table 13-7** Response file variables specific to configuring VCS users

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_userenpw} | List | List of encoded passwords for VCS users<br>The value in the list can be "Administrators Operators Guests"<br>**Note:** The order of the values for the vcs_userenpw list must match the order of the values in the vcs_username list.<br>(Optional) |
| CFG{vcs_username} | List | List of names of VCS users<br>(Optional) |
| CFG{vcs_userpriv} | List | List of privileges for VCS users<br>**Note:** The order of the values for the vcs_userpriv list must match the order of the values in the vcs_username list.<br>(Optional) |

Table 13-8 lists the response file variables that specify the required information to configure VCS notifications using SMTP.

**Table 13-8** Response file variables specific to configuring VCS notifications using SMTP

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_smtpserver} | Scalar | Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for Web notification.<br>(Optional) |
| CFG{vcs_smtprecp} | List | List of full email addresses (example: user@symantecexample.com) of SMTP recipients.<br>(Optional) |

**Table 13-8** Response file variables specific to configuring VCS notifications using SMTP *(continued)*

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_smtprsev} | List | Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SMTP recipients are to receive. Note that the ordering of severity levels must match that of the addresses of SMTP recipients.<br>(Optional) |

Table 13-9 lists the response file variables that specify the required information to configure VCS notifications using SNMP.

**Table 13-9** Response file variables specific to configuring VCS notifications using SNMP

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_snmpport} | Scalar | Defines the SNMP trap daemon port (default=162).<br>(Optional) |
| CFG{vcs_snmpcons} | List | List of SNMP console system names<br>(Optional) |
| CFG{vcs_snmpcsev} | List | Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names.<br>(Optional) |

Table 13-10 lists the response file variables that specify the required information to configure SFCFSHA global clusters.

**Table 13-10** Response file variables specific to configuring SFCFSHA global clusters

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{vcs_gconic}<br>{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.<br>(Optional) |
| CFG{vcs_gcovip} | Scalar | Defines the virtual IP address to that the Global Cluster Option uses.<br>(Optional) |
| CFG{vcs_gconetmask} | Scalar | Defines the Netmask of the virtual IP address that the Global Cluster Option uses.<br>(Optional) |

# Sample response file for Veritas Storage Foundation Cluster File System High Availability configuration

The following example shows a response file for configuring Veritas Storage Foundation Cluster File System High Availability.

```
##############################################
#Auto generated sfcfsha responsefile #
##############################################


our %CFG;
$CFG{accepteula}=1;
$CFG{opt}{rsh}=1;
$CFG{opt}{trace}=0;
$CFG{vcs_allowcomms}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vr}=1;
$CFG{opt}{configure}=1;
$CFG{prod}="SFCFSHA60";
$CFG{systems}=[ qw( system01 system02 ) ];
$CFG{sfcfs_cvmtimeout}=200;
```

```
$CFG{sfcfs_fencingenabled}=0;
$CFG{vm_newnames_file}{system01}=0;
$CFG{vm_restore_cfg}{system01}=0;
$CFG{vm_newnames_file}{system02}=0;
$CFG{vm_restore_cfg}{system02}=0;
$CFG{vcs_clusterid}=127;
$CFG{vcs_clustername}="uxrt6_sol";
$CFG{vcs_username}=[ qw(admin operator) ];
$CFG{vcs_userenpw}=[ qw(JlmElgLimHmmKumGlj
bQOsOUnVQoOUnTQsOSnUQuOUnPQtOS) ];
$CFG{vcs_userpriv}=[ qw(Administrators Operators) ];
$CFG{vcs_lltlink1}{system01}="bge1";
$CFG{vcs_lltlink2}{system01}="bge2";
$CFG{vcs_lltlink1}{system02}="bge1";
$CFG{vcs_lltlink2}{system02}="bge2";
$CFG{vcs_enabled}=1;
$CFG{opt}{logpath}="/opt/VRTS/install/logs/installsfcfs-xxxxxx/
installsfcfs-xxxxxx.response";

1;
```

Chapter 14

# Performing an automated I/O fencing configuration using response files

This chapter includes the following topics:


- Configuring I/O fencing using response files
- Response file variables to configure disk-based I/O fencing
- Sample response file for configuring disk-based I/O fencing
- Configuring CP server using response files
- Response file variables to configure server-based I/O fencing
- Sample response file for configuring server-based I/O fencing
- Response file variables to configure non-SCSI-3 server-based I/O fencing
- Sample response file for configuring non-SCSI-3 server-based I/O fencing


## Configuring I/O fencing using response files

Typically, you can use the response file that the installer generates after you perform I/O fencing configuration to configure I/O fencing for SFCFSHA.

**To configure I/O fencing using response files**

1. Make sure that SFCFSHA 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 73.
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 184.

   See "Sample response file for configuring server-based I/O fencing" on page 190.
4. Edit the values of the response file variables as necessary.

   See "Response file variables to configure disk-based I/O fencing" on page 181.

   See "Response file variables to configure server-based I/O fencing" on page 189.
5. Start the configuration from the system to which you copied the response file. For example:

   ```
   # /opt/VRTS/install/installsfcfsha<version>
   -responsefile /tmp/response_file
   ```

   Where *<version>* is the specific release version, and */tmp/response_file* is the response file's full path name.

   See "About the Veritas installer" on page 44.

# Response file variables to configure disk-based I/O fencing

Table 14-1 lists the response file variables that specify the required information to configure disk-based I/O fencing for SFCFSHA.

**Table 14-1** Response file variables specific to configuring disk-based I/O fencing

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{opt}{fencing} | Scalar | Performs the I/O fencing configuration.<br>(Required) |

**Table 14-1** Response file variables specific to configuring disk-based I/O fencing *(continued)*

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{fencing_option} | Scalar | Specifies the I/O fencing configuration mode.<br>■ 1—Coordination Point Server-based I/O fencing<br>■ 2—Coordinator disk-based I/O fencing<br>■ 3—Disabled mode<br>■ 4—Fencing migration when the cluster is online<br>(Required) |
| CFG {fencing_scsi3_disk_policy} | Scalar | Specifies the I/O fencing mechanism.<br>This variable is not required if you had configured fencing in disabled mode. For disk-based fencing, you must configure the fencing_scsi3_disk_policy variable and either the fencing_dgname variable or the fencing_newdg_disks variable.<br>(Optional) |
| CFG{fencing_dgname} | Scalar | Specifies the disk group for I/O fencing.<br>(Optional)<br>**Note:** You must define the fencing_dgname variable to use an existing disk group. If you want to create a new disk group, you must use both the fencing_dgname variable and the fencing_newdg_disks variable. |

**Table 14-1** Response file variables specific to configuring disk-based I/O fencing *(continued)*

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{fencing_newdg_disks} | List | Specifies the disks to use to create a new disk group for I/O fencing.<br>(Optional)<br>**Note:** You must define the fencing_dgname variable to use an existing disk group. If you want to create a new disk group, you must use both the fencing_dgname variable and the fencing_newdg_disks variable. |
| CFG{fencing_cpagent_monitor_freq} | Scalar | Specifies the frequency at which the Coordination Point Agent monitors for any changes to the Coordinator Disk Group constitution.<br>**Note:** Coordination Point Agent can also monitor changes to the Coordinator Disk Group constitution such as a disk being accidently deleted from the Coordinator Disk Group. The frequency of this detailed monitoring can be tuned with the LevelTwoMonitorFreq attribute. For example, if you set this attribute to 5, the agent will monitor the Coordinator Disk Group constitution every five monitor cycles. If LevelTwoMonitorFreq attribute is not set, the agent will not monitor any changes to the Coordinator Disk Group. 0 means not to monitor the Coordinator Disk Group constitution. |
| CFG {fencing_config_cpagent} | Scalar | Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not.<br>Enter "0" if you do not want to configure the Coordination Point agent using the installer.<br>Enter "1" if you want to use the installer to configure the Coordination Point agent. |

**Table 14-1** Response file variables specific to configuring disk-based I/O fencing *(continued)*

| Variable | List or Scalar | Description |
|---|---|---|
| CFG {fencing_cpagentgrp} | Scalar | Name of the service group which will have the Coordination Point agent resource as part of it.<br>**Note:** This field is obsolete if the **fencing_config_cpagent** field is given a value of '0'. |

# Sample response file for configuring disk-based I/O fencing

Review the disk-based I/O fencing response file variables and their definitions.

See "Response file variables to configure disk-based I/O fencing" on page 181.

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

$CFG{fencing_config_cpagent}=1;
$CFG{fencing_cpagent_monitor_freq}=5;
$CFG{fencing_cpagentgrp}="vxfen";
$CFG{fencing_dgname}="fencingdg1";
$CFG{fencing_newdg_disks}=[ qw(emc_clariion0_155
 emc_clariion0_162 emc_clariion0_163) ];
$CFG{fencing_option}=2;
$CFG{fencing_scsi3_disk_policy}="dmp";
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;

$CFG{prod}="SFCFSHA60";

$CFG{systems}=[ qw(pilot25) ];
$CFG{vcs_clusterid}=32283;
$CFG{vcs_clustername}="whf";
1;
```

# Configuring CP server using response files

You can configure a CP server using a generated responsefile.

**On a single node VCS cluster:**

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

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

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

  See "About the Veritas installer" on page 44.

**On a SFHA cluster:**

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

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

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

  See "About the Veritas installer" on page 44.

## Response file variables to configure CP server

Table 14-2 shows the response file variables reuired to configure CP server.

**Table 14-2** describes response file variables to configure CP server

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{opt}{configcps} | Scalar | This variable performs CP server configuration task |
| CFG{cps_singlenode_config} | Scalar | This variable describes if the CP server will be configured on a singlenode VCS cluster |
| CFG{cps_sfha_config} | Scalar | This variable describes if the CP server will be configured on a SFHA cluster |
| CFG{cps_unconfig} | Scalar | This variable describes if the CP server will be unconfigured |

**Table 14-2** describes response file variables to configure CP server *(continued)*

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

**Table 14-2** describes response file variables to configure CP server *(continued)*

| Variable | List or Scalar | Description |
|---|---|---|
| CFG{cps_newvol_volsize} | Scalar | This variable describes the volume size to create a new volume for the CP server database |
| CFG{cps_delete_database} | Scalar | This variable describes if deleting the database of the CP server during the unconfiguration |
| CFG{cps_delete_config_log} | Scalar | This variable describes if deleting the config files and log files of the CP server during the unconfiguration |

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

Review the response file variables and their definitions.

See Table 14-2 on page 185.

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

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

```
$CFG{vcs_clustername}="vcs92216";


1;
```

## Sample response file for configuring the CP server on SFHA cluster

Review the response file variables and their definitions.

See Table 14-2 on page 185.

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

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

1;
```

# Response file variables to configure server-based I/O fencing

You can use a coordination point server-based fencing response file to configure server-based customized I/O fencing.

Table 14-3 lists the fields in the response file that are relevant for server-based customized I/O fencing.

**Table 14-3** Coordination point server (CP server) based fencing response file definitions

| Response file field | Definition |
|---|---|
| CFG {fencing_config_cpagent} | Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not.<br>Enter "0" if you do not want to configure the Coordination Point agent using the installer.<br>Enter "1" if you want to use the installer to configure the Coordination Point agent. |
| CFG {fencing_cpagentgrp} | Name of the service group which will have the Coordination Point agent resource as part of it.<br>**Note:** This field is obsolete if the `fencing_config_cpagent` field is given a value of '0'. |
| CFG {fencing_cps} | Virtual IP address or Virtual hostname of the CP servers. |
| CFG {fencing_reusedg} | This response file field indicates whether to reuse an existing DG name for the fencing configuration in customized fencing (CP server and coordinator disks).<br>Enter either a "1" or "0".<br>Entering a "1" indicates reuse, and entering a "0" indicates do not reuse.<br>When reusing an existing DG name for the mixed mode fencing configuration. you need to manually add a line of text , such as "$CFG{fencing_reusedg}=0" or "$CFG{fencing_reusedg}=1" before proceeding with a silent installation. |

**Table 14-3** Coordination point server (CP server) based fencing response file definitions *(continued)*

| Response file field | Definition |
|---|---|
| CFG {fencing_dgname} | The name of the disk group to be used in the customized fencing, where at least one disk is being used. |
| CFG {fencing_disks} | The disks being used as coordination points if any. |
| CFG {fencing_ncp} | Total number of coordination points being used, including both CP servers and disks. |
| CFG {fencing_ndisks} | The number of disks being used. |
| CFG {fencing_cps_vips} | The virtual IP addresses or the fully qualified host names of the CP server. |
| CFG {fencing_cps_ports} | The port that the virtual IP address or the fully qualified host name of the CP server listens on. |
| CFG {fencing_scsi3_disk_policy} | The disk policy that the customized fencing uses.<br>The value for this field is either "raw" or "dmp" |

# Sample response file for configuring server-based I/O fencing

The following is a sample response file used for server-based I/O fencing:

```
$CFG{fencing_config_cpagent}=0;
$CFG{fencing_cps}=[ qw(10.200.117.145) ];
$CFG{fencing_cps_vips}{"10.200.117.145"}=[ qw(10.200.117.145) ];
$CFG{fencing_dgname}="vxfencoorddg";
$CFG{fencing_disks}=[ qw(emc_clariion0_37 emc_clariion0_13) ];
$CFG{fencing_scsi3_disk_policy}="raw";
$CFG{fencing_ncp}=3;
$CFG{fencing_ndisks}=2;
$CFG{fencing_cps_ports}{"10.200.117.145"}=14250;
$CFG{fencing_reusedg}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="SFCFSHA60";
$CFG{systems}=[ qw(sys1 sys2) ];
$CFG{vcs_clusterid}=1256;
```

```
$CFG{vcs_clustername}="clus1";
$CFG{fencing_option}=1;
```

# Response file variables to configure non-SCSI-3 server-based I/O fencing

Table 14-4 lists the fields in the response file that are relevant for non-SCSI-3 server-based customized I/O fencing.

See "About I/O fencing for SFCFSHA in virtual machines that do not support SCSI-3 PR" on page 27.

**Table 14-4** Non-SCSI-3 server-based I/O fencing response file definitions

| Response file field | Definition |
|---|---|
| CFG{non_scsi3_fencing} | Defines whether to configure non-SCSI-3 server-based I/O fencing.<br>Valid values are 1 or 0. Enter 1 to configure non-SCSI-3 server-based I/O fencing. |
| CFG {fencing_config_cpagent} | Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not.<br>Enter "0" if you do not want to configure the Coordination Point agent using the installer.<br>Enter "1" if you want to use the installer to configure the Coordination Point agent. |
| CFG {fencing_cpagentgrp} | Name of the service group which will have the Coordination Point agent resource as part of it.<br>**Note:** This field is obsolete if the `fencing_config_cpagent` field is given a value of '0'. |
| CFG {fencing_cps} | Virtual IP address or Virtual hostname of the CP servers. |
| CFG {fencing_cps_vips} | The virtual IP addresses or the fully qualified host names of the CP server. |
| CFG {fencing_ncp} | Total number of coordination points (CP servers only) being used. |
| CFG {fencing_cps_ports} | The port of the CP server that is denoted by *cps* . |

# Sample response file for configuring non-SCSI-3 server-based I/O fencing

The following is a sample response file used for non-SCSI-3 server-based I/O fencing :

```
$CFG{fencing_config_cpagent}=0;
$CFG{fencing_cps}=[ qw(10.198.89.251 10.198.89.252 10.198.89.253) ];
$CFG{fencing_cps_vips}{"10.198.89.251"}=[ qw(10.198.89.251) ];
$CFG{fencing_cps_vips}{"10.198.89.252"}=[ qw(10.198.89.252) ];
$CFG{fencing_cps_vips}{"10.198.89.253"}=[ qw(10.198.89.253) ];
$CFG{fencing_ncp}=3;
$CFG{fencing_ndisks}=0;
$CFG{fencing_cps_ports}{"10.198.89.251"}=14250;
$CFG{fencing_cps_ports}{"10.198.89.252"}=14250;
$CFG{fencing_cps_ports}{"10.198.89.253"}=14250;
$CFG{non_scsi3_fencing}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="SFCFSHA60";
$CFG{systems}=[ qw(sys1 sys2) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{fencing_option}=1;
```

Section 6

# Installation using operating system-specific methods


- Chapter 15. Installing SFCFSHA using operating system-specific methods
- Chapter 16. Configuring SFCFSHA using operating system-specific methods
- Chapter 17. Manually configuring SFCFSHA clusters for data integrity

Chapter 15

# Installing SFCFSHA using operating system-specific methods

This chapter includes the following topics:


- Installing SFCFSHA on Solaris 11 using Automated Installer
- Manually installing packages on Solaris brand non-global zones
- Manually installing packages on solaris10 brand zones
- Installing SFCFSHA on Solaris 10 using JumpStart
- Installing SFCFSHA using the system command


## Installing SFCFSHA on Solaris 11 using Automated Installer

You can use the Oracle Solaris Automated Installer (AI) to install the Solaris 11 operating system on multiple client systems in a network. AI performs a hands-free installation (automated installation without manual interactions) of both x86 and SPARC systems. You can also use AI media (AI bootable image, provided by Oracle, which can be downloaded from the Oracle Web site) to install the Oracle Solaris OS on a single SPARC or x86 platform. All cases require access to a package repository on the network to complete the installation.

# About Automated Installation

AI automates the installation of the Oracle Solaris 11 OS on one or more SPARC or x86 clients in a network. Automated Installation applies to Solaris 11 only. You can install the Oracle Solaris OS on many different types of clients.The clients can differ in:

- architecture
- memory charecteristics
- MAC address
- IP address
- CPU

The installations can differ depending on specifications including network configuration and packages installed.

**An automated installation of a client in a local network consists of the following high-level steps:**

1. A client system boots and gets IP information from the DHCP server
2. Characteristics of the client determine which AI service and which installation instructions are used to install the client.
3. The installer uses the AI service instructions to pull the correct packages from the package repositories and install the Oracle Solaris OS on the client.

# Using Automated Installer

To use Automated Installer to install systems over the network, set up DHCP and set up an AI service on an AI server. The DHCP server and AI server can be the same system or two different systems.

Make sure that the systems can access an Oracle Solaris Image Packaging System (IPS) package repository. The IPS package repository can reside on the AI server, on another server on the local network, or on the Internet.

An AI service is associated with a SPARC or x86 AI install image and one or more sets of installation instructions. The installation instructions specify one or more IPS package repositories from where the system retrieves the packages needed to complete the installation. The installation instructions also include the names of additional packages to install and information such as target device and partition information. You can also specify instructions for post-installation configuration of the system.

Consider the operating systems and packages you are installing on the systems. Depending on your configuration and needs, you may want do one of the following:

- If two systems have different architectures or need to be installed with different versions of the Oracle Solaris OS, create two AI services, and associate each AI service with a different AI image.
- If two systems need to be installed with the same version of the Oracle Solaris OS but need to be installed differently in other ways, create two sets of installation instructions for the AI service. The different installation instructions can specify different packages to install or a different slice as the install target.

The installation begins when you boot the system. DHCP directs the system to the AI install server, and the system accesses the install service and the installation instructions within that service.

For more information, see the *Oracle® Solaris 11 Express Automated Installer Guide*.

## Using AI to install the Solaris 11 operating system and SFHA products

Use the following procedure to install the Solaris 11 operating system and SFHA products using AI.

**To use AI to install the Solaris 11 operating system and SFHA products**

1. Follow the Oracle documentation to setup a Solaris AI server and DHCP server.

   You can find the documentation at http://docs.oracle.com.

2. Set up the Symantec package repository.

   Run the following commands to start up necessary SMF services and create directories:

   ```
   # svcadm enable svc:/network/dns/multicast:default
   # mkdir /ai
   # zfs create -o compression=on -o mountpoint=/ai rpool/ai
   ```

3 Run the following commands to set up the IPS repository for Symantec Opteron packages:

```
# mkdir -p /ai/repo_symc_x64
# pkgrepo create /ai/repo_symc_x64
# pkgrepo add-publisher -s /ai/repo_symc_x64 Symantec
# pkgrecv -s <media_x64>/pkgs/VRTSpkgs.p5p -d /ai/repo_symc_x64 '*'
# svccfg -s pkg/server add symcx64
# svccfg -s pkg/server list
# svccfg -s pkg/server:symcx64 addpg pkg application
# svccfg -s pkg/server:symcx64 setprop pkg/port=10002
# svccfg -s pkg/server:symcx64 setprop pkg/inst_root=/ai/repo_symc_x64
# svccfg -s pkg/server:symcx64 addpg general framework
# svccfg -s pkg/server:symcx64 addpropvalue
general/complete astring: symcx64
# svccfg -s pkg/server:symcx64 addpropvalue general/enable
boolean: true
# svcs -a | grep pkg/server
# svcadm refresh application/pkg/server:symcx64
# svcadm enable application/pkg/server:symcx64
```

Or run the following commands to set up the private depot server for testing purposes:

```
# /usr/lib/pkg.depotd -d /ai/repo_symc_x64 -p 10002 > /dev/null &
```

Check the following URL on IE or Firefox browser:

http://<host>:10002

4 Run the following commands to setup IPS repository for Symantec Sparc packages:

```
# mkdir -p /ai/repo_symc_sparc
# pkgrepo create /ai/repo_symc_sparc
# pkgrepo add-publisher -s /ai/repo_symc_sparc Symantec
# pkgrecv -s <media_sparc>/pkgs/VRTSpkgs.p5p -d
/ai/repo_symc_sparc '*'
# svccfg -s pkg/server list
# svcs -a | grep pkg/server
# svccfg -s pkg/server add symcsparc
# svccfg -s pkg/server:symcsparc addpg pkg application
# svccfg -s pkg/server:symcsparc setprop pkg/port=10003
# svccfg -s pkg/server:symcsparc setprop pkg/inst_root=
/ai/repo_symc_sparc
# svccfg -s pkg/server:symcsparc addpg general framework
# svccfg -s pkg/server:symcsparc addpropvalue general/complete
astring: symcsparc
# svccfg -s pkg/server:symcsparc addpropvalue general/enable
boolean: true
# svcs -a | grep pkg/server
# svcadm refresh application/pkg/server:symcsparc
# svcadm enable application/pkg/server:symcsparc
```

Or run the following commands to set up the private depot server for testing purposes:

```
# /usr/lib/pkg.depotd -d /ai/repo_symc_sparc -p 10003 > /dev/null &
```

Check the following URL on IE or Firefox browser:

http://<host>:10003

5 Run the following commands to setup IPS repository to merge Symantec Sparc and x64 packages:

```
# mkdir /ai/repo_symc
# pkgrepo create /ai/repo_symc
# pkgrepo add-publisher -s /ai/repo_symc Symantec
# pkgmerge -s arch=sparc,/ai/repo_symc_sparc -s arch=i386,
/ai/repo_symc_x64 -d /ai/repo_symc
# svcs -a | grep pkg/server
# svccfg -s pkg/server list
# svccfg -s pkg/server add symcmerged
# svccfg -s pkg/server:symcmerged addpg pkg application
# svccfg -s pkg/server:symcmerged setprop pkg/port=10004
# svccfg -s pkg/server:symcmerged setprop pkg/inst_root=/ai/repo_symc
# svccfg -s pkg/server:symcmerged addpg general framework
# svccfg -s pkg/server:symcmerged addpropvalue general/complete
astring: symcmerged
# svccfg -s pkg/server:symcmerged addpropvalue general/enable
boolean: true
# svcadm refresh application/pkg/server:symcmerged
# svcadm enable application/pkg/server:symcmerged
# svcs -a | grep pkg/server
```

Or run the following commands to set up the private depot server for testing purposes:

```
# # /usr/lib/pkg.depotd -d /ai/repo_symc -p 10004 > /dev/null &
```

Check the following URL on IE or Firefox browser:

http://<host>:10004

6 Set up the install service on the AI server.

Run the following command:

```
# mkdir /ai/iso
```

Download the AI image from the Oracle Web site and place the `iso` in the `/ai/iso` directory.

Create an install service.

For example:

To set up the AI install server for Opteron platform::

```
# installadm create-service -n sol11x86 -s
/ai/iso/sol-11-1111-ai-x86.iso -d /ai/aiboot/
```

To set up the AI install server for SPARC platform::

```
# # installadm create-service -n sol11sparc -s\
 /ai/iso/sol-11-1111-ai-sparc.iso -d /ai/aiboot/
```

7 Run the installer to generate manifest XML files for all the SFHA products that you plan to install.

```
# mkdir /ai/manifests
# <media>/installer -ai /ai/manifests
```

8 For each system, generate the system configuration and include the hostname, user accounts, and IP addresses. For example, enter one of the following:

```
# mkdir /ai/profiles
# sysconfig create-profile -o /ai/profiles/profile_client.xml
```

or

```
# cp /ai/aiboot/auto-install/sc_profiles/sc_sample.xml
/ai/profiles/profile_client.xml
```

9 Add a system and match it to the specified product manifest and system configuration.

Run the following command to add an Opteron system, for example:

```
# installadm create-client -e "<client_MAC>" -n sol11x86
# installadm add-manifest -n sol11x86 -f
/ai/manifests/vrts_manifest_sfha.xml
# installadm create-profile -n sol11x86 -f
/ai/profiles/profile_client.xml -p profile_sc
# installadm set-criteria -n sol11x86 -m vrts_sfha
-p profile_sc -c mac="<client_MAC>"
# installadm list -m -c -p -n sol11x86
```

Run the following command to add a SPARC system, for example:

```
# installadm create-client -e "<client_MAC>" -n sol11sparc
# installadm add-manifest -n sol11sparc -f \
/ai/manifests/vrts_manifest_sfha.xml
# installadm create-profile -n sol11sparc -f \
/ai/profiles/profile_client.xml -p profile_sc
# installadm set-criteria -n sol11sparc -m \
vrts_sfha -p profile_sc -c mac="<client_MAC>"
# installadm list -m -c -p -n sol11sparc
```

10 For Opteron system, use Preboot Execution Environment(PXE) to reboot the system and install the operating system and Storage Foundation products.

For Sparc system, run the following command to reboot the system and install the operating system and Storage Foundation products:

```
# boot net:dhcp - install
```

# Manually installing packages on Solaris brand non-global zones

With Oracle Solaris 11, you must manually install SFCFSHA packages inside non-global zones. The native non-global zones are called Solaris brand zones.

**To install packages manually on Solaris brand non-global zones:**

1. Ensure that the SMF service svc:/application/pkg/system-repository:default is online on the global zone.

   ```
   # svcs svc:/application/pkg/system-repository
   ```

2. Log on to the non-global zone as a superuser.
3. Copy the VRTSpkgs.p5p package from the pkgs directory from the installation media to the non-global zone (for example at `/tmp/install` directory).
4. Disable the publishers that are not reachable, as package install may fail if any of the already added repositories are unreachable.

   ```
   #pkg set-publisher --disable <publisher name>
   ```

5. Add a file-based repository in the non-global zone.

   ```
   # pkg set-publisher -p/tmp/install/VRTSpkgs.p5p Symantec
   ```

6. Install the required packages.

   ```
   # pkg install --accept VRTSperl VRTSvlic VRTSvxfs VRTSvcs VRTSvcsag
   VRTSvcsea VRTSodm
   ```

7. Remove the publisher on the non-global zone.

   ```
   #pkg unset-publisher Symantec
   ```

8. Clear the state of the SMF service, as setting the file-based repository causes SMF service svc:/application/pkg/system-repository:default to go into maintenance state.

   ```
   # svcadm clear svc:/application/pkg/system-repository:default
   ```

9. Enable the publishers that were disabled earlier.

   ```
   # pkg set-publisher --enable <publisher>
   ```

**Note:** Perform steps 2 through 9 on each non-global zone.

# Manually installing packages on solaris10 brand zones

**You need to manually install SFCFSHA 6.0.1 packages inside the solaris10 brand zones.**

1. Boot the zone.
2. Logon to the solari10 brand zone as a super user.
3. Copy the Solaris 10 packages from the pkgs directory from the installation media to the non-global zone (such as `/tmp/install` directory).
4. Install the following SFCFSHA packages on the brand zone.

```
# cd /tmp/install
# pkgadd -d VRTSvlic.pkg
# pkgadd -d VRTSperl.pkg
# pkgadd -d VRTSvcs.pkg
# pkgadd -d VRTSvxfs.pkg
# pkgadd -d VRTSvcsag.pkg
# pkgadd -d VRTSvcsea.pkg
# pkgadd -d VRTSodm.pkg
```

**Note:** Perform all the above steps on each solaris10 brand zone.

# Installing SFCFSHA on Solaris 10 using JumpStart

This installation method applies only to Solaris 10. These JumpStart instructions assume a working knowledge of JumpStart. See the JumpStart documentation that came with your operating system for details on using JumpStart.

Upgrading is not supported. The following procedure assumes a stand-alone configuration.

For the language pack, you can use JumpStart to install packages. You add the language packages in the script, and put those files in the JumpStart server directory.

You can use a Flash archive to install SFCFSHA and the operating system in conjunction with JumpStart.

See "Using a Flash archive to install SFCFSHA and the operating system" on page 207.

## Overview of JumpStart installation tasks

Review the summary of tasks before you perform the JumpStart installation.

**Summary of tasks**

1. Add a client (register to the JumpStart server). See the JumpStart documentation that came with your operating system for details.
2. Read the JumpStart installation instructions.
3. Generate the finish scripts.

   See "Generating the finish scripts" on page 204.
4. Prepare shared storage installation resources.

   See "Preparing installation resources" on page 205.
5. Modify the rules file for JumpStart.

   See the JumpStart documentation that came with your operating system for details.
6. Install the operating system using the JumpStart server.
7. When the system is up and running, run the installer command from the installation media to configure the Veritas software.

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

   See "About the Veritas installer" on page 44.

## Generating the finish scripts

Perform these steps to generate the finish scripts to install SFCFSHA.

**To generate the script**

1. Run the product installer program to generate the scripts for all products.

   ```
   ./installer -jumpstart directory_to_generate_scripts
   ```

   Or

   ```
   ./install<productname> -jumpstart directory_to_generate_script
   ```

   where <*productname*> is the product's installation command, and *directory_to_generate_scripts* is where you want to put the product's script.

   For example:

   ```
   # ./installsfcfs -jumpstart /js_scripts
   ```
2. When you are prompted to encapsulate the root disk automatically, choose **yes** to do so. If you do not want to encapsulate it automatically, choose **no** and go to step 6.

3 Specify a disk group name for the root disk.

```
Specify the disk group name of the root disk to be encapsulated:
rootdg
```

4 Specify private region length.

```
Specify the private region length of the root disk to be
encapsulated: (65536)
```

5 Specify the disk's media name of the root disk to encapsulate.

```
Specify the disk media name of the root disk to be encapsulated:
(rootdg_01)
```

6 JumpStart finish scripts and encapsulation scripts are generated in the directory you specified in step 1.

Output resembles:

```
The finish scripts for VM is generated at /js_scripts/
jumpstart_sfcfsha.fin
The encapsulation boot disk script for SFCFSHA is generated at
/js_scripts/encap_bootdisk_vm.fin
```

List the js_scripts directory.

```
# ls /js_scripts
```

Output resembles:

```
encap_bootdisk_vm.fin jumpstart_sfcfsha.fin
```

## Preparing installation resources

Prepare resources for the JumpStart installation.

**To prepare the resources**

1 Copy the pkgs directory of the installation media to the shared storage.

```
# cd /path_to_installation_media
# cp -r pkgs BUILDSRC
```

2 Generate the response file with the list of packages.

```
# cd BUILDSRC/pkgs/
# pkgask -r package_name.response -d /
BUILDSRC/pkgs/packages_name.pkg
```

3 Create the adminfile file under *BUILDSRC*/pkgs/ directory.

```
mail=
instance=overwrite
partial=nocheck
runlevel=quit
idepend=quit
rdepend=nocheck
space=quit
setuid=nocheck
conflict=nocheck
action=nocheck
basedir=default
```

4 If you want to encapsulate the root disk automatically when you perform the JumpStart installation, copy the scripts `encap_bootdisk_vm.fin` generated previously to *ENCAPSRC*.

See "Generating the finish scripts" on page 204.

## Adding language pack information to the finish file

To add the language pack information to the finish file, perform the following procedure.

**To add the language pack information to the finish file**

1. For the language pack, copy the language packages from the language pack installation disc to the shared storage.

```
# cd /cdrom/cdrom0/pkgs
# cp -r * BUILDSRC/pkgs
```

If you downloaded the language pack:

```
# cd /path_to_language_pack_installation_media/pkgs
# cp -r * BUILDSRC/pkgs
```

2. In the finish script, copy the product package information and replace the product packages with language packages.
3. The finish script resembles:

```
. . .
for PKG in product_packages
do
...
done. . .
for PKG in language_packages
do
...
done. . .
```

# Using a Flash archive to install SFCFSHA and the operating system

You can only use Flash archive on the Solaris 10 operating system. In the following outline, refer to Solaris documentation for Solaris-specific tasks.

---

**Note:** Symantec does not support Flash Archive installation if the root disk of the master system is encapsulated.

---

The following is an overview of the creation and installation of a Flash archive with Veritas software.

- If you plan to start flar (flash archive) creation from bare metal, perform step 1 through step 10.
- If you plan to start flar creation from a system where you have installed, but not configured the product, perform step 1 through step 4. Skip step 5 and finish step 6 through step 10.

- If you plan to start flar creation from a system where you have installed and configured the product, perform step 5 through step 10.

**Flash archive creation overview**

1. Ensure that you have installed Solaris 10 on the master system.
2. Use JumpStart to create a clone of a system.
3. Reboot the cloned system.
4. Install the Veritas products on the master system.

   Perform one of the installation procedures from this guide.
5. If you have configured the product on the master system, create the `vrts_deployment.sh` file and the `vrts_deployment.cf` file and copy them to the master system.

   See "Creating the Veritas post-deployment scripts" on page 208.
6. Use the `flarcreate` command to create the Flash archive on the master system.
7. Copy the archive back to the JumpStart server.
8. Use JumpStart to install the Flash archive to the selected systems.
9. Configure the Veritas product on all nodes in the cluster. Start configuration with the following command:

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

   See "About the Veritas installer" on page 44.
10. Perform post-installation and configuration tasks.

    See the product installation guide for the post-installation and configuration tasks.

## Creating the Veritas post-deployment scripts

The generated files vrts_deployment.sh and vrts_post-deployment.cf are customized Flash archive post-deployment scripts. These files clean up Veritas product settings on a cloned system before you reboot it for the first time. Include these files in your Flash archives.

**To create the post-deployment scripts**

1. Mount the product disc.
2. From the prompt, run the `-flash_archive` option for the installer. Specify a directory where you want to create the files.

   ```
   # ./installer -flash_archive /tmp
   ```

3. Copy the vrts_postedeployment.sh file and the vrts_postedeployment.cf file to the golden system.
4. On the golden system perform the following:
   - Put the vrts_postdeployment.sh file in the /etc/flash/postdeployment directory.
   - Put the vrts_postdeployment.cf file in the /etc/vx directory.
5. Make sure that the two files have the following ownership and permissions:

   ```
   # chown root:root /etc/flash/postdeployment/vrts_postdeployment.sh
   # chmod 755 /etc/flash/postdeployment/vrts_postdeployment.sh
   # chown root:root /etc/vx/vrts_postdeployment.cf
   # chmod 644 /etc/vx/vrts_postdeployment.cf
   ```

   Note that you only need these files in a Flash archive where you have installed Veritas products.

# Installing SFCFSHA using the system command

Installing SFCFSHA on Solaris 10 using the pkgadd command

On Solaris 10, the packages must be installed while in the global zone.

**To install SFCFSHA on Solaris 10 using the pkgadd command**

1. Mount the software disc.

   See "Mounting the product disc" on page 63.

2. Copy the supplied VRTS* files from the installation media to a temporary location. Modify them if needed.

   ```
   # cp /cdrom/cdrom0/pkgs/VRTS* \
     /tmp/pkgs
   ```

3 Create the admin file in the current directory. Specify the `-a adminfile` option when you use the `pkgadd` command:

```
mail=
instance=overwrite
partial=nocheck
 runlevel=quit
idepend=quit
rdepend=nocheck
space=quit
setuid=nocheck
conflict=nocheck
action=nocheck
basedir=default
```

4 Use the product-specific install command with one of the following options to get a list of packages in the order to be installed:

- minpkgs
- recpkgs
- allpkgs

See "About the Veritas installer" on page 44.

See "Installation script options" on page 429.

5 Install the packages listed in step 4.

```
# pkgadd -a adminfile -d /tmp/pkgs pkgname.pkg
```

On Solaris 10, these packages must be installed while in the global zone. If a package's `pkginfo` file contains the variable SUNW_PKG_ALLZONES set not equal to true, the `-G` option should additionally be specified to the `pkgadd` command.

6 Verify that the packages are installed:

```
# pkginfo -l
   packagename
```

7 Start the processes.

Installing SFCFSHA on Solaris 11 using the pkg install command

**To install SFCFSHA on Solaris 11 using the pkg install command**

1. Mount the software disc.

   See "Mounting the product disc" on page 63.

2. Copy the supplied VRTS* files from the installation media to a temporary location. Modify them if needed.

   ```
   # cp /cdrom/cdrom0/pkgs/VRTS* \
       /tmp/pkgs
   ```

3. Use the product-specific install command with one of the following options to get a list of packages in the order to be installed:

   - minpkgs
   - recpkgs
   - allpkgs

   See "About the Veritas installer" on page 44.

   See "Installation script options" on page 429.

4. Install the packages listed in step 3.

   ```
   # /usr/bin/pkg set-publisher -p /tmp/pkgs/VRTSpkgs.p5p Symantec

   # /usr/bin/pkg install -accept pkgname

   # /usr/bin/pkg unset-publisher Symantec
   ```

5. Verify that the packages are installed:

   ```
   # pkg info packagename
   ```

6. Start the processes.

Chapter 16

# Configuring SFCFSHA using operating system-specific methods

This chapter includes the following topics:


- Configuring Veritas Storage Foundation Cluster File System High Availability manually


## Configuring Veritas Storage Foundation Cluster File System High Availability manually

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

### 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 Storage Foundation Administrator's Guide*.

In releases of VxVM (Volume Manager) before 4.0, a system that was installed with VxVM was configured with a default disk group, `rootdg`. The `rootdg` disk group had to contain at least one disk. By default, operations were directed to the `rootdg`

disk group. From release 4.0 onward, VxVM can function without any disk group having been configured.

## 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:

```
# vxdctl 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:

```
# vxdctl 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 `vxdctl`(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 to16. 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.

## Using vxinstall to configure Veritas Volume Manager

If you used the Veritas Installation Menu or the installvm script, you do not need to carry out the instructions in this section. Licensing, configuration of enclosure based naming and creation of a default disk group are managed by the menu installer and the installvm script.

Because you are no longer required to configure VxVM disks immediately, the vxinstall command no longer invokes the vxdiskadm program, making it much simpler than in previous releases.

The utility provides the following functions:

- Licensing VxVM.
- Setting up a system-wide default disk group.
- Starting VxVM daemons in case installation of SF has been done manually.

To run the command, enter

```
# vxinstall
```

which will prompt you to enter a license key:

```
Are you prepared to enter a license key [y,n,q,?] (default: y) y
```

The `vxinstall` program then asks if you want to set up a system-wide default disk group, which is optional:

```
Do you want to setup a system wide default disk group ?
[y,n,q,?] (default: y)
```

VxVM will continue with the question:

```
Which disk group [<group>,list,q,?] ?
```

If you know the name of the disk group that you want to use as the default disk group, enter it at the prompt, or use the `list` option and make a selection.

In releases prior to VxVM 4.0, the default disk group was `rootdg` (the root disk group). For VxVM 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. For operations that require a disk group, the system-wide default disk group will be used if the VxVM command is not specified with the `-g` option. The main benefit of creating a default disk group is that VxVM commands default to the default disk group and you will not need to use the `-g` option. To verify the default disk group after it has been created, enter the command:

```
# vxdg defaultdg
```

VxVM does not allow you to use the following names for the default disk group because they are reserved words: `bootdg`, `defaultdg` and `nodg`.

At this stage, the installation of VxVM is complete. To carry out further tasks such as disk encapsulation or initialization, see the *Veritas Storage Foundation Administrator's Guide*.

## Excluding a device that VxVM controls

This section describes how to exclude a device that is under VxVM control. The option to prevent paths from being multi-pathed by the Dynamic Multi-Pathing (DMP) driver, vxdmp, is deprecated.

**To suppress devices from being seen by VxVM**

1 Enter the command

```
# vxdiskadm
```

2 Select menu item `VolumeManager/Disk/ExcludeDevices` from the `vxdiskadm` main menu.

The following message displays:

```
VxVM INFO V-5-2-5950 This operation might lead to
some devices being suppressed from VxVM's view. (This operation
can be reversed using the vxdiskadm command).

Do you want to continue? [y,n,q,?] (default: n) y
```

3 Enter `y`.

4 Select one of the following operations:

- Suppress all paths through a controller from VxVM's view:
  Select Option 1.
  Enter a controller name when prompted:

  ```
  Enter a controller name:[ctlr_name,all,list,list-exclude,q,?]
  ```

- Suppress a path from VxVM's view:
  Select Option 2.
  Enter a path when prompted.

  ```
  Enter a pathname or pattern:[<Pattern>,all,list,list-exclude,q?]
  ```

- Suppress disks from VxVM's view by specifying a VID:PID combination:
  Select Option 3 and read the messages displayed on the screen.
  Enter a VID:PID combination when prompted.

  ```
  Enter a VID:PID combination:[<Pattern>,all,list,exclude,q,?]
  ```

  The disks that match the VID:PID combination are excluded from VxVM. Obtain the Vendor ID and Product ID from the Standard SCSI inquiry data returned by the disk.

If you selected any of the options, reboot the system for device exclusion to take effect.

## Enabling optional cluster support in VxVM

An optional cluster feature enables you to use VxVM 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.

### Converting existing VxVM 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
```

Make sure that CVM is started. To check the master node:

```
# vxdctl -c mode
```

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 disk_group_name
```

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.

Also, hot-relocation can be configured.

### 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.

## 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/vfstab
```

The Veritas-specific commands are described in the Storage Foundation guides and online manual pages.

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

### Loading and unloading the file system module

The `vxfs` file system module automatically loads on the first reference to a VxFS file system. This occurs when a user tries to mount a VxFS disk layout. In some instances, you may want to load the file system module manually. To do this, first load `vxfs`, then `vxportal`. `vxportal` is a pseudo device driver that enables VxFS commands to issue ioctls to the VxFS modules even when there are no file systems mounted on the system.

```
# modload /kernel/fs/vxfs
# modload /kernel/drv/vxportal
```

If you have a license for the Veritas Quick I/O feature, you can load its kernel modules:

```
# modload /usr/kernel/drv/sparcv9/fdd
```

To determine if the modules successfully loaded, enter:

```
# modinfo | grep vxportal
# modinfo | grep vxfs
```

The above commands provide information about the modules. The first field in the output is the module ID.

You can unload the module by entering:

```
# modunload -i portal_module_id
# modunload -i vxfs_module_id
```

The `modunload` command fails if any mounted VxFS file systems exist. To determine if any VxFS file systems are mounted, enter:

```
# df -F vxfs
```

## 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 /opt/VRTS/bin/vxtunefs
# chgrp 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 Storage Foundation Administrator's Guide*.

Chapter 17

# Manually configuring SFCFSHA clusters for data integrity

This chapter includes the following topics:

- Setting up disk-based I/O fencing manually
- Setting up server-based I/O fencing manually
- Setting up non-SCSI-3 fencing in virtual environments manually

## Setting up disk-based I/O fencing manually

Table 17-1 lists the tasks that are involved in setting up I/O fencing.

**Table 17-1** Tasks to set up I/O fencing manually

| Task | Reference |
|---|---|
| Initializing disks as VxVM disks | See "Initializing disks as VxVM disks" on page 124. |
| Identifying disks to use as coordinator disks | See "Identifying disks to use as coordinator disks" on page 222. |
| Checking shared disks for I/O fencing | See "Checking shared disks for I/O fencing" on page 125. |
| Setting up coordinator disk groups | See "Setting up coordinator disk groups" on page 222. |

**Table 17-1** Tasks to set up I/O fencing manually *(continued)*

| Task | Reference |
|---|---|
| Creating I/O fencing configuration files | See "Creating I/O fencing configuration files" on page 223. |
| Modifying SFCFSHA configuration to use I/O fencing | See "Modifying VCS configuration to use I/O fencing" on page 224. |
| Configuring CoordPoint agent to monitor coordination points | See "Configuring CoordPoint agent to monitor coordination points" on page 236. |
| Verifying I/O fencing configuration | See "Verifying I/O fencing configuration" on page 226. |

# Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See "Initializing disks as VxVM disks" on page 124.

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 125.

# Setting up coordinator disk groups

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

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

Refer to the *Veritas Storage Foundation Administrator's Guide* for details on how to create disk groups.

The following example procedure assumes that the disks have the device names c1t1d0s2, c2t1d0s2, and c3t1d0s2.

**To create the vxfencoorddg disk group**

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

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

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

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

3 Deport the coordinator disk group:

```
# vxdg deport vxfencoorddg
```

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

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

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

```
# vxdg deport vxfencoorddg
```

## Creating I/O fencing configuration files

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

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

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

1 On each nodes, type:

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

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

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

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

- For DMP configuration:

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

- For raw device configuration:

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

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

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

4 Ensure that you edit the following file on each node in the cluster to change the values of the VXFEN_START and the VXFEN_STOP environment variables to 1:

/etc/default/vxfen

## Modifying VCS configuration to use I/O fencing

After you add coordination points and configure I/O fencing, add the UseFence = SCSI3 cluster attribute to the VCS configuration file /etc/VRTSvcs/conf/config/main.cf.

If you reset this attribute to UseFence = None, VCS does not make use of I/O fencing abilities while failing over service groups. However, I/O fencing needs to be disabled separately.

**To modify VCS configuration to enable I/O fencing**

1 Save the existing configuration:

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

2 Stop VCS on all nodes:

```
# hastop -all
```

3 To ensure High Availability has stopped cleanly, run `gabconfig -a`.

In the output of the commans, check that Port h is not present.

4 If the I/O fencing driver vxfen is already running, stop the I/O fencing driver.

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

5 Make a backup copy of the main.cf file:

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

6 On one node, use vi or another text editor to edit the main.cf file. To modify the list of cluster attributes, add the UseFence attribute and assign its value as SCSI3.

```
cluster clus1(
UserNames = { admin = "cDRpdxPmHpzS." }
Administrators = { admin }
HacliUserLevel = COMMANDROOT
CounterInterval = 5
UseFence = SCSI3
)
```

Regardless of whether the fencing configuration is disk-based or server-based, the value of the cluster-level attribute UseFence is set to SCSI3.

7 Save and close the file.

8 Verify the syntax of the file /etc/VRTSvcs/conf/config/main.cf:

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

9 Using rcp or another utility, copy the VCS configuration file from a node (for example, sys1) to the remaining cluster nodes.

For example, on each remaining node, enter:

```
# rcp sys1:/etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config
```

10 Start the I/O fencing driver and VCS. Perform the following steps on each node:

- Start the I/O fencing driver.
  The vxfen startup script also invokes the `vxfenconfig` command, which configures the vxfen driver to start and use the coordination points that are listed in /etc/vxfentab.

  ```
  # svcadm enable vxfen
  ```

- Start VCS.

  ```
  # /opt/VRTS/bin/hastart
  ```

## Verifying I/O fencing configuration

Verify from the vxfenadm output that the SCSI-3 disk policy reflects the configuration in the /etc/vxfenmode file.

**To verify I/O fencing configuration**

1 On one of the nodes, type:

```
# vxfenadm -d
```

Output similar to the following appears if the fencing mode is SCSI3 and the SCSI3 disk policy is dmp:

```
I/O Fencing Cluster Information:
================================

Fencing Protocol Version: 201
Fencing Mode: SCSI3
Fencing SCSI3 Disk Policy: dmp
Cluster Members:

   * 0 (sys1)
   1 (sys2)

RFSM State Information:
   node 0 in state 8 (running)
   node 1 in state 8 (running)
```

2 Verify that the disk-based I/O fencing is using the specified disks.

```
# vxfenconfig -l
```

# Setting up server-based I/O fencing manually

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

**Table 17-2** Tasks to set up server-based I/O fencing manually

| Task | Reference |
|---|---|
| Preparing the CP servers for use by the SFCFSHA cluster | See "Preparing the CP servers manually for use by the SFCFSHA cluster" on page 227. |

**Table 17-2** Tasks to set up server-based I/O fencing manually *(continued)*

| Task | Reference |
|---|---|
| Modifying I/O fencing configuration files to configure server-based I/O fencing | See "Configuring server-based fencing on the SFCFSHA cluster manually" on page 230. |
| Modifying SFCFSHA configuration to use I/O fencing | See "Modifying VCS configuration to use I/O fencing" on page 224. |
| Configuring Coordination Point agent to monitor coordination points | See "Configuring CoordPoint agent to monitor coordination points" on page 236. |
| Verifying the server-based I/O fencing configuration | See "Verifying server-based I/O fencing configuration" on page 238. |

# Preparing the CP servers manually for use by the SFCFSHA cluster

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

Table 17-3 displays the sample values used in this procedure.

**Table 17-3** Sample values in procedure

| CP server configuration component | Sample name |
|---|---|
| CP server | cps1 |
| Node #1 - SFCFSHA cluster | sys1 |
| Node #2 - SFCFSHA cluster | sys2 |
| Cluster name | clus1 |
| Cluster UUID | {f0735332-1dd1-11b2} |

**To manually configure CP servers for use by the SFCFSHA cluster**

1 Determine the cluster name and uuid on the SFCFSHA cluster.

For example, issue the following commands on one of the SFCFSHA cluster nodes (sys1):

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

cluster clus1

# cat /etc/vx/.uuids/clusuuid

{f0735332-1dd1-11b2-bb31-00306eea460a}
```

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

For example:

```
# cpsadm -s cps1.symantecexample.com -a list_nodes

ClusName  UUID                                    Hostname(Node ID) Registered
clus1  {f0735332-1dd1-11b2-bb31-00306eea460a} sys1(0)         0
clus1  {f0735332-1dd1-11b2-bb31-00306eea460a} sys2(1)         0
```

If the output does not show the cluster and nodes, then add them as described in the next step.

For detailed information about the `cpsadm` command, see the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide.*

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

For example, issue the following command on the CP server (cps1.symantecexample.com) to add the cluster:

```
# cpsadm -s cps1.symantecexample.com -a add_clus\
 -c clus1  -u {f0735332-1dd1-11b2}

Cluster clus1 added successfully
```

Issue the following command on the CP server (cps1.symantecexample.com) to add the first node:

```
# cpsadm -s cps1.symantecexample.com -a add_node\
 -c clus1 -u {f0735332-1dd1-11b2} -h sys1 -n0

Node 0 (sys1) successfully added
```

Issue the following command on the CP server (cps1.symantecexample.com) to add the second node:

```
# cpsadm -s cps1.symantecexample.com -a add_node\
 -c clus1 -u {f0735332-1dd1-11b2} -h sys2 -n1

Node 1 (sys2) successfully added
```

4 If security is to be enabled, check whether the CPSADM@VCS_SERVICES@*cluster_uuid* users are created in the CP server.

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

```
# cpsadm -s cps1.symantecexample.com -a list_users

Username/Domain Type  Cluster Name / UUID         Role

CPSADM@VCS_SERVICES@f0735332-1dd1-11b2/vx
                      clus1/{f0735332-1dd1-11b2} Operator
```

If security is to be disabled, then add the user name "cpsclient@hostname" to the server instead of the CPSADM@VCS_SERVICES@*cluster_uuid* (for example, cpsclient@sys1).

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

5 Add the users to the CP server.

Issue the following commands on the CP server (cps1.symantecexample.com):

```
# cpsadm -s cps1.symantecexample.com -a add_user -e\
 CPSADM@VCS_SERVICES@cluster_uuid\
 -f cps_operator -g vx

User CPSADM@VCS_SERVICES@cluster_uuid
successfully added
```

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

For example, issue the following command on the CP server (cps1.symantecexample.com) for SFCFSHA cluster clus1 with two nodes sys1 and sys2:

```
# cpsadm -s cps1.symantecexample.com -a\
add_clus_to_user -c clus1\
 -u {f0735332-1dd1-11b2}\
 -e CPSADM@VCS_SERVICES@cluster_uuid\
 -f cps_operator -g vx

Cluster successfully added to user
 CPSADM@VCS_SERVICES@cluster_uuid privileges.
```

## Configuring server-based fencing on the SFCFSHA cluster manually

The configuration process for the client or SFCFSHA cluster to use CP server as a coordination point requires editing the `/etc/vxfenmode` file.

You need to edit this file to specify the following information for your configuration:

- Fencing mode
- Fencing mechanism
- Fencing disk policy (if applicable to your I/O fencing configuration)
- Appropriate value for the security configuration
- CP server or CP servers
- Coordinator disk group (if applicable to your I/O fencing configuration)

**Note:** Whenever coordinator disks are used as coordination points in your I/O fencing configuration, you must create a disk group (vxfencoorddg). You must specify this disk group in the `/etc/vxfenmode` file.

See "Setting up coordinator disk groups" on page 222.

The customized fencing framework also generates the `/etc/vxfentab` file which has security setting and the coordination points (all the CP servers and disks from disk group specified in `/etc/vxfenmode` file).

**To configure server-based fencing on the SFCFSHA cluster manually**

1. Use a text editor to edit the following file on each node in the cluster:

   `/etc/default/vxfen`

   You must change the values of the VXFEN_START and the VXFEN_STOP environment variables to 1.

2. Use a text editor to edit the `/etc/vxfenmode` file values to meet your configuration specifications.

   If your server-based fencing configuration uses a single highly available CP server as its only coordination point, make sure to add the `single_cp=1` entry in the `/etc/vxfenmode` file.

   The following sample file output displays what the `/etc/vxfenmode` file contains:

   See "Sample vxfenmode file output for server-based fencing" on page 231.

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

   For example:

   ```
   # svcadm enable vxfen
   ```

4. Make sure that `/etc/vxfenmode` file contains the value of security is set to 1.

   Make sure that following command displays the certificate being used by cpsadm client,

   ```
   EAT_DATA_DIR=/vat/VRTSvcs/vcsauth/data/CPSADM cpsat showcred
   ```

## Sample vxfenmode file output for server-based fencing

The following is a sample vxfenmode file for server-based fencing:

```
#
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
```

```
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=customized

# vxfen_mechanism determines the mechanism for customized I/O
# fencing that should be used.
#
# available options:
# cps      - use a coordination point server with optional script
#            controlled scsi3 disks
# security - 1
# security - 0

vxfen_mechanism=cps

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

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

#
# Specify 3 or more odd number of coordination points in this file,
# one in its own line. They can be all-CP servers, all-SCSI-3
# compliant coordinator disks, or a combination of CP servers and
# SCSI-3 compliant coordinator disks. Please ensure that the CP
```

```
# server coordination points are numbered sequentially and in the
# same order on all the cluster nodes.
#
# Coordination Point Server(CPS) is specified as:
#
#  cps<number>=[<vip/vhn>]:<port>
#
# If a CPS supports multiple virtual IPs or virtual hostnames over
# different subnets, all of the IPs/names can be specified in a
# comma separated list as follows:
#
# cps<number>=[<vip_1/vhn_1>]:<port_1>,[<vip_2/vhn_2>]:<port_2>,...,
#  [<vip_n/vhn_n>]:<port_n>
#
# Where,
# <number>
#  is the serial number of the CPS as a coordination point; must
#  start with 1.
# <vip>
#  is the virtual IP address of the CPS, must be specified in
#  square brackets ("[]").
# <vhn>
#  is the virtual hostname of the CPS, must be specified in square
#  brackets ("[]").
# <port>
#  is the port number bound to a particular <vip/vhn> of the CPS.
#  It is optional to specify a <port>. However, if specified, it
#  must follow a colon (":") after <vip/vhn>. If not specified, the
#  colon (":") must not exist after <vip/vhn>.
#
# For all the <vip/vhn>s which do not have a specified <port>, a
# default port can be specified as follows:
#
# port=<default_port>
#
#  Where <default_port> is applicable to all the <vip/vhn>s for
#  which a <port> is not specified. In other words, specifying <port>
#  with a <vip/vhn> overrides the <default_port> for that <vip/vhn>.
# If the <default_port> is not specified, and there are <vip/vhn>s for
# which <port> is not specified, then port number 14250 will be used
# for such <vip/vhn>s.
#
# Example of specifying CP Servers to be used as coordination points:
```

```
# port=57777
# cps1=[192.168.0.23],[192.168.0.24]:58888,[cps1.company.com]
# cps2=[192.168.0.25]
# cps3=[cps2.company.com]:59999
#
# In the above example,
# - port 58888 will be used for vip [192.168.0.24]
# - port 59999 will be used for vhn [cps2.company.com], and
# - default port 57777 will be used for all remaining <vip/vhn>s:
#    [192.168.0.23]
#    [cps1.company.com]
#    [192.168.0.25]
# - if default port 57777 were not specified, port 14250 would be used
#   for all remaining <vip/vhn>s:
#    [192.168.0.23]
#    [cps1.company.com]
#    [192.168.0.25]
#
# SCSI-3 compliant coordinator disks are specified as:
#
#  vxfendg=<coordinator disk group name>
# Example:
#  vxfendg=vxfencoorddg
#
# Examples of different configurations:
#  1. All CP server coordination points
# cps1=
# cps2=
# cps3=
#
# 2. A combination of CP server and a disk group having two SCSI-3
# coordinator disks
# cps1=
# vxfendg=
# Note: The disk group specified in this case should have two disks
#
# 3. All SCSI-3 coordinator disks
# vxfendg=
# Note: The disk group specified in case should have three disks
#
```

Table 17-4 defines the vxfenmode parameters that must be edited.

**Table 17-4** vxfenmode file parameters

| vxfenmode File Parameter | Description |
|---|---|
| vxfen_mode | Fencing mode of operation. This parameter must be set to “customized”. |
| vxfen_mechanism | Fencing mechanism. This parameter defines the mechanism that is used for fencing. If one of the three coordination points is a CP server, then this parameter must be set to “cps”. |
| scsi3_disk_policy | Configure the vxfen module to use either DMP devices, "dmp" or the underlying raw character devices, "raw".<br>**Note:** The configured disk policy is applied on all the nodes. |
| security | Security parameter 1 indicates that secure mode is used for CP server communications.<br>Security parameter 0 indicates that communication with the CP server is made in non-secure mode.<br>The default security value is 1. |
| fips_mode | [For future use] Set the value to 0. |
| cps1, cps2, or vxfendg | Coordination point parameters.<br>Enter either the virtual IP address or the FQHN (whichever is accessible) of the CP server.<br>`cps<number>=[virtual_ip_address/virtual_host_name]:port`<br>Where *port* is optional. The default port value is 14250.<br>If you have configured multiple virtual IP addresses or host names over different subnets, you can specify these as comma-separated values. For example:<br>`cps1=[192.168.0.23],[192.168.0.24]:58888, [cps1.company.com]`<br>**Note:** Whenever coordinator disks are used in an I/O fencing configuration, a disk group has to be created (vxfencoorddg) and specified in the /etc/vxfenmode file. Additionally, the customized fencing framework also generates the /etc/vxfentab file which specifies the security setting and the coordination points (all the CP servers and the disks from disk group specified in /etc/vxfenmode file). |

**Table 17-4** vxfenmode file parameters *(continued)*

| vxfenmode File Parameter | Description |
|---|---|
| port | Default port for the CP server to listen on.<br>If you have not specified port numbers for individual virtual IP addresses or host names, the default port number value that the CP server uses for those individual virtual IP addresses or host names is 14250. You can change this default port value using the port parameter. |
| single_cp | Value 1 for single_cp parameter indicates that the server-based fencing uses a single highly available CP server as its only coordination point.<br>Value 0 for single_cp parameter indicates that the server-based fencing uses at least three coordination points. |

## Configuring CoordPoint agent to monitor coordination points

The following procedure describes how to manually configure the CoordPoint agent to monitor coordination points.

The CoordPoint agent can monitor CP servers and SCSI-3 disks.

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

**To configure CoordPoint agent to monitor coordination points**

1. Ensure that your SFCFSHA cluster has been properly installed and configured with fencing enabled.
2. Create a parallel service group vxfen and add a coordpoint resource to the vxfen service group using the following commands:

```
# haconf -makerw
# hagrp -add vxfen
# hagrp -modify vxfen SystemList sys1 0 sys2 1
# hagrp -modify vxfen AutoFailOver 0
# hagrp -modify vxfen Parallel 1
# hagrp -modify vxfen SourceFile "./main.cf"
# hares -add coordpoint CoordPoint vxfen
# hares -modify coordpoint FaultTolerance 0
# hares -override coordpoint LevelTwoMonitorFreq
# hares -modify coordpoint LevelTwoMonitorFreq 5
# hares -modify coordpoint Enabled 1
# haconf -dump -makero
```

3 Verify the status of the agent on the SFCFSHA cluster using the `hares` commands. For example:

```
# hares -state coordpoint
```

The following is an example of the command and output::

```
# hares -state coordpoint

# Resource    Attribute   System   Value
coordpoint   State        sys1   ONLINE
coordpoint   State        sys2   ONLINE
```

4 Access the engine log to view the agent log. The agent log is written to the engine log.

The agent log contains detailed CoordPoint agent monitoring information; including information about whether the CoordPoint agent is able to access all the coordination points, information to check on which coordination points the CoordPoint agent is reporting missing keys, etc.

To view the debug logs in the engine log, change the dbg level for that node using the following commands:

```
# haconf -makerw

# hatype -modify Coordpoint LogDbg 10

# haconf -dump -makero
```

The agent log can now be viewed at the following location:

/var/VRTSvcs/log/engine_A.log

## Verifying server-based I/O fencing configuration

Follow the procedure described below to verify your server-based I/O fencing configuration.

**To verify the server-based I/O fencing configuration**

1 Verify that the I/O fencing configuration was successful by running the `vxfenadm` command. For example, run the following command:

```
# vxfenadm -d
```

**Note:** For troubleshooting any server-based I/O fencing configuration issues, refer to the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide*.

2 Verify that I/O fencing is using the specified coordination points by running the `vxfenconfig` command. For example, run the following command:

```
# vxfenconfig -l
```

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

# Setting up non-SCSI-3 fencing in virtual environments manually

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

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

See "Setting up server-based I/O fencing manually" on page 226.

2 Make sure that the SFCFSHA cluster is online and check that the fencing mode is customized.

```
# vxfenadm -d
```

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

```
# haclus -value UseFence
```

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

```
data_disk_fencing=off
```

5 On each node, edit the /kernel/drv/vxfen.conf file as follows:

```
vxfen_vxfnd_tmt=25
```

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

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

Refer to the sample /etc/vxfenmode file.

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

- Run the following command:

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

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

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

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

- Make the VCS configuration file writable:

```
# haconf -makerw
```

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

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

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

- Run the following command to verify the value:

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

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

The command should not list any resources.

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

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

- Make the VCS configuration file read-only

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

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

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

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

  ```
  # svcadm disable -t vcs
  ```

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

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

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

  ```
  # svcadm enable vxfen
  ```

## Sample /etc/vxfenmode file for non-SCSI-3 fencing

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

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

#
# scsi3_disk_policy determines the way in which I/O Fencing
# communicates with the coordination disks. This field is required
# only if customized coordinator disks are being used.
```

```
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
# scsi3_disk_policy=dmp

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

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

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

#
# Specify 3 or more odd number of coordination points in this file,
# one in its own line. They can be all-CP servers, all-SCSI-3
# compliant coordinator disks, or a combination of CP servers and
# SCSI-3 compliant coordinator disks. Please ensure that the CP
# server coordination points are numbered sequentially and in the
# same order on all the cluster nodes.
#
# Coordination Point Server(CPS) is specified as:
#
#  cps<number>=[<vip/vhn>]:<port>
#
# If a CPS supports multiple virtual IPs or virtual hostnames over
# different subnets, all of the IPs/names can be specified in a
# comma separated list as follows:
```

```
#
# cps<number>=[<vip_1/vhn_1>]:<port_1>,[<vip_2/vhn_2>]:<port_2>,...,
#  [<vip_n/vhn_n>]:<port_n>
#
# Where,
# <number>
#  is the serial number of the CPS as a coordination point; must
#  start with 1.
# <vip>
#  is the virtual IP address of the CPS, must be specified in
#  square brackets ("[]").
# <vhn>
#  is the virtual hostname of the CPS, must be specified in square
#  brackets ("[]").
# <port>
#  is the port number bound to a particular <vip/vhn> of the CPS.
#  It is optional to specify a <port>. However, if specified, it
#  must follow a colon (":") after <vip/vhn>. If not specified, the
#  colon (":") must not exist after <vip/vhn>.
#
# For all the <vip/vhn>s which do not have a specified <port>, a
# default port can be specified as follows:
#
# port=<default_port>
#
#  Where <default_port> is applicable to all the <vip/vhn>s for
#  which a <port> is not specified. In other words, specifying <port>
#  with a <vip/vhn> overrides the <default_port> for that <vip/vhn>.
# If the <default_port> is not specified, and there are <vip/vhn>s for
# which <port> is not specified, then port number 14250 will be used
# for such <vip/vhn>s.
#
# Example of specifying CP Servers to be used as coordination points:
# port=57777
# cps1=[192.168.0.23],[192.168.0.24]:58888,[cps1.company.com]
# cps2=[192.168.0.25]
# cps3=[cps2.company.com]:59999
#
# In the above example,
# - port 58888 will be used for vip [192.168.0.24]
# - port 59999 will be used for vhn [cps2.company.com], and
# - default port 57777 will be used for all remaining <vip/vhn>s:
#    [192.168.0.23]
```

```
#    [cps1.company.com]
#    [192.168.0.25]
# - if default port 57777 were not specified, port 14250 would be used
#   for all remaining <vip/vhn>s:
#    [192.168.0.23]
#    [cps1.company.com]
#    [192.168.0.25]
#
# SCSI-3 compliant coordinator disks are specified as:
#
#  vxfendg=<coordinator disk group name>
# Example:
#  vxfendg=vxfencoorddg
#
# Examples of different configurations:
#  1. All CP server coordination points
# cps1=
# cps2=
# cps3=
#
# 2. A combination of CP server and a disk group having two SCSI-3
# coordinator disks
# cps1=
# vxfendg=
# Note: The disk group specified in this case should have two disks
#
# 3. All SCSI-3 coordinator disks
# vxfendg=
# Note: The disk group specified in case should have three disks
#
cps1=[cps1.company.com]
cps2=[cps2.company.com]
cps3=[cps3.company.com]
port=14250
==============================
```

Section 7

# Upgrade of SFCFSHA


- Chapter 18. Planning to upgrade SFCFSHA
- Chapter 19. Performing a typical Storage Foundation Cluster File System High Availability upgrade using the installer
- Chapter 20. Performing a rolling upgrade of SFCFSHA
- Chapter 21. Performing a phased upgrade of SFCFSHA
- Chapter 22. Performing an automated SFCFSHA upgrade using response files
- Chapter 23. Upgrading the operating system
- Chapter 24. Upgrading Veritas Volume Replicator
- Chapter 25. Upgrading language packages
- Chapter 26. Migrating from SFHA to SFCFSHA
- Chapter 27. Upgrading SFCFSHA using Live Upgrade
- Chapter 28. Performing post-upgrade tasks

Chapter 18

# Planning to upgrade SFCFSHA

This chapter includes the following topics:


- Upgrade methods for SFCFSHA
- Supported upgrade paths for SFCFSHA 6.0.1
- About using the installer to upgrade when the root disk is encapsulated
- Preparing to upgrade SFCFSHA


## Upgrade methods for SFCFSHA

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 18-1** Review this table to determine how you want to perform the upgrade

| Upgrade types and considerations | Methods available for upgrade |
|---|---|
| Typical upgrades—use a Veritas provided tool or you can perform the upgrade manually. Requires some server downtime. | Script-based—you can use this to upgrade for the supported upgrade paths<br>Web-based—you can use this to upgrade for the supported upgrade paths<br>Manual—you can use this to upgrade from the previous release<br>Response file—you can use this to upgrade from the supported upgrade paths |

**Table 18-1** Review this table to determine how you want to perform the upgrade *(continued)*

| Upgrade types and considerations | Methods available for upgrade |
|---|---|
| Native operating system upgrade—use the upgrade software that comes with the operating system. Note that not all operating systems support native upgrades. | Operating system specific methods<br>Operating system upgrades |

# Supported upgrade paths for SFCFSHA 6.0.1

The following tables describe upgrading to 6.0.1.

**Table 18-2** Solaris SPARC upgrades using the script- or Web-based installer

| Veritas software versions | Solaris 8 or older | Solaris 9 | Solaris 10 | Solaris 11 |
|---|---|---|---|---|
| 3.5<br>3.5 MP4<br>4.0<br>4.0 MP1<br>4.0 MP2 | Upgrade the operating system to at least Solaris 10, then upgrade product to 5.0 MP3. Upgrade to 6.0.1 using the installer script. | Upgrade the operating system to at least Solaris 10, then upgrade product to 5.0 MP3. Upgrade to 6.0.1 using the installer script. | N/A | N/A |
| 4.1<br>4.1 MP1<br>4.1 MP2<br>5.0<br>5.0 MP1 | Upgrade the operating system to at least Solaris 10, then upgrade product to 5.0 MP3. Upgrade to 6.0.1 using the installer script. | Upgrade the operating system to at least Solaris 10, then upgrade product to 5.0MP3. Upgrade to 6.0.1 using the installer script. | Upgrade the product to 5.0 MP3. Upgrade to 6.0.1 using the installer script. | N/A |

**Table 18-2** Solaris SPARC upgrades using the script- or Web-based installer *(continued)*

| Veritas software versions | Solaris 8 or older | Solaris 9 | Solaris 10 | Solaris 11 |
|---|---|---|---|---|
| 5.0 MP3<br>5.0 MP3 RPx | Upgrade the operating system to at least Solaris 10. Upgrade to 6.0.1 using the installer script. | Upgrade operating system to at least Solaris 10. Upgrade to 6.0.1 using the installer script. | Upgrade directly to 6.0.1 using the installer script. | N/A |
| 5.1<br>5.1 RPx<br>5.1 SP1<br>5.1 SP1 RPx | N/A | Upgrade the operating system to at least Solaris 10. Upgrade to 6.0.1 using the installer script. | Upgrade directly to 6.0.1 using the installer script. | N/A |
| 6.0<br>6.0 RPx | N/A | Upgrade the operating system to at least Solaris 10. Upgrade to 6.0.1 using the installer script. | Upgrade directly to 6.0.1 using the installer script. | Upgrade directly to 6.0.1 using the installer script. |
| 6.0 PR1 | N/A | N/A | N/A | Upgrade directly to 6.0.1 using the installer script. |

**Table 18-3** Solaris x64 upgrades using the script- or Web-based installer

| Veritas software versions | Solaris 10 | Solaris 11 |
|---|---|---|
| 4.1<br>4.1 Phase 2 | Upgrade to 5.0 MP3. Upgrade to 6.0.1 using the installer script. | N/A |
| 5.0<br>5.0 MP3<br>5.0 MP3 RPx | Upgrade to 5.0 MP3. Upgrade to 6.0.1 using the installer script. | N/A |

**Table 18-3** Solaris x64 upgrades using the script- or Web-based installer *(continued)*

| Veritas software versions | Solaris 10 | Solaris 11 |
|---|---|---|
| 5.1<br>5.1 RPx<br>5.1 SP1*<br>5.1 SP1 RPx | Use the installer to upgrade to 6.0.1. | N/A |
| 6.0<br>6.0 RPx | Use the installer to upgrade to 6.0.1. | Upgrade directly to 6.0.1 using the installer script. |
| 6.0 PR1 | N/A | Upgrade directly to 6.0.1 using the installer script. |

*When you upgrade to 6.0.1 from 5.1 SP1 using the Web-based installer, you must first upgrade to 5.1 SP1 RP1 if you want the installer to create a backup of the boot disk. You can upgrade directly to 6.0.1 from 5.1 SP1 if you do not want the installer to create a backup of the boot disk.

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

In prior versions of SFCFSHA, when upgrading a system with an encapsulated root disk, you first had to unencapsulate. When upgrading to SFCFSHA 6.0.1, that is no longer necessary, as shown in the table below.

**Table 18-4** Upgrading using installer when the root disk is encapsulated

| Starting version | Ending version | Action required |
|---|---|---|
| 5.0 MP3 RPx | 6.0.1 | Do not unencapsulate. The installer runs normally. Reboot after upgrade. |
| 5.1 or 5.1 RPx | 6.0.1 | Do not unencapsulate. The installer runs normally. Reboot after upgrade. |
| 5.1 SP1 or 5.1 SP1 RPx | 6.0.1 | Do not unencapsulate. The installer runs normally. Reboot after upgrade. |

# Preparing to upgrade SFCFSHA

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

## Getting ready for the upgrade

Complete the following tasks before you perform the upgrade:

- Review the *Veritas Storage Foundation Cluster File System High Availability Release Notes* for any late-breaking information on upgrading your system.
- Review the Symantec Technical Support website for additional information: http://www.symantec.com/techsupp/
- Perform the following system-level settings:
  - Set `diag-level` to `min` to perform the minimum amount of diagnostics when the system boots. Depending on the configuration of your systems you may want to re-enable this after you perform the upgrade.

    ```
    {1} ok setenv diag-level min

     diag-level=min
    ```

  - Set **auto-boot?** to `false`. For tight control when systems reboot, set this variable to false. Re-enable this variable after the upgrade.

    ```
    {1} ok setenv auto-boot? false

    auto-boot?=false
    ```

  - Deactivate cron to make sure that extraneous jobs are not performed while you upgrade the systems. Do one of the following:
    Solaris 9:

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

    Solaris 10:

    ```
     # svcadm disable -t system/cron:default
    ```

    Solaris 11:

    ```
    # ps -ef | grep cron
    # kill cron pid
    # svcadm disable svc:/system/cron:default
    ```

- For Solaris 10, make sure that all non-global zones are booted and in the running state before you use the Veritas product installer to upgrade the Storage Foundation products in the global zone. If the non-global zones are not mounted and running at the time of the upgrade, you must upgrade each package in each non-global zone manually.
  For Live Upgrade, if the alternative root environment also has a zone, you cannot install `VRTSodm`. You must remove the `VRTSodm` package first then install the Storage Foundation product. After you reboot the alternative root, you can install `VRTSodm`.
- Make sure that the administrator who performs the upgrade has root access and a good knowledge of the operating system's administration.
- Make sure that all users are logged off and that all major user applications are properly shut down.
- Make sure that you have created a valid backup.
  See "Creating backups" on page 252.
- Ensure that you have enough file system space to upgrade. Identify where you want to copy the packages, for example `/packages/Veritas` when the root file system has enough space or `/var/tmp/packages` if the `/var` file system has enough space.
  Do not put the files under `/tmp`, which is erased during a system reboot.
  Do not put the files on a file system that is inaccessible prior to running the upgrade script.
  You can use a Veritas-supplied disc for the upgrade as long as modifications to the upgrade script are not required.
  If `/usr/local` was originally created as a slice, modifications are required.
- Unmount all the file systems not on the `root disk`. Comment out their entries in `/etc/vfstab`. Stop the associated volumes and deport the associated disk groups. Any file systems that the Solaris operating system or Storage Foundation assumes should be in `rootdg` but are not, must be unmounted and the associated entry in `/etc/vfstab` commented out.
- For any startup scripts in `/sbin/rcS.d`, comment out any application commands or processes that are known to hang if their file systems are not present.
- Make sure that the current operating system supports version 6.0.1 of the product. If the operating system does not support it, plan for a staged upgrade.
- Schedule sufficient outage time and downtime for the upgrade and any applications that use the Veritas products. Depending on the configuration, the outage can take several hours.

- Any swap partitions not in `rootdg` must be commented out of `/etc/vfstab`. If possible, swap partitions other than those on the root disk should be commented out of `/etc/vfstab` and not mounted during the upgrade. Active swap partitions that are not in `rootdg` cause `upgrade_start` to fail.
- Make sure the file systems are clean before upgrading.
  See "Verifying that the file systems are clean" on page 260.
- Symantec recommends that you upgrade VxFS disk layouts to a supported version prior to installing VxFS 6.0.1. Unsupported disk layout versions 4, 5, and 6 can be mounted for the purpose of online upgrading in VxFS 6.0.1. You can upgrade unsupported layout versions online before installing VxFS 6.0.1.
- Upgrade arrays (if required).
  See "Upgrading the array support" on page 261.
- To reliably save information on a mirrored disk, shut down the system and physically remove the mirrored disk. Removing the disk in this manner offers a failback point.
- Determine if the root disk is encapsulated.
  See "Determining if the root disk is encapsulated" on page 253.

## 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.

   Back up the `/etc/system` file.
3. Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.

   If not, a warning message is displayed.

   **Warning:** Backup `/etc/vx/cbr/bk` directory.
4. Copy the `vfstab` file to `vfstab.orig`:

   ```
   # cp /etc/vfstab /etc/vfstab.orig
   ```

5 Run the `vxlicrep`, `vxdisk list`, and `vxprint -ht` commands and record the output. Use this information to reconfigure your system after the upgrade.

6 If you are installing the high availability version of the Veritas Storage Foundation 6.0.1 software, follow the guidelines given in the *Veritas Cluster Server Installation Guide* and *Veritas Cluster Server Release Notes* for information on preserving your VCS configuration across the installation procedure.

## Determining if the root disk is encapsulated

Before you upgrade, you need to determine if the root disk is encapsulated by running the following command:

```
# mount | grep "/ on"
```

If the output from this command includes a path name that contains `vx` and `rootvol` as in `/dev/vx/dsk/bootdg/rootvol`, then the root disk is encapsulated.

If the root disk is encapsulated, follow the appropriate upgrade procedures.

See "About using the installer to upgrade when the root disk is encapsulated" on page 249.

## Pre-upgrade planning for Veritas Volume Replicator

Before installing or upgrading Veritas Volume Replicator (VVR):

- Confirm that your system has enough free disk space to install VVR.
- Make sure you have root permissions. You must have root permissions to perform the install and upgrade procedures.
- If replication using VVR is configured, Symantec recommends that the disk group version is at least 110 prior to upgrading.
  You can check the Disk Group version using the following command:

  ```
  # vxdg list diskgroup
  ```

- If replication using VVR is configured, make sure the size of the SRL volume is greater than 110 MB.
  Refer to the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide*.
- If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date on all the hosts.

  ```
  # /usr/sbin/vxrlink -g diskgroup status rlink_name
  ```

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

- If VCS is used to manage VVR replication, follow the preparation steps to upgrade VVR and VCS agents.
- Make sure that you have worked out all terminal emulation issues. Make sure that the terminal you use is fully functional for OpenBoot prompts and single-user and multi-user run levels.

See the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide* for more information.

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

## Planning an upgrade from the previous VVR version

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

See the *Veritas Storage Foundation Cluster File System High Availability Release Notes* for information regarding VVR support for replicating across Storage Foundation versions

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

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in Table 18-5, if either the Primary or Secondary are running a version of VVR prior to 6.0.1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 6.0.1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

**Table 18-5** VVR versions and checksum calculations

| VVR prior to 6.0.1 (DG version <= 140) | VVR 6.0.1 (DG version >= 150) | VVR calculates checksum TCP connections? |
|---|---|---|
| Primary | Secondary | Yes |
| Secondary | Primary | Yes |
| Primary and Secondary | | Yes |
| | Primary and Secondary | No |

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

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

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

### Planning and upgrading VVR to use IPv6 as connection protocol

Veritas Storage Foundation Cluster File System 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

### Additional settings for using VVR in a localized environment

If the language packages for VVR are installed, VVR displays localized messages, if the client locale is a supported non-English locale. The client locale is the locale from which you are accessing the VVR command line or GUI. For example, if the Japanese version of VVR is installed, then the messages are displayed in the Japanese locale, if the client locale is Japanese.

Make sure that the appropriate locale has been installed on all the hosts that are intended to be a part of the VVR RDS setup. Otherwise, some VVR error messages will be displayed in English, because it is the default locale. Make sure the following settings are done on all hosts that are intended to be part of the RDS:

- Install the required client locale from the Operating System disc.
- Install the required Volume Manager and VVR localized packages.
- Set the client locale, before using any of the VVR interfaces:
  - For the VVR command line, set the locale using the appropriate method for your operating system.
  - For VRW, select the locale from the VRW login page.

## Preparing to upgrade VVR when VCS agents are configured

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

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

### Freezing the service groups and stopping all the applications

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

To freeze the service groups and stop applications

**Perform the following steps for the Primary and Secondary clusters:**

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

   In a shared disk group environment:

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

In a private disk group environment:

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

---

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

---

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

```
# haconf -makerw
```

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

```
# hagrp -list
```

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

```
# hagrp -freeze group_name -persistent<sys_name>
```

---

**Note:** Make a note of the list of frozen service groups for future use.

---

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

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

---

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

---

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

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

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

9 Repeat step 8 for each node of the cluster.

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

See "Determining the nodes on which disk groups are online" on page 258.

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

```
# vxdctl -c mode
```

Note the master and record it for future use.

### Determining the nodes on which disk groups are online

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

**To determine the online disk groups**

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

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

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

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

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

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

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

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

## Preparing for the upgrade when VCS agents are configured

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

**To prepare a configuration with VCS agents for an upgrade**

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

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

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

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

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

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

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

```
# vxrecover -bs
```

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

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

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

## Verifying that the file systems are clean

Verify that all file systems have been cleanly unmounted.

**To make sure the file systems are clean**

1 Verify that all file systems have been cleanly unmounted:

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

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

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

```
# opt/VRTS/bin/fsck -F vxfs filesystem
# opt/VRTS/bin/mount -F vxfs Block_Device
   mountpoint
# opt/VRTS/bin/umount mountpoint
```

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

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

```
file system device busy
```

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

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

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

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

# Upgrading the array support

The Storage Foundation 6.0.1 release includes all array support in a single package, VRTSaslapm. The array support package includes the array support previously included in the VRTSvxvm package. The array support package also includes support previously packaged as external array support libraries (ASLs) and array policy modules (APMs).

See the 6.0.1 Hardware Compatibility List for information about supported arrays.

See “Hardware compatibility list (HCL)” on page 32.

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

After you have installed Storage Foundation 6.0.1, Symantec provides support for new disk arrays through updates to the `VRTSaslapm` package.

For more information about array support, see the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide*.

Chapter 19

# Performing a typical Storage Foundation Cluster File System High Availability upgrade using the installer

This chapter includes the following topics:


- Performing a full upgrade


## Performing a full upgrade

Performing a full upgrade involves the following tasks:

- Ensuring that the file systems are clean
- Updating the main.cf file
- Performing the upgrade
- Updating the configuration and confirming startup

### Ensuring the file systems are clean

Before upgrading to SFCFSHA 6.0.1, ensure that the file systems are clean. To ensure that the logs have been replayed and the file systems are marked clean:

**To ensure the file systems are clean**

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

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

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

   Repeat this step for each SFCFSHA service group.

   **Note:** This unmounts the CFS file systems.

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

   ```
   # umount mount_point
   ```

4. Check and repair each VxFS file system:

   ```
   # fsck -F vxfs /dev/vx/rdsk/diskgroup/volume
   ```

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

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

   Repeat this step for each file system.

# Modifying the main.cf file

Save a copy of the `main.cf` file and modify the configuration information in the `main.cf` file.

**To modify the main.cf file**

1 On any node, make a copy of the current `main.cf` file. For example:

```
# cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/main.save
```

2 Choose one node from the cluster to execute step 3 through step 9.

3 On the node you selected in step 2, enter:

```
# haconf -makerw
# hares -unlink vxfsckd qlogckd
# hares -unlink qlogckd cvm_clus
# hares -link vxfsckd cvm_clus
# hares -delete qlogckd
# haconf -dump -makero
```

4 On all the nodes in the cluster, enter:

```
# ps -ef | grep qlogckd
# kill -9 pid_of_qlogckd
# modinfo | grep -i qlog
# modunload -i module_id_of_qlog
```

5 On the node you selected in step 2, stop VCS on all nodes:

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

6 On the node you selected in step 2 and if you have configured the VCS Cluster Manager (Web Console), complete the following to modify the `/etc/VRTSvcs/conf/config/main.cf` file.

- Remove VRTSweb:

```
Process VRTSweb (
      PathName = "/opt/VRTSvcs/bin/haweb"
      Arguments = "10.129.96.64 8181"
      )
```

- Replace it with:

```
VRTSWebApp VCSweb (
              Critical =0
              AppName = vcs
              InstallDir = "/opt/VRTSweb/VERITAS"
```

```
        TimeForOnline = 5
        )
```

- Add the NIC resource in the ClusterService group. For example, where the name of the NIC resource is named csgnic and the public NIC device is hme0, add:

```
NIC csgnic (
        Device = hme0
```

- Add new dependencies for the new resources in the ClusterService group. For example, using the names of the VRTSWebApp, NotifierMngr, IP, and NIC resources, enter lines that resemble:

```
VCSweb requires webip
    ntfr requires csgnic
    webip requires csgnic
```

7 On the node you selected in step 2, remove `qlogckd` from the `/etc/VRTSvcs/conf/config/main.cf` file. For example:

```
CFSQlogckd qlogckd (
       Critical = 0
       )
```

Make sure you remove all dependencies on `qlogckd` from the `main.cf` file.

8 On the node you selected in step 2, verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file:

```
# cd /etc/VRTSvcs/conf/config
# /opt/VRTS/bin/hacf -verify .
```

9 On the node you selected in step 2, start VCS:

```
# /opt/VRTS/bin/hastart
```

10 On the remaining nodes in the cluster, start VCS:

```
# /opt/VRTS/bin/hastart
```

11 If VVR is configured, freeze the service groups and stop the applications.

See "Freezing the service groups and stopping all the applications" on page 256.

# Performing the upgrade

**To perform the upgrade**

1. Log in as superuser.
2. Insert the appropriate media disc into your system's DVD-ROM drive.
3. If volume management software is running on your system, the software disc automatically mounts as `/cdrom`.

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

   ```
   # mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
   ```

   where *c#t#d#* is the location of the CD drive.
4. Change to the top-level directory on the disc:

   ```
   # cd /cdrom
   ```

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

   ```
   # mount -p | grep vxfs
   ```

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

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

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

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

   ```
   # umount mount_point
   ```

   Repeat this step for each SFCFSHA service group.
6. Start the upgrade from any node in the cluster. Enter the following command, and then press **y** to upgrade the cluster configuration.

   ```
   # ./installsfcfsha -upgrade
   ```

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

```
Do you agree with the terms of the End User License Agreement
as specified in the storage_foundation_cluster_file_system_ha/EULA/
en/EULA_CFSHA_Ux_6.0.1.pdf file present on media? [y,n,q,?] y
```

8 The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the system's boot disk group before the upgrade proceeds. If you want to split the boot disk group to create a backup, answer **y**.

9 The installer then prompts you to name the backup boot disk group. Enter the name for it or press **Enter** to accept the default.

10 If you are prompted to start the split operation. Press **y** to continue.

**Note:** The split operation can take some time to complete.

11 You are prompted to enter the system names (in the following example, "sys1" and "sys2") on which the software is to be upgraded. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces on which to
install SFCFSHA: sys1 sys2
```

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

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

See "About configuring secure shell or remote shell communication modes before installing products" on page 467.

13 After you accept EULA and the system checks complete, the installer displays a list of the packages that will be upgraded. Press Enter to continue with the upgrade.

14 Output shows information that SFCFSHA must be stopped on a running system. Enter **y** to continue.

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

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

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

17 Update the configuration.

18 Only perform this step if you have split the mirrored root disk to back it up. After a successful reboot, verify the upgrade and re-join the backup disk group. If the upgrade fails, revert to the backup disk group.

See "Re-joining the backup boot disk group into the current disk group" on page 331.

See "Reverting to the backup boot disk group after an unsuccessful upgrade" on page 332.

## Updating the configuration and confirming startup

Perform the following steps on each upgraded node.

**To update the configuration and confirm startup**

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

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

2 Reboot the upgraded nodes, if root disk is encapsulated.

```
# /usr/sbin/shutdown -i6 -g0 -y
```

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

```
# lltconfig
  LLT is running
```

4 Verify GAB is configured:

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

5 Verify VxVM daemon is started and enabled:

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

6 Confirm all upgraded nodes are in a running state.

```
# gabconfig -a
```

7 If any process fails to start after the upgrade, enter the following to start it:

```
# /opt/VRTS/install/installsfcfsha<version> -start sys1 sys2
```

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

See "About the Veritas installer" on page 44.

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

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

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

- Make the configuration read/write.

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

- Unfreeze the group.

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

- Save the configuration.

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

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

Bring online the CVM groups on all systems.

```
# /opt/VRTS/bin/hagrp -online group_name -sys sys1
# /opt/VRTS/bin/hagrp -online group_name -sys sys2
```

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

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

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

Bring online the SFCFSHA groups on all systems.

```
# /opt/VRTS/bin/hagrp -online group_name -sys sys1
# /opt/VRTS/bin/hagrp -online group_name -sys sys2
```

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

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

---

**Note:** If you upgrade to SFCFSHA 6.0.1 and the file systems are dirty, you have to deport the shared disk group and import it as non-shared. After the import, run `fsck`. `fsck` should succeed. Then deport the disk group and import it back as shared.

---

10 Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

11 On the CVM master node, upgrade the CVM protocol. Enter the following:

```
# vxdctl upgrade
```

Chapter 20

# Performing a rolling upgrade of SFCFSHA

This chapter includes the following topics:


- Performing a rolling upgrade using the installer


## Performing a rolling upgrade using the installer

Use a rolling upgrade to upgrade Veritas Storage Foundation Cluster File System High Availability to the latest release with minimal application downtime.

### About rolling upgrades

The rolling upgrade minimizes downtime for highly available clusters to the amount of time that it takes to perform a service group failover. The rolling upgrade has two main phases where the installer upgrades kernel packages in phase 1 and VCS agent packages in phase 2.

---

**Note:** You need to perform a rolling upgrade on a completely configured cluster.

---

The following is an overview of the flow for a rolling upgrade:

1. The installer performs prechecks on the cluster.

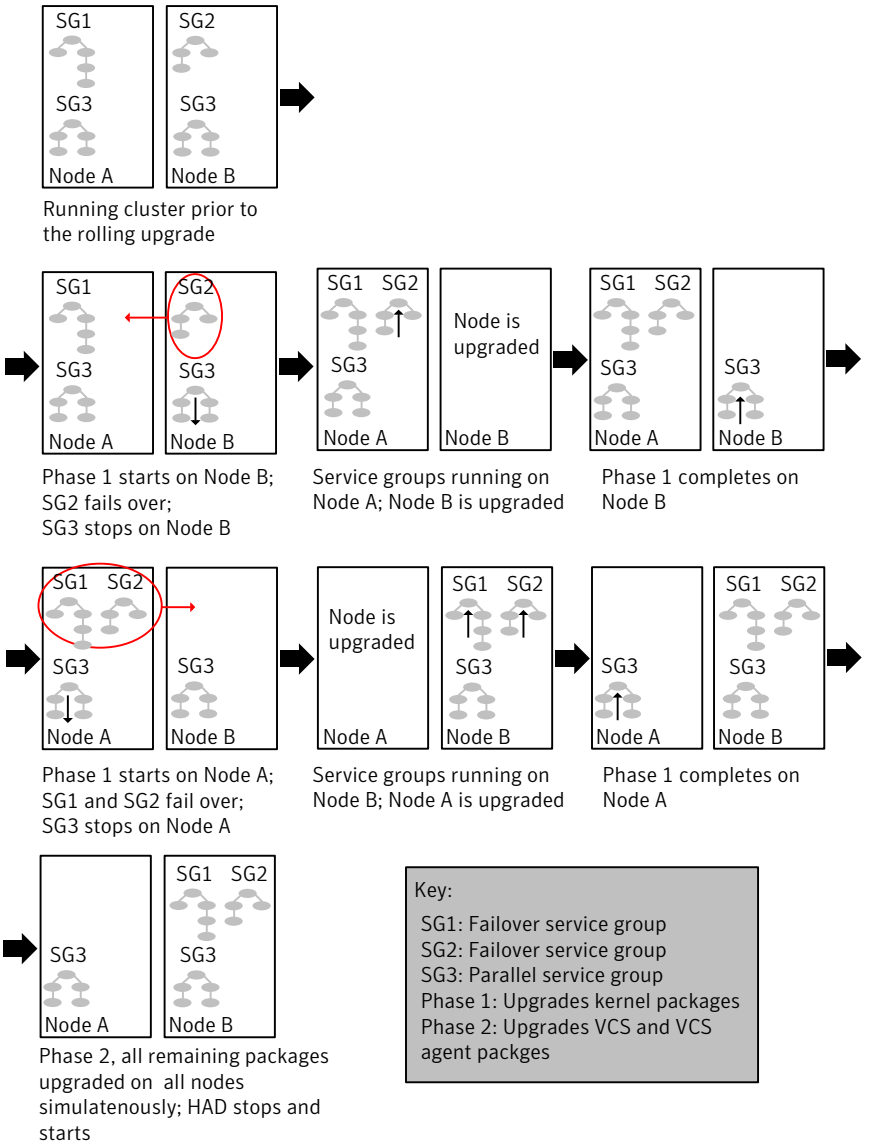
2. The installer moves service groups to free nodes for the first phase of the upgrade as is needed.

   Application downtime occurs during the first phase as the installer moves service groups to free nodes for the upgrade. The only downtime that is incurred is the normal time required for the service group to fail over. The downtime is limited to the applications that are failed over and not the entire cluster.

3. The installer performs the second phase of the upgrade on all of the nodes in the cluster. The second phase of the upgrade includes downtime of the Veritas Cluster Server (VCS) engine HAD, but does not include application downtime.

Figure 20-1 illustrates an example of the installer performing a rolling upgrade for three service groups on a two node cluster.

**Figure 20-1** Example of the installer performing a rolling upgrade




The following limitations apply to rolling upgrades:

- Rolling upgrades are not compatible with phased upgrades. Do not mix rolling upgrades and phased upgrades.
- You can perform a rolling upgrade from 5.1 and later versions.

# Supported rolling upgrade paths

You can perform a rolling upgrade of SFCFSHA with the script-based installer, the Web-based installer, or manually.

The rolling upgrade procedures support both major and minor operating system upgrades.

Table 20-1 shows the versions of SFCFSHA for which you can perform a rolling upgrade to Veritas Storage Foundation Cluster File System High Availability 6.0.1.

**Table 20-1** Supported rolling upgrade paths

| Platform | SFCFSHA version |
|---|---|
| Solaris 10 SPARC | 5.1, 5.1RPs<br>5.1SP1, 5.1SP1RPs, 5.1SP1PR3<br>6.0, 6.0RP1 |
| Solaris 11 SPARC | 6.0PR1 |
| Solaris 10 x64 | 5.1, 5.1RPs<br>5.1SP1, 5.1SP1RPs, 5.1SP1PR3<br>6.0, 6.0RP1 |
| Solaris 11 x64 | 6.0PR1 |

**Note:** Before performing a rolling upgrade from version 5.1SP1RP3 to version 6.0.1, install patch VRTSvxfen-5.1SP1RP3P2. For downloading the patch, search VRTSvxfen-5.1SP1RP3P2 in Patch Lookup on the SORT website.

# Performing a rolling upgrade using the script-based installer

Before you start the rolling upgrade, make sure that Veritas Cluster Server (VCS) is running.

**To perform a rolling upgrade**

1 Complete the preparatory steps on the first sub-cluster.

2 Complete updates to the operating system, if required. For instructions, see the operating system documentation.

The nodes are restarted after the operating system update.

If you are performing a major OS upgrade (such as Solaris 9 to Solaris 10), do the following:

- Mount the software disc for the previous version of SFCFSHA.
- From the top level disc directory, start the installer.
- Uninstall the SFCFSHA packages.
- To finish the uninstallation, start the installer again, and install the packages for the previous version of SFCFSHA on the upgraded OS.
  When the installation completes, the CPI prompts you to reboot the nodes again.

Restart the nodes again manually. Failing to perform this additional reboot prevents the upgrade from proceeding further.

```
# shutdown -g0 -y -i6
```

3 Log in as superuser and mount the SFCFSHA 6.0.1 installation media.

4 Complete the preparatory steps again for the first sub-cluster.

5 From root, start the installer.

```
# ./installer
```

6 From the menu, select `Upgrade` and from the sub menu, select `Rolling Upgrade`.

7 The installer suggests system names for the upgrade. Enter `Yes` to upgrade the suggested systems, or enter `No`, and then enter the name of any one system in the cluster on which you want to perform a rolling upgrade.

8 The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type **y** to continue.

9 The installer inventories the running service groups and determines the node or nodes to upgrade in phase 1 of the rolling upgrade. Type **y** to continue. If you choose to specify the nodes, type **n** and enter the names of the nodes.

10 The installer performs further prechecks on the nodes in the cluster and may present warnings. You can type **y** to continue or quit the installer and address the precheck's warnings.

11 Review the end-user license agreement, and type **y** if you agree to its terms.

12 After the installer shows the package list, it detects if there are online failover service groups on the nodes to be upgraded. If there are online failover service groups, the installer prompts you to do one of the following:

- Manually switch service groups

- Use the CPI to automatically switch service groups

The downtime is the time that it normally takes for the service group's failover.

13 The installer prompts you to stop the applicable processes. Type **y** to continue.

The installer evacuates all service groups to the node or nodes that are not upgraded at this time. The installer stops parallel service groups on the nodes that are to be upgraded.

14 The installer stops relevant processes, uninstalls old kernel packages, and installs the new packages. When prompted, enable replication or global cluster capabilities, if required, and register the software.

The installer performs the upgrade configuration and re-starts processes.

If some processes fail to start, you may need to reboot the nodes and manually check the cluster's status.

15 Complete the preparatory steps on the nodes that you have not yet upgraded.

16 Complete updates to the operating system, if required, on the nodes that you have not yet upgraded. For instructions, see the operating system documentation.

The nodes are restarted after the operating system update.

If you are performing a major OS upgrade (such as Solaris 9 to Solaris 10), do the following:

- Mount the software disc for the previous version of SFCFSHA.
- From the top level disc directory, start the installer.
- Uninstall the SFCFSHA packages.
- To finish the uninstallation, start the installer again, and install the packages for the previous version of SFCFSHA on the upgraded OS.
  When the installation completes, the CPI prompts you to reboot the nodes again.

Restart the nodes again manually. Failing to perform this additional reboot prevents the upgrade from proceeding further.

```
# shutdown -g0 -y -i6
```

17 The installer begins phase 1 of the upgrade on the remaining node or nodes. Type **y** to continue the rolling upgrade.

If the installer prompts to reboot nodes, reboot the nodes.

Restart the installer.

The installer repeats step 9 through step 14.

For clusters with larger number of nodes, this process may repeat several times. Service groups come down and are brought up to accommodate the upgrade.

18 When phase 1 of the rolling upgrade completes, begin phase 2 of the upgrade. Phase 2 of the upgrade includes downtime for the VCS engine (HAD), which does not include application downtime. Type **y** to continue.

19 The installer determines the remaining packages to upgrade. Press **Enter** to continue.

20 The installer stops Veritas Cluster Server (VCS) processes but the applications continue to run. Type **y** to continue.

The installer performs prechecks, uninstalls old packages, and installs the new packages. It performs post-installation tasks, and the configuration for the upgrade.

21 Type **y** or **n** to help Symantec improve the automated installation.

22 If you have network connection to the Internet, the installer checks for updates.

If updates are discovered, you can apply them now.

23 A prompt message appears to ask if the user would like to read the summary file. You can choose **y** if you want to read the install summary file.

24 To upgrade VCS or Storage Foundation High Availability (SFHA) on the Coordination Point (CP) server systems to version 6.0.1, upgrade VCS or SFHA on the CP server systems. You then upgrade all the application clusters to 6.0.1.

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

# Performing a rolling upgrade of SFCFSHA using the Web-based installer

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

See "About rolling upgrades" on page 272.

**To start the rolling upgrade—phase 1**

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

2 Complete updates to the operating system, if required. For instructions, see the operating system documentation.

The nodes are restarted after the operating system update.

If you are performing a major OS upgrade (such as Solaris 9 to Solaris 10), do the following:

- Mount the software disc for the previous version of SFCFSHA.
- From the top level disc directory, start the installer.
- Uninstall the SFCFSHA packages.
- To finish the uninstallation, start the installer again, and install the packages for the previous version of SFCFSHA on the upgraded OS.
  When the installation completes, the CPI prompts you to reboot the nodes again.

Restart the nodes again manually. Failing to perform this additional reboot prevents the upgrade from proceeding further.

```
# shutdown -g0 -y -i6
```

3 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 144.

4 In the Task pull-down menu, select `Rolling Upgrade`.

Click the **Next** button to proceed.

5 Enter the name of any one system in the cluster on which you want to perform a rolling upgrade.The installer identifies the cluster information of the system and displays the information.

Click **Yes** to confirm the cluster information. The installer now displays the nodes in the cluster that will be upgraded during phase 1 of the upgrade.

6 Review the systems that the installer has chosen for phase 1 of the rolling upgrade. These systems are chosen to minimize downtime during the upgrade.

Click **Yes** to proceed.

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

7 Review the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.

8 If you have online failover service groups, the installer prompts you to choose to switch these service groups either manually or automatically. Choose any option and follow the steps to switch all the failover service groups to the other subcluster.

9 The installer stops all processes. Click **Next** to proceed.

The installer removes old software and upgrades the software on the systems that you selected.

10 If you want to enable volume or file replication or global cluster capabilities, select from the following options:

- Veritas Volume Replicator
- Veritas File Replicator
- Global Cluster Option

Click **Register** to register the software. Click the **Next** button.

The installer starts all the relevant processes and brings all the service groups online.

11 When prompted by the installer, reboot the nodes on the first half of the cluster.

Restart the installer.

12 Repeat step 6 through step 11 until the kernel packages of all the nodes are upgraded. For clusters with larger number of nodes, this process may get repeated several times. Service groups come down and are brought up to accommodate the upgrade.

13 Complete updates to the operating system on the nodes that you have not yet upgraded. For instructions, see the operating system documentation.

The nodes are restarted after the operating system update.

If you are performing a major OS upgrade (such as Solaris 9 to Solaris 10), do the following:

- Mount the software disc for the previous version of SFCFSHA.
- From the top level disc directory, start the installer.
- Uninstall the SFCFSHA packages.
- To finish the uninstallation, start the installer again, and install the packages for the previous version of SFCFSHA on the upgraded OS.
  When the installation completes, the CPI prompts you to reboot the nodes again.

Restart the nodes again manually. Failing to perform this additional reboot prevents the upgrade from proceeding further.

```
# shutdown -g0 -y -i6
```

14 When prompted, perform step 4 through step 11 on the nodes that you have not yet upgraded.

15 When prompted, start phase 2. Click **Yes** to continue with the rolling upgrade.

You may need to restart the Web-based installer to perform phase 2.

See "Starting the Veritas Web-based installer" on page 144.

**To upgrade the non-kernel components—phase 2**

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

Click the **Next** button to proceed.

2 The installer detects the information of cluster and the state of rolling upgrade.

The installer validates systems. Click **Next**. If it throws an error, address the error and return to the installer.

3 Review the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.

4 The installer stops the `HAD` and `CmdServer` processes in phase 2 of the rolling upgrade process. Click **Next** to proceed.

5 The installer removes old software and upgrades the software on the systems that you selected. Review the output and click the **Next** button when prompted. Register the software and click **Next** to proceed. The installer starts all the relevant processes and brings all the service groups online.

6 If you have network connection to the Internet, the installer checks for updates.

If updates are discovered, you can apply them now.

7 A prompt message appears to ask if the user would like to read the summary file. You can choose **y** if you want to read the install summary file.

The upgrade is complete.

Chapter 21

# Performing a phased upgrade of SFCFSHA

This chapter includes the following topics:


- Performing a phased upgrade of SFCFSHA


## Performing a phased upgrade of SFCFSHA

Performing a phased upgrade involves the following tasks:

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

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

### Prerequisites for a phased upgrade

Before you start the upgrade, confirm that you have licenses for all the nodes that you plan to upgrade. Note that your applications have downtime during this procedure.

## Planning for a phased upgrade

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

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

## Phased upgrade limitations

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

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

## Moving the service groups to the second subcluster

**To move the service groups to the second subcluster**

1. Switch failover groups from the first half of the cluster to one of the nodes in the second half of the cluster. In this procedure, `sys1` is a node in the first half of the cluster and `sys4` is a node in the second half of the cluster. Enter the following:

   ```
   # hagrp -switch failover_group -to sys4
   ```

2. On the first half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the applications.

3 On the first half of the cluster, unmount the VxFS or CFS file systems that are not managed by VCS.

```
# mount -p | grep vxfs
```

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

```
# fuser -c mount_point
```

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

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

```
# umount /mount_point
```

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

```
# hagrp -offline group_name -sys sys1
```

When the CVM group becomes OFFLINE, all the parallel service groups such as the CFS file system will also become OFFLINE on the first half of the cluster nodes.

5 Verify that the VCS service groups are offline on all the nodes in first half of the cluster. Enter the following:

```
# hagrp -state group_name
```

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

```
# haconf -makerw
# hasys -freeze -persistent sys1
# haconf -dump -makero
```

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

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

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

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

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

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

Verify that no volumes remain open. Enter the following:

```
# vxprint -Aht -e v_open
```

10 On first half of the cluster, upgrade the operating system on all the nodes, if applicable. For instructions, see the upgrade paths for the operating system.

See "Supported upgrade paths for SFCFSHA 6.0.1" on page 247.

# Upgrading the SFCFSHA stack on the first subcluster

**To upgrade the SFCFSHA stack on the first subcluster**

- **Note:** This procedure is based on an "in-place" upgrade path; that is, if the operating system is upgraded, the release will be the same, but only the path level will change. If you are moving from major operating system release to another, you must uninstall the SFCFSHA stack before you upgrade the operating system. After the operating system is upgraded, you must reinstall SFCFSHA.

  On the first half of the cluster, upgrade SFCFSHA by using the installsfcfsha script. For example use the installsfcfsha script as shown below:

  ```
  # ./installsfcfsha sys1
  ```

  where *<sys1>* is the node on the first subcluster.

  After the upgrade for first half of the cluster is complete, no GAB ports will be shown in `gabconfig -a` output.

  To upgrade your operating system, follow the normal procedures for your platform.

  **Note:** After the installation completes, you can safely ignore any instructions that the installer displays.

# Preparing the second subcluster

**To prepare the second subcluster**

1. On the second half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the application. [Downtime starts now.]
2. On the second half of the cluster, unmount the VxFS and CFS file systems that are not managed by VCS. Enter the following:

   ```
   # mount -p | grep vxfs
   ```

   Verify that no processes use the VxFS and CFS mount point. Enter the following:

   ```
   # fuser -c mount_point
   ```

   Stop any processes using a VxFS and CFS mount point with the mechanism provided by the application.

   Unmount the VxFS and CFS file system. Enter the following:

   ```
   # umount /mount_point
   ```

3. On the second half of the cluster, unfreeze all the VCS service groups on all the nodes using the following commands:

   ```
   # haconf -makerw
   # hagrp -unfreeze group_name -persistent
   # haconf -dump -makero
   ```

4. On the second half of the cluster, bring all the VCS service groups offline, including CVM group. Enter the following:

   ```
   # hagrp -offline group_name -sys sys4
   ```

5. On the second half of the cluster, verify that the VCS service groups are offline. Enter the following:

   ```
   # hagrp -state group_name
   ```

6. Stop VCS on the second half of the cluster. Enter the following:

   ```
   # hastop -local
   ```

7 On each node of the second half of the cluster, change the contents of the `/etc/vxfenmode` file to configure I/O fencing in disabled mode.

```
# cp /etc/vxfen.d/vxfenmode_disabled /etc/vxfenmode
# cat /etc/vxfenmode#
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=disabled
```

8 If the cluster-wide attribute UseFence is set to SCSI3, reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file, in second half of the cluster.

9 On the second half on cluster, stop the following SFCFSHA modules: VCS, VxFEN, ODM, GAB, and LLT. Enter the following:

For Solaris 9:

```
# modunload -i [modid of vxglm]
# modunload -i [modid of vxgms]
# /etc/init.d/vxodm stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

For Solaris 10 and 11:

```
# modunload -i [modid of vxglm]
# /usr/sbin/svcadm -st disable vxodm
# modunload -i [modid of vxgms]
# /usr/sbin/svcadm -st disable vxfen
# /usr/sbin/svcadm -st disable gab
# /usr/sbin/svcadm -st disable llt
```

Or

You can enter the following to stop all these processes:

```
# ./installer/installsfcfs/installsfcfsha - stop
```

**Note:** You can use this command to stop the processes only if you have upgraded to product version 5.1 or later. You should use the manual steps if you have upgraded from 5.0 MP3.

10 If the cluster-wide attribute UseFence is set to NONE, reset the value to SCSI3 in the `/etc/VRTSvcs/conf/config/main.cf` file, in first half of the cluster.

# Activating the first subcluster

**To activate the first subcluster**

1. Restart the upgraded nodes in the first half of the cluster:

   ```
   # /usr/sbin/shutdown -i6 -g0 -y
   ```

   When the first half of the cluster nodes come up, no GAB ports are OPEN. The following command does not show any GAB ports:

   ```
   # /sbin/gabconfig -a
   GAB Port Memberships
   ===============================================================
   ```

2. If required, force gab to form a cluster after the upgraded nodes are rebooted in first half of the cluster.

   ```
   # /sbin/gabconfig -x
   ```

   GAB ports a, b, d and h appear in `gabconfig -a` command output.

   **Note:** If port b and h are not up, you need to bring fencing and VCS manually online.

3. For nodes that use Solaris 10, start VCS in first half of the cluster:

   ```
   # svcadm enable system/vcs
   ```

4. On the first half of the cluster, bring the VCS service groups online. Enter the following:

   ```
   # hagrp -online group_name -sys node_name
   ```

   After you bring the CVM service group ONLINE, all the GAB ports u, v, w and f come ONLINE and all the CFS mounts service groups also come ONLINE automatically. Only failover service groups need to be brought ONLINE manually.

5. Manually mount the VxFS and CFS file systems that are not managed by VCS. [Downtime ends now.]

# Upgrading the operating system on the second subcluster

**To upgrade the operating system on the second subcluster**

- Enter the following.

  For Solaris 9:

```
# modunload -i [modid of vxglm]
# modunload -i [modid of vxgms]
# /etc/init.d/vxodm stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

  For Solaris 10 and 11:

```
# modunload -i [modid of vxglm]
# /usr/sbin/svcadm -st disable vxodm
# modunload -i [modid of vxgms]
# /usr/sbin/svcadm -st disable vxfen
# /usr/sbin/svcadm -st disable gab
# /usr/sbin/svcadm –st disable llt
```

  Or

  You can enter the following to stop all these processes:

```
# ./installer/installsfcfs/installsfcfsha - stop
```

  **Note:** You can use this command to stop the processes only if you have upgraded to product version 5.1 or later. You should use the manual steps if you have upgraded from 5.0 MP3.

  On the second half of the cluster, upgrade the operating system, if applicable. For instructions, see the upgrade paths for the operating system.

# Upgrading the second subcluster

**To upgrade the second subcluster**

- Enter the following:

```
# ./installsfcfsha node_name
```

# Completing the phased upgrade

**To complete the phased upgrade**

1. Verify that the cluster UUID on the nodes in the second subcluster is the same as the cluster UUID on the nodes in the first subcluster. Run the following command to display the cluster UUID:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -display nodename
```

   If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -copy -from_sys \
node01 -to_sys node03 node04
```

2. Restart the upgraded nodes in the second half of the cluster:

```
# /usr/sbin/shutdown -i6 -g0 -y
```

   When second half of the nodes come up, all the GAB ports a, b, d, h, u, v, w and f are ONLINE. Also all the CFS mounts service groups come online automatically.

3. For nodes that use Solaris 10, start VCS in first half of the cluster:

```
# svcadm enable system/vcs
```

4. Manually mount the VxFS and CFS file systems that are not managed by VCS in the second half of the cluster.
5. Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

6. On the CVM master node, upgrade the CVM protocol. Enter the following:

```
# vxdctl upgrade
```

Chapter 22

# Performing an automated SFCFSHA upgrade using response files

This chapter includes the following topics:


- Upgrading SFCFSHA using response files
- Response file variables to upgrade Veritas Storage Foundation Cluster File System High Availability
- Sample response file for upgrading Veritas Storage Foundation Cluster File System High Availability


## Upgrading SFCFSHA using response files

Typically, you can use the response file that the installer generates after you perform SFCFSHA upgrade on one system to upgrade SFCFSHA on other systems. You can also create a response file using the `makeresponsefile` option of the installer.

**To perform automated SFCFSHA upgrade**

1. Make sure the systems where you want to upgrade SFCFSHA meet the upgrade requirements.
2. Make sure the pre-upgrade tasks are completed.
3. Copy the response file to one of the systems where you want to upgrade SFCFSHA.
4. Edit the values of the response file variables as necessary.

5 Mount the product disc and navigate to the folder that contains the installation program.

6 Start the upgrade from the system to which you copied the response file. For example:

```
# ./installer -responsefile /tmp/response_file

# ./installsfcfsha -responsefile /tmp/response_file
```

Where /tmp/*response_file* is the response file's full path name.

# Response file variables to upgrade Veritas Storage Foundation Cluster File System High Availability

Table 22-1 lists the response file variables that you can define to configure SFCFSHA.

**Table 22-1** Response file variables for upgrading SFCFSHA

| Variable | Description |
|---|---|
| CFG{accepteula} | Specifies whether you agree with the EULA.pdf file on the media.<br>List or scalar: scalar<br>Optional or required: required |
| CFG{systems} | List of systems on which the product is to be installed or uninstalled.<br>List or scalar: list<br>Optional or required: required |
| CFG{opt}{keyfile} | Defines the location of an ssh keyfile that is used to communicate with all remote systems.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{tmppath} | Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp.<br>List or scalar: scalar<br>Optional or required: optional |

**Table 22-1** Response file variables for upgrading SFCFSHA *(continued)*

| Variable | Description |
|---|---|
| CFG{opt}{logpath} | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{upgrade} | Upgrades all packages installed, without configuration.<br>List or scalar: list<br>Optional or required: optional |
| CFG{mirrordgname}{system} | If the root dg is encapsulated and you select split mirror is selected:<br>Splits the target disk group name for a system.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{splitmirror}{system} | If the root dg is encapsulated and you select split mirror is selected:<br>Indicates the system where you want a split mirror backup disk group created.<br>List or scalar: scalar<br>Optional or required: optional |

# Sample response file for upgrading Veritas Storage Foundation Cluster File System High Availability

The following example shows a response file for upgrading Veritas Storage Foundation Cluster File System High Availability.

```
our %CFG;
$CFG{accepteula}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{redirect}=1;
$CFG{opt}{upgrade}=1;
$CFG{opt}{vr}=1;
$CFG{systems}=[ qw(lxvcs05 lxvcs06) ];
$CFG{vcs_allowcomms}=1;
```

```
1;
```

Chapter 23

# Upgrading the operating system

This chapter includes the following topics:


- Upgrading the Solaris operating system


## Upgrading the Solaris operating system

If you are running Veritas Storage Foundation Cluster File System High Availability 6.0.1 with an earlier release of the Solaris operating system, you can upgrade the Solaris operating system using the following procedure.

---

**Warning:** You should only use this procedure to upgrade the Solaris operating system if you are running Veritas Storage Foundation Cluster File System High Availability 6.0.1.

---

The directory `/opt` must exist, be writable, and must not be a symbolic link. This is because the volumes not temporarily converted by the `upgrade_start` are unavailable during the upgrade process. If you have a symbolic link from `/opt` to one of the unconverted volumes, the symbolic link will not function during the upgrade and items in `/opt` will not be installed.

**To upgrade the Solaris operating system only**

1. Bring the system down to single-user mode using the following command:

   ```
   # init S
   ```

   You must mount `/opt` manually if `/opt` is on its own partition.

2. Load and mount the software disc from the currently installed version of Veritas Storage Foundation Cluster File System High Availability.

   See "Mounting the product disc" on page 63.

3. Change directory:

   ```
   # cd /mount_point/scripts
   ```

4. Run the `upgrade_start` with the `-check` argument to detect any problems that exist which could prevent a successful upgrade. Use the `upgrade_start` script that was supplied with the currently installed SF release. If this command reports success, you can proceed with running the `upgrade_start` script, but if it reports errors, correct the problem(s) and rerun `upgrade_start -check`.

   ```
   # ./upgrade_start -check
   ```

5. Run the `upgrade_start` script so that the system can come up with partitions. The `upgrade_start` script searches for volumes containing file systems, and if any are found, converts them to partitions:

   ```
   # ./upgrade_start
   ```

6. Bring the system down to run level 0.

   ```
   # init 0
   ```

7. Upgrade the operating system to a supported version of Solaris.

   You should boot up the system from run level 0 depending on the Solaris upgrade procedure that you want to follow. Refer to the Solaris installation documentation for instructions on how to upgrade the Solaris operating system.

8. After installing the Solaris operating system, install any Solaris patches required by Veritas Storage Foundation Cluster File System High Availability 6.0.1.

   See the *Veritas Storage Foundation Cluster File System High Availability Release Notes*.

9 After the system is up with the upgraded Solaris operating system, bring the system down to single-user mode by entering:

```
# init S
```

10 Ensure that `/opt` is mounted.

11 Load and mount the software disc from the currently installed version of Veritas Storage Foundation Cluster File System High Availability.

12 If you upgraded to Solaris 10, you must reinstall certain Veritas Storage Foundation Cluster File System High Availability packages in order to support Solaris 10 functionality.

To reinstall the required packages, follow the steps below:

- Remove the existing packages in the reverse order of their installation. For example, if you chose the installation of all packages then uninstall those in the following order.

```
# pkgrm VRTSsfmh VRTSodm VRTSgms
VRTScavf VRTSglm VRTSdbed VRTSvcsea VRTSvcsag
VRTScps VRTSvcs VRTSamf VRTSvxfen VRTSgab
VRTSllt VRTSat VRTSfssdk VRTSvxfs VRTSob
VRTSaslapm VRTSvxvm VRTSspt VRTSperl VRTSvlic
```

- Run the following commands.
  To obtain a list of recommended packages to install:

```
# ./installsfcfsha -recpkgs
```

  Or
  To obtain a list of all packages to install:

```
# ./installsfcfsha -allpkgs
```

- Change to the directory containing the appropriate packages.

```
# cd /mount_point/pkgs
```

- Use the `pkgadd` command to install the packages from the list you generated.

- Reboot the system.

13 Complete the upgrade from the software disc from the currently installed version of Storage Foundation by entering:

```
# devlinks
# ./upgrade_finish
```

Chapter 24

# Upgrading Veritas Volume Replicator

This chapter includes the following topics:


- Upgrading Veritas Volume Replicator


## Upgrading Veritas Volume Replicator

If a previous version of Veritas Volume Replicator (VVR) is configured, the product installer upgrades VVR automatically when you upgrade the Storage Foundation products.

When upgrading from 4.1 MP1 or later, you have the option to upgrade without disrupting replication.

See "Upgrading VVR without disrupting replication" on page 301.

### 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 254.

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 5.1 or later to VVR 6.0.1 on the Secondary.

3. Do one of the following:

   - Upgrade the disk group now. Enter the following:

     ```
     # vxdg upgrade dgname
     ```

   - Upgrade the disk group later.
     If you upgrade the disk group later, be sure to pause replication before you upgrade the disk group.

4. 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.

**To upgrade the Primary**

1. Stop replication to the Primary host by initiating a Primary pause using the following command:

   ```
   # vradmin -g diskgroup pauserep local_rvgname
   ```

2. Upgrade from VVR 5.1 or later to VVR 6.0.1 on the Secondary.

3. Do one of the following:

   - Upgrade the disk group now. Enter the following:

```
# vxdg upgrade dgname
```

- Upgrade the disk group later.
  If you upgrade the disk group later, be sure to pause replication before you upgrade the disk group.

4 Resume the replication from the Primary using the following command:

```
# vradmin -g diskgroup resumerep local_rvgname
    sec_hostname
```

See “Planning an upgrade from the previous VVR version” on page 254.

Chapter 25

# Upgrading language packages

This chapter includes the following topics:


- Upgrading language packages


## Upgrading language packages

If you are upgrading Veritas products in a language other than English, you must install the required language packages after installing the English packages.Verify that the English installation is correct before proceeding.

Install the language packages as for an initial installation.

See “Installing language packages” on page 72.

Chapter 26

# Migrating from SFHA to SFCFSHA

This chapter includes the following topics:


- Migrating from SFHA to SFCFSHA 6.0.1


## Migrating from SFHA to SFCFSHA 6.0.1

This section describes how to migrate Storage Foundation High Availability (SFHA) 6.0.1 to Storage Foundation Cluster File System High Availability (SFCFSHA) 6.0.1.

The product installer does not support direct upgrades from a previous version of SFHA or SFCFSHA6.0.1. Ensure that you upgrade the existing SFHA to 6.0.1 before beginning this procedure.

**To migrate from SFHA 6.0.1 to SFCFSHA 6.0.1**

1. Back up the `main.cf` file before beginning the upgrade.
2. Confirm that the storage disks are visible on all the nodes in the 6.0.1 SFHA cluster.
3. Bring all the failover service groups offline, using the following command:

   ```
   # hagrp -offline group_name -any
   ```

   The above command brings the service group offline on the node where the service group is currently online.

4 Unmount all the VxFS file systems which are not under VCS control. If the local file systems are under VCS control, then VCS unmounts the file systems when the failover service group is brought offline in step 3.

On the nodes that have any mounted VxFS local file systems that are not under VCS control:

```
# umount -F vxfs -a
```

5 Stop all of the activity on the volumes and deport the local disk groups. If the local disk groups are part of VCS failover service groups, then VCS deports the disk groups when the failover service group is brought offline in step 3.

```
# vxvol -g diskgroup_name stopall
# vxdg deport diskgroup_name
```

6 Upgrade the existing SFHA to SFCFSHA 6.0.1:

```
# ./installsfcfsha
```

7 After installation is completed, the install script asks you to install licenses. Enter the correct license key to register the key.

8 The installer prompts to reconfigure the VCS. Provide the same cluster name, cluster ID, and LLT link interfaces details that were used during configuration of the SFHA cluster.

9 Find out which node is the CVM master, using the following command:

```
# vxdctl -c mode
```

10 On the CVM Master node, re-import all the required disk groups which must be in shared mode:

```
# vxdg -s import diskgroup_name
```

11 Start all the volumes whose disk groups have been imported as shared in step 10. Use the following command:

```
# vxdg -g diskgroup_name startall
```

12 Run the following command for each of the file systems you want to mount as CFS:

```
# cfsmntadm add diskgroup_name volume_name mount_point \
 all=cluster_mount_options
```

13 Run the following command to mount CFS file systems on all the nodes:

```
# cfsmount mount_point
```

14 Import all other local disk groups which have not been imported in shared mode in step 10.

```
# vxdg import diskgroup_name
```

Start all the volumes of these disk groups using:

```
# vxvol -g diskgroup_name startall
```

Mount these volumes.

15 For any of the file systems which VCS needs to monitor through failover service groups, create these failover service groups by adding the Mount, Diskgroup & Volume resources for VxFS file systems under VCS control.

Chapter 27

# Upgrading SFCFSHA using Live Upgrade

This chapter includes the following topics:


- About Live Upgrade
- Supported upgrade paths for Live Upgrade
- Performing Live Upgrade in a Solaris zone environment
- Before you upgrade SFCFSHA using Solaris Live Upgrade
- Upgrading SFCFSHA and Solaris using Live Upgrade
- Upgrading Solaris using Live Upgrade
- Upgrading SFCFSHA using Live Upgrade
- Administering boot environments

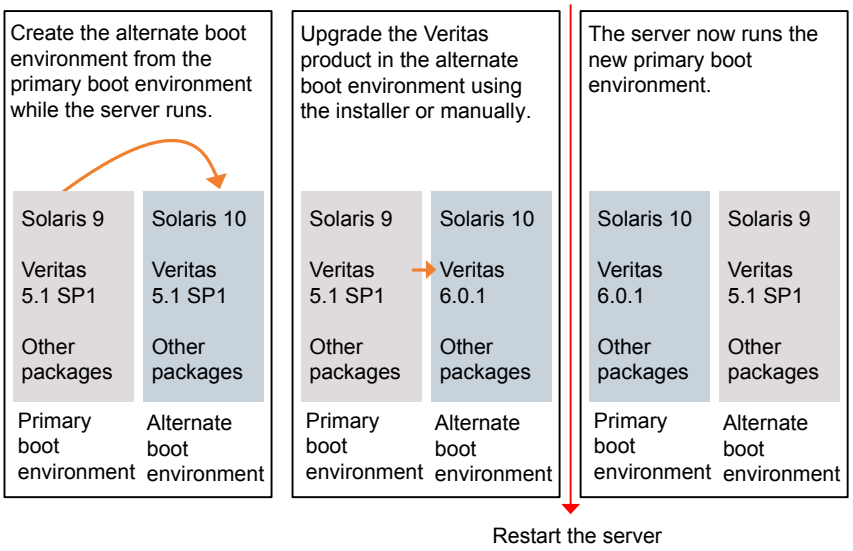

## About Live Upgrade

You can use Live Upgrade on Solaris 10 systems to perform the following types of upgrade:

- Upgrade the operating system and SFCFSHA.
  See "Upgrading SFCFSHA and Solaris using Live Upgrade" on page 315.
- Upgrade the operating system.
  See "Upgrading Solaris using Live Upgrade" on page 324.
- Upgrade SFCFSHA.
  See "Upgrading SFCFSHA using Live Upgrade" on page 326.

Figure 27-1 illustrates an example of an upgrade of Veritas products from 5.1 SP1 to 6.0.1, and the operating system from Solaris 9 to Solaris 10.

**Figure 27-1** Live Upgrade process




Some service groups (failover and parallel) may be online in this cluster and they are not affected by the Live Upgrade process. The only downtime experienced is when the server is rebooted to boot into the alternate boot disk.

## About Live Upgrade in a Veritas Volume Replicator (VVR) environment

In a SFCFSHA environment that uses Veritas Volume Replicator, the following scripts provide the means to upgrade the VVR configuration:

- vvr_upgrade_lu_start
- vvr_upgrade_lu_finish

The scripts are available in the scripts directory in the install media.

This section provides an overview of the VVR upgrade process. See the Live Upgrade procedures for SFCFSHA for the complete procedure.

See "Upgrading SFCFSHA and Solaris using Live Upgrade" on page 315.

- Use the `vxlustart` script to perform upgrade steps for SFCFSHA.

- Immediately before rebooting the system to switch over to the alternate boot environment, run the `vvr_upgrade_lu_start` script.

  **Note:** Use the `vvr_upgrade_lu_start` script only when the applications are stopped and the next step is to switch over to the alternate boot environment.

- After the `vvr_upgrade_lu_start` script completes successfully, reboot the system. This reboot results in the system booting from the alternate boot environment.
- After the objects are recovered, and the disk group version is upgraded (if desired), run the `vvr_upgrade_lu_finish` script.

# Supported upgrade paths for Live Upgrade

The systems where you plan to use Live Upgrade must run Solaris 9 or Solaris 10. You can upgrade from systems that run Solaris 9, but SFCFSHA 6.0.1 is not supported on Solaris 9. The `vxlustart` and `vxlufinish` are not supported on Solaris 11. ZFS root is not supported by `vxlustart` script.

For Live Upgrade, if the alternative root environment also has a zone, you cannot install `VRTSodm`. You must remove the `VRTSodm` package first then install the Storage Foundation product on the alternate boot environment. After you reboot the alternative root, you can install `VRTSodm`.

SFCFSHA version must be at least 5.0 MP3.

Symantec requires that both global and non-global zones run the same version of Veritas products.

You can use Live Upgrade in the following virtualized environments:

**Table 27-1** Live Upgrade support in virtualized environments

| Environment | Procedure |
|---|---|
| Solaris native zones | Perform Live Upgrade to upgrade both global and non-global zones.<br>If you have a zone root that resides on a VxVM volume, use the following procedure.<br>See "Performing Live Upgrade in a Solaris zone environment" on page 311.<br>Use the standard procedure for the other standby nodes.<br>See "Upgrading SFCFSHA and Solaris using Live Upgrade" on page 315. |
| Solaris branded zones (BrandZ) | Perform Live Upgrade to upgrade the global zone.<br>See "Upgrading SFCFSHA and Solaris using Live Upgrade" on page 315.<br>Manually upgrade the branded zone separately.<br>Note that while you can perform a Live Upgrade in the presence of branded zones, the branded zones are not upgraded. |
| Oracle VM Server for SPARC | Perform Live Upgrade on the Control domain only.<br>Perform Live Upgrade on the Guest domain only.<br>Use the standard Live Upgrade procedure for both types of logical domains.<br>See "Upgrading SFCFSHA and Solaris using Live Upgrade" on page 315. |

# Performing Live Upgrade in a Solaris zone environment

If you have a zone root that resides on a VxVM volume, then you must use the following procedure to perform a Live Upgrade on the nodes where zones are online.

You have to create a VxVM volume of the same or more size as that of the existing zone root for copying the file system contents to alternate boot environment. Use VxVM commands for creating the volume.

By default, resources of the Zone agent attribute, `BootState` is set to "multi-user." After you complete the upgrade, you may need to adjust this attribute to the appropriate value before you start your zone through VCS.

**Note:** Symantec recommends that you set `BootState` to "multi-user-server" to run applications inside non-global zones.

# Before you upgrade SFCFSHA using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

**To prepare for the Live Upgrade**

1. Make sure that the SFCFSHA installation media and the operating system installation images are available and on hand.
2. On the nodes to be upgraded, select an alternate boot disk that is at least the same size as the root partition of the primary boot disk.

   If the primary boot disk is mirrored, you need to break off the mirror for the alternate boot disk.
3. Before you perform the Live Upgrade, take offline any services that involve non-root file systems. This prevents file systems from being copied to the alternate boot environment that could potentially cause a root file system to run out of space.
4. On the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.
5. The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:
   - Remove the installed Live Upgrade packages for the current operating system version:
     All Solaris versions: SUNWluu, SUNWlur packages.
     Solaris 10 update 7 or later also requires: SUNWlucfg package.
     Solaris 10 zones or Branded zones also requires: SUNWluzone package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:
     All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.
     Solaris 10 zones or Branded zones also requires: SUNWluzone package.

**Note:** While you can perform Live Upgrade in the presence of branded zones, they must be halted, and the branded zones themselves are not upgraded.

Solaris installation media comes with a script for this purpose named liveupgrade20. Find the script at /*cdrom*/*solaris_release*/Tools/Installers/liveupgrade20. If scripting, you can use:

```
# /cdrom/solaris_release/Tools/Installers/liveupgrade20 \
-nodisplay -noconsole
```

6 Symantec provides the `vxlustart` script that runs a series of commands to create the alternate boot disk for the upgrade.

To preview the commands, specify the `vxlustart` script with the `-V` option.

Symantec recommends that you preview the commands to ensure there are no problems before beginning the Live Upgrade process.

The `vxlustart` script is located on the distribution media, in the scripts directory.

```
# cd /cdrom/scripts
```

```
# ./vxlustart -V -u targetos_version -s osimage_path -d diskname
```

-V Lists the commands to be executed during the upgrade process without executing them and pre-checks the validity of the command.

If the operating system is being upgraded, the user will be prompted to compare the patches that are installed on the image with the patches installed on the primary boot disk to determine if any critical patches are missing from the new operating system image.

-u Specifies the operating system version for the upgrade on the alternate boot disk. For example, use `5.10` for Solaris 10.

-U Specifies that only the Storage Foundation products are upgraded. The operating system is cloned from the primary boot disk.

-s Indicates the path of the operating system image to be installed on the alternate boot disk. If this option is omitted, you are prompted to insert the discs that contain the operating system image.

If the `-U` option is specified, you can omit the **-s** option. The operating system is cloned from the primary boot disk.

-d Indicates the name of the alternate boot disk on which you intend to upgrade. If you do not specify this option with the script, you are prompted for the disk information.

-v Indicates verbose, the executing commands display before they run.

-Y Indicates a default yes with no questions asked.

-D Prints with debug option on, and is for debugging.

-F Specifies the rootdisk's file system, where the default is `ufs`.

-t Specifies the number of CDs involved in upgrade.

-r Specifies that if the machine crashes or reboots before the `vxlufinish` command is run, the alternate disk is remounted using this option.

For example, to preview the commands to upgrade only the Veritas product:

```
# ./vxlustart -V -u 5.10 -U -d disk_name
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6 -d c0t1d0s0
```

**Note:** This command prompts you to compare the patches that are installed on the image with the patches installed on the primary boot disk. If any patches are missing from the new operating system's image, note the patch numbers. To ensure the alternate boot disk is the same as the primary boot disk, you will need to install these patches on the alternate boot disk.

7 If the specified image is missing patches that are installed on the primary boot disk, note the patch numbers. To ensure that the alternate boot disk is the same as the primary boot disk, you need to install any missing patches on the alternate boot disk.

# Upgrading SFCFSHA and Solaris using Live Upgrade

Upgrading SFCFSHA using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See "Before you upgrade SFCFSHA using Solaris Live Upgrade" on page 312.
- Create a new boot environment on the alternate boot disk.
  See "Creating a new boot environment on the alternate boot disk" on page 316.
- Upgrade to Veritas Storage Foundation Cluster File System High Availability 6.0.1 on the alternate boot environment manually or using the installer.

  To upgrade SFCFSHA manually, refer to the following procedure:

  - See "Upgrading SFCFSHA manually" on page 320.

  To upgrade SFCFSHA using the installer, refer to the following procedure:

  - See "Upgrading SFCFSHA using the installer for a Live Upgrade" on page 319.
- Switch the alternate boot environment to be the new primary.
  See "Completing the Live Upgrade " on page 322.
- Verify Live Upgrade of SFCFSHA.
  See "Verifying Live Upgrade of SFCFSHA" on page 323.

# Creating a new boot environment on the alternate boot disk

Run the `vxlustart` command on each node in the cluster to create a new boot environment on the alternate boot disk.

Table 27-2 shows the various usages of the `vxlustart` option.

**Table 27-2** Usages of the vxlustart option

| vxlustart option | Usage |
|---|---|
| -V | Lists the commands to be executed during the upgrade process without executing them. |
| -v | Indicates verbose, print commands before executing them. |
| -f | Forces the vtoc creation on the disk. |
| -Y | Indicates a default yes with no questions asked. |
| -m | Uses the already existing vtoc on the disk. |
| -D | Prints with debug option on, and is for debugging. |
| -U | Specifies that only the Storage Foundation products are upgraded. |
| -g | Specifies the DG to which the rootdisk belongs. Optional. |
| -d | Indicates the name of the alternate boot disk **c#t#d#s2** on which you intend to upgrade. The default disk is **mirrordisk**. |
| -u | Specifies the operating system version for the upgrade on the alternate boot disk. For example, use `5.10` for Solaris 10.<br>If you want to upgrade only SF products, specify the current OS version. |
| -F | Specifies the rootdisk's file system, where the default is `ufs`. |
| -s | Specifies the path to the Solaris image. It can be a network/directory path. If the installation uses the CD, this option must not be specified. See *Solaris Live Upgrade installation guide* for more information about the path. |
| -r | If the machine crash/reboot before vxlufinish, you can remount the alternate disk using this option. |
| -k | Specifies the location of file containing auto-registration information. This file is required by luupgrade(1M) for OS upgrade to Solaris 10 9/10 or a later release. |
| -x | Excludes file from newly created BE. (`lucreate -x` option) |

**Table 27-2** Usages of the vxlustart option *(continued)*

| vxlustart option | Usage |
|---|---|
| -X | Excludes file list from newly created BE. (`lucreate -f` option) |
| -i | Includes file from newly created BE. (`lucreate -y` option) |
| -I | Includes file list from newly created BE. (`lucreate -Y` option) |
| -z | Filters file list from newly created BE. (`lucreate -z` option) |
| -w | Specifies additional mount points. (`lucreate -m` option) |
| -W | Specifies additional mount points in a file (`lucreate -M` option) |

If the `-U` option is specified, you can omit the `-s` option. The operating system is cloned from the primary boot disk.

Symantec recommends that you preview the commands with `-V` option to ensure there are no problems before beginning the Live Upgrade process. The `vxlustart` script is located on the distribution media, in the scripts directory.

For example, to preview the commands to upgrade only the Symantec product:

```
# ./vxlustart -V -u 5.10 -U -d disk_name
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6 -d c0t1d0s2
```

In the procedure examples, the primary or current boot environment resides on*Disk0 (c0t0d0s2)* and the alternate or inactive boot environment resides on *Disk1 (c0t1d0s2)*.

**Note:** This step can take several hours to complete. Do not interrupt the session as it may leave the boot environment unstable.

At the end of the process:

- The Solaris operating system on the alternate boot disk is upgraded, if you have chosen to upgrade the operating system.
- A new boot environment is created on the alternate boot disk by cloning the primary boot environment.

**To create a new boot environment on the alternate boot disk**

Perform the steps in this procedure on each node in the cluster.

1 Navigate to the install media for the Symantec products:

```
# cd /cdrom/scripts
```

2 View the list of VxVM disks on which you want to create the new boot environment.

```
# vxdisk list
```

3 Run one of the following commands to perform the upgrade:

To upgrade the operating system, by itself or together with upgrading the Veritas products:

```
# ./vxlustart -v -u targetos_version \
-s osimage_path -d disk_name
```

where *targetos_version* is the version of the operating system

*osimage_path* is the full path to the operating system image

*disk_name* is the name of the disk as displayed in the output of step 2.

To upgrade the Veritas product only:

```
# ./vxlustart -v -u 5.10 -U -d disk_name
```

The options to the `vxlustart` command are listed in the preupgrade section.

See "Before you upgrade SFCFSHA using Solaris Live Upgrade" on page 312.

For example, to upgrade to Solaris 10 update 6:

```
# ./vxlustart -v -u 5.10 -s /mnt/Solaris_10u6
```

4 Review the output of `df` commands and note the new mount points. If the system is rebooted before completion of the upgrade or if the mounts become unmounted, you may need to remount the disks.

If you need to remount, run the command:

```
# vxlustart -r -u targetos_version -d disk_name
```

5 After the alternate boot disk is created and mounted on */altroot.5.10*, install any operating system patches or packages on the alternate boot disk that are required for the Veritas product installation:

```
# pkgadd -R /altroot.5.10 -d pkg_dir
```

# Upgrading SFCFSHA using the installer for a Live Upgrade

You can use the Veritas product installer to upgrade SFCFSHA as part of the Live Upgrade.

On a node in the cluster, run the installer on the alternate boot disk to upgrade SFCFSHA on all the nodes in the cluster. The program uninstalls the existing version of SFCFSHA on the alternate boot disk during the process.

At the end of the process the following occurs:

- Veritas Storage Foundation Cluster File System High Availability 6.0.1 is installed on the alternate boot disk.

**To perform Live Upgrade of SFCFSHA using the installer**

1. Insert the product disc with Veritas Storage Foundation Cluster File System High Availability 6.0.1 or access your copy of the software on the network.
2. Run the installer script specifying the root path as the alternate boot disk, enter the following:

   ```
   # ./installsfcfsha -upgrade -rootpath /altroot.5.10
   ```

   See "Removing and reinstalling SFCFSHA using the installer" on page 325.
3. Enter the names of the nodes that you want to upgrade to Veritas Storage Foundation Cluster File System High Availability 6.0.1.

   **Note:** Make sure that the installed version of VxFS uses the disk layout version 6 or later. If you are on a previous disk layout version, upgrade the version before you proceed with the SFCFSHA installation.

   The installer displays the list of packages to be installed or upgraded on the nodes.
4. Press **Return** to continue with the installation.

   During Live Upgrade, if the OS of the alternate boot disk is upgraded, the installer will not update the VCS configurations for Oracle, Netlsnr, and Sybase resources. If cluster configurations include these resources, you will be prompted to run a list of commands to manually update the configurations after the cluster restarts from the alternate boot disks.
5. Verify that the version of the Veritas packages on the alternate boot disk is 6.0.1.

   ```
   # pkginfo -R /altroot.5.10 -l VRTSpkgname
   ```

   For example:

```
# pkginfo -R /altroot.5.10 -l VRTSvxvm
```

Review the installation logs at `/altroot.5.10/opt/VRTS/install/logs`.

# Upgrading SFCFSHA manually

You can perform a manual upgrade of SFCFSHA using Live Upgrade. On each node, remove and install the appropriate SFCFSHA packages.

---

**Note:** `#cp /mnt/etc/VRTSvcs/conf/config/PrivNIC.cf /tmp/PrivNIC.cf.save`

---

At the end of the process the following occurs:

- Veritas Storage Foundation Cluster File System High Availability 6.0.1 is installed on the alternate boot disk.

**To perform Live Upgrade of SFCFSHA manually**

1. Remove the SFCFSHA packages on the alternate boot disk in the following order:

```
# pkgrm   -R  /altroot.5.10 \
VRTSodm VRTSgms VRTSvxmsa VRTScavf VRTSglm VRTSfsmnd \
VRTSfssdk VRTSfsman VRTSvrw VRTSvcsvr VRTSvrpro \
VRTSddlpr VRTSvdid VRTSalloc VRTSdcli VRTSvmpro \
VRTSvmman VRTSfspro VRTSdsa VRTSvxvm VRTScmccc \
VRTScmcs VRTSacclib VRTScssim VRTScscm VRTSweb \
VRTScscw VRTScutil VRTSjre15 VRTSvcsmn VRTSvcsag \
VRTSvcsmg VRTSvcs VRTSvxfen VRTSgab VRTSllt \
VRTSvxfs VRTSspt VRTSaa VRTSmh VRTSccg VRTSobgui \
VRTSob VRTSobc33 VRTSat VRTSpbx VRTSicsco VRTSvlic \
VRTSperl
```

   The `-R` option removes the packages from the root path `/altroot.5.10` on the alternate boot disk.

   Note that this package list is an example. Full package lists vary from release to release and by product option.

2. Install SFCFSHA 6.0.1 packages in the following order one at a time to the alternate boot disk using the `pkgadd` command:

```
VRTSvlic VRTSperl VRTSspt VRTSvxvm
VRTSaslapm VRTSob VRTSsfmh VRTSvxfs
VRTSfsadv VRTSfssdk VRTSllt VRTSgab
VRTSvxfen VRTSamf VRTSvcs VRTScps
```

```
VRTSvcsag VRTSvcsea VRTSdbed VRTSglm
VRTScavf VRTSgms VRTSodm VRTSsfcpi601
```

For example:

```
# pkgadd -R /altroot.5.10 -d package_name.pkg
```

Where you replace *package_name.pkg* with a package's name, for example VRTSvxvm.pkg.

```
#  pkgadd -R /altroot.5.10 -d VRTSvxvm.pkg
```

3 Verify that the version of the Veritas packages on the alternate boot disk is 6.0.1.

```
# pkginfo -R /altrootpath -l VRTSpkgname
```

For example:

```
# pkginfo -R /altroot.5.10 -l VRTSvxvm
```

4 Set the INSTALL_ROOT_PATH environment variable to the root path, and then configure a VCS cluster UUID on the alternative root path. Enter the following commands:

```
# export INSTALL_ROOT_PATH=/altroot.5.10
# /altroot.5.10/opt/VRTSvcs/bin/uuidconfig.pl -clus -configure \
-use_llthost
```

5 Confirm that you have created the Universal Unique Identifier for the cluster:

```
# /altroot.5.10/opt/VRTSvcs/bin/uuidconfig.pl -clus -display \
-use_llthost
```

6 In a zones or branded zones environment, perform the following steps to ensure that all non-global zones contain a universally unique identifier (UUID):

```
# zoneadm -z zone1 detach
# zoneadm -z zone1 attach
# zoneadm -z zone1 boot
# zoneadm list -p
0:global:running:/::native:shared
3:zone1:running:/zone1:3770b7b9-f96a-ef34-f4c5-bc125d56ec27:
native:shared
```

For a Solaris environment without zones, run the following command on the alternate root path of any one node in the cluster to configure a unique VCS cluster ID:

```
# /mnt/opt/VRTSvcs/bin/uuidconfig.pl -clus -configure -use_llthost
```

The `-use_llthost` option indicates that the `/etc/llthost` file is used to determine the names of the nodes in the cluster. Alternatively, you can specify the node names instead of the file name.

## Completing the Live Upgrade

At the end of the process:

- If the original primary boot disk was encapsulated, the alternate boot disk is encapsulated.
- The alternate boot environment is activated.
- The system is booted from the alternate boot disk.

**To complete the Live Upgrade**

1. Complete the Live upgrade process using one of the following commands. You must enter the command on all nodes in the cluster.

   If the primary root disk is not encapsulated, run the following command:

   ```
   # ./vxlufinish -u target_os_version
   Live Upgrade finish on the Solaris release <5.10>
   ```

   If the primary root disk is encapsulated by VxVM, run the following command:

   ```
   # ./vxlufinish -u target_os_version -g diskgroup
   Live Upgrade finish on the Solaris release <5.10>
   ```

   The Live Upgrade process encapsulates the alternate root disk if the primary root disk was encapsulated.

2. If the system crashes or reboots before Live Upgrade completes successfully, you can remount the alternate disk using the following command:

   ```
   # ./vxlustart -r -u target_os_version
   ```

   Then, rerun the vxlufinish command from step 1

   ```
   # ./vxlufinish -u target_os_version
   ```

3 If you are upgrading VVR, run the `vvr_upgrade_lu_start` command.

**Note:** Only run the `vvr_upgrade_lu_start` command when you are ready to reboot the nodes and switch over to the alternate boot environment.

4 **Note:** Do not use the `reboot`, `halt`, or `uadmin` commands to reboot the system. Use either the `init` or the `shutdown` commands to enable the system to boot using the alternate boot environment.

You can ignore the following error if it appears: ERROR: boot environment <dest.13445> already mounted on </altroot.5.10>.

```
# shutdown -g0 -y -i6
```

5 After the alternate boot environment is activated, you can switch boot environments. If the root disk is encapsulated, refer to the procedure to switch the boot environments manually.

See "Administering boot environments" on page 326.

6 After the upgrade, perform any required post-upgrade tasks such as upgrading the disk group.

7 After the objects are recovered, and the disk group version is upgraded (if desired), run the `vvr_upgrade_lu_finish` script.

8 If you want to upgrade CP server systems that use VCS or SFHA to this version, make sure that you upgraded all application clusters to this version. Then, upgrade VCS or SFHA on the CP server systems.

For instructions to upgrade VCS or SFHA on the CP server systems, see the VCS or SFHA Installation Guide.

## Verifying Live Upgrade of SFCFSHA

To ensure that Live Upgrade has completed successfully, verify that all the nodes have booted from the alternate boot environment and joined the cluster.

**To verify that Live Upgrade completed successfully**

1 Verify that the alternate boot environment is active.

```
# lustatus
```

If the alternate boot environment is not active, you can revert to the primary boot environment.

See "Reverting to the primary boot environment" on page 326.

2 In a cluster environment, make sure that all the GAB ports are up. Note different ports appear for different products.

3 Perform other verification as required to ensure that the new boot environment is configured correctly. The non-global zones must be brought to configured state and then attached with `-U` option so that packages are upgraded inside the non-global zone also.

4 In a zone environment, verify the zone configuration.

# Upgrading Solaris using Live Upgrade

If you are upgrading Solaris only, you must remove and reinstall SFCFSHA from the alternate boot environment prior to completing the Live Upgrade. You must remove and reinstall because SFCFSHA has kernel components that are specific to Solaris operating system versions. The correct version of the SFCFSHA packages must be installed.

Upgrading Solaris using Live Upgrade involves the following steps:

- Preparing to upgrade using Solaris Live Upgrade.
  See "Before you upgrade SFCFSHA using Solaris Live Upgrade" on page 312.
- Creating a new boot environment on the alternate boot disk
  See "Creating a new boot environment on the alternate boot disk" on page 316.
- Removing and reinstalling Veritas Storage Foundation Cluster File System High Availability 6.0.1 on the alternate boot environment:
  Using manual steps:
  See "Upgrading SFCFSHA manually" on page 320.
  Using the installer:
  See "Removing and reinstalling SFCFSHA using the installer" on page 325.

---

**Note:** Do NOT configure the Veritas Storage Foundation Cluster File System High Availability 6.0.1

---

- Switching the alternate boot environment to be the new primary
  See "Completing the Live Upgrade " on page 322.
- Verifying Live Upgrade of SFCFSHA.
  See "Verifying Live Upgrade of SFCFSHA" on page 323.

# Removing and reinstalling SFCFSHA using the installer

SFCFSHA has kernel components that are specific for Solaris operating system versions. When you use Solaris Live Upgrade to upgrade the Solaris operating system, you must complete these steps to ensure the correct version of SFCFSHA components are installed.

On a node in the cluster, run the installer on the alternate boot disk to remove and reinstall Veritas Storage Foundation Cluster File System High Availability 6.0.1 on all the nodes in the cluster.

At the end of the process the following occurs:

- Veritas Storage Foundation Cluster File System High Availability 6.0.1 is installed on the alternate boot disk, with the correct binaries for the new operating system version

**To remove and reinstall SFCFSHA using the installer**

1. Enter the names of the nodes that you want to uninstall.

   The installer displays the list of packages that will be uninstalled.

2. Press **Return** to continue.

3. Install using the installer script, specifying the root path as the alternate boot disk as follows:

   ```
   # /cdrom/storage_foundation_cluster_file_system_ha/installsfcfsha \
   -install -rootpath /altrootpath
   ```

4. Press **Return** to continue.

5. Verify that the version of the Veritas packages on the alternate boot disk is 6.0.1.

   ```
   # pkginfo -R /altroot.5.10 -l VRTSpkgname
   ```

   For example:

   ```
   # pkginfo -R /altroot.5.10 -l VRTSvxvm
   ```

   Review the installation logs at `/altroot.5.10/opt/VRTS/install/log`.

# Upgrading SFCFSHA using Live Upgrade

Perform the Live Upgrade manually or use the installer. The nodes will not form a cluster until all of the nodes are upgraded to Veritas Storage Foundation Cluster File System High Availability 6.0.1. At the end of the Live Upgrade of the last node, all the nodes must boot from the alternate boot environment and join the cluster.

Upgrading SFCFSHA using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See "Before you upgrade SFCFSHA using Solaris Live Upgrade" on page 312.
- Create a new boot environment on the alternate boot disk.
  See "Creating a new boot environment on the alternate boot disk" on page 316.
- Upgrade to Veritas Storage Foundation Cluster File System High Availability 6.0.1 on the alternate boot environment manually or using the installer. Refer to one of the following:

  To upgrade SFCFSHA manually:

  - See "Upgrading SFCFSHA manually" on page 320.

  To upgrade SFCFSHA using the installer:

  - See "Upgrading SFCFSHA using the installer for a Live Upgrade" on page 319.
- Switch the alternate boot environment to be the new primary.
  See "Completing the Live Upgrade " on page 322.
- Verify Live Upgrade of SFCFSHA.
  See "Verifying Live Upgrade of SFCFSHA" on page 323.

# Administering boot environments

Use the following procedures to perform relevant administrative tasks for boot environments.

## Reverting to the primary boot environment

If the alternate boot environment fails to start, you can revert to the primary boot environment.

On each node, start the system from the primary boot environment in the PROM monitor mode.

```
ok> boot disk0
```

where *disk0* is the primary boot disk.

# Switching the boot environment for Solaris SPARC

You do not have to perform the following procedures to switch the boot environment when you use the `vxlufinish` scripts to process Live Upgrade. You must perform the following procedures when you perform a manual Live Upgrade.

Two different procedures exist to switch the boot environment, choose one of the following procedures based on the encapsulation of the root disk:

- See "To switch the boot environment if the root disk is not encapsulated" on page 327.
- See "To switch the boot environment if the root disk is encapsulated" on page 328.

The switching procedures for Solaris SPARC vary, depending on whether VxVM encapsulates the root disk.

**To switch the boot environment if the root disk is not encapsulated**

1 Display the status of Live Upgrade boot environments.

```
# lustatus

Boot Environment  Is       Active Active    Can    Copy
Name              Complete Now    On Reboot Delete Status
----------------  -------- ------ --------- ------ ------
source.2657       yes      yes    yes       no     -
dest.2657         yes      no     no        yes    -
```

In this example, the primary boot disk is currently (source.2657). You want to activate the alternate boot disk (dest.2657)

2 Unmount any file systems that are mounted on the alternate root disk (dest.2657).

```
# lufslist dest.2657

               boot environment name: dest.2657

Filesystem        fstype device size  Mounted on Mount Options
----------------- ------ ------------ ---------- -------------
/dev/dsk/c0t0d0s1 swap     4298342400 -          -
/dev/dsk/c0t0d0s0 ufs     15729328128 /          -
/dev/dsk/c0t0d0s5 ufs      8591474688 /var       -
/dev/dsk/c0t0d0s3 ufs      5371625472 /vxfs      -

# luumount dest.2657
```

3 Activate the Live Upgrade boot environment.

```
# luactivate dest.2657
```

4 Reboot the system.

```
# shutdown -g0 -i6 -y
```

The system automatically selects the boot environment entry that was activated.

**To switch the boot environment if the root disk is encapsulated**

1 Display the current boot disk device and device aliases

```
# eeprom
boot-device=vx-rootdg vx-int_disk
use-nvramrc?=true
nvramrc=devalias vx-int_disk /pci@1c,600000/scsi@2/disk@0,0:a
devalias vx-rootdg01 /pci@1c,600000/scsi@2/disk@1,0:a
```

2 Set the device from which to boot using the eeprom command. This example shows booting from the primary root disk.

```
# eeprom boot-device=vx-rootdg01
```

3 Reboot the system.

```
# shutdown -g0 -i6 -y
```

## Switching the boot environment for Solaris x86-64

You do not have to perform the following procedures to switch the boot environment when you use the `vxlufinish` scripts to process Live Upgrade. You must perform the following procedures when you perform a manual Live Upgrade.

Two different procedures exist to switch the boot environment, choose one of the following procedures based on the encapsulation of the root disk:

- See "To switch the boot environment if root disk is not encapsulated" on page 329.
- See "To switch the boot environment if root disk is encapsulated" on page 330.

**To switch the boot environment if root disk is not encapsulated**

1 Display the status of Live Upgrade boot environments.

```
# lustatus

Boot Environment Is       Active Active    Can    Copy
Name             Complete Now    On Reboot Delete Status
---------------- -------- ------ --------- ------ ------
source.2657      yes      yes    yes       no     -
dest.2657        yes      no     no        yes    -
```

In this example, the primary boot disk is currently (source.2657). You want to activate the alternate boot disk (dest.2657)

2 Unmount any file systems that are mounted on the alternate root disk (dest.2657).

```
# lufslist dest.2657

               boot environment name: dest.2657

Filesystem        fstype device size  Mounted on Mount Options
----------------- ------ ------------ ---------- --------------
/dev/dsk/c0t0d0s1 swap    4298342400  -          -
/dev/dsk/c0t0d0s0 ufs    15729328128  /          -
/dev/dsk/c0t0d0s5 ufs     8591474688  /var       -
/dev/dsk/c0t0d0s3 ufs     5371625472  /vxfs      -

# luumount dest.2657
```

3 Activate the Live Upgrade boot environment.

```
# luactivate dest.2657
```

4 Reboot the system.

```
# shutdown -g0 -i6 -y
```

When the system boots up, the GRUB menu displays the following entries for the Live Upgrade boot environments:

```
source.2657
dest.2657
```

The system automatically selects the boot environment entry that was activated.

**To switch the boot environment if root disk is encapsulated**

- If the root disk is encapsulated, for releases before Solaris 10 update 6 (2.10u6), you can use the `luactivate` method. For Solaris 10 update 6 and subsequent Solaris 10 updates, do one of the following:
  - Select the GRUB entry for the source boot environment or destination boot environment when the system is booted. You can also use the following procedure to manually set the default GRUB menu.lst entry to the source (PBE) or destination (ABE) grub entry:
  - If the system is booted from the alternate boot environment, perform the following steps to switch to the primary boot environment:

    ```
    # mkdir /priroot
    # mount rootpath /priroot
    # bootadm list-menu -R /priroot
    # bootadm list-menu
    # bootadm set-menu -R /priroot default=PBE_menu_entry
    # bootadm set-menu default=PBE_menu_entry
    # shutdown -g0 -i6 -y
    ```

    Where:
    ***rootpath*** is the path to the root device, such as `/dev/vx/dsk/rootdg/rootvol`
    ***priroot*** is the primary root device
    ***PBE_menu_entry*** is the number of the primary boot environment in the GRUB menu.
  - If the system is booted from the primary boot environment, perform the following steps to switch to the alternate boot environment:

    ```
    # bootadm list-menu
    # bootadm set-menu default=ABE_menu_entry
    ABE booting
    ```

Chapter 28

# Performing post-upgrade tasks

This chapter includes the following topics:


- Re-joining the backup boot disk group into the current disk group
- Reverting to the backup boot disk group after an unsuccessful upgrade


## Re-joining the backup boot disk group into the current disk group

Perform this procedure to rejoin the backup boot disk if you split the mirrored boot disk during upgrade. After a successful upgrade and reboot, you no longer need to keep the boot disk group backup.

See "Performing a rolling upgrade using the installer" on page 272.

**To re-join the backup boot disk group**

- Re-join the *backup_bootdg* disk group to the boot disk group.

  ```
  # /etc/vx/bin/vxrootadm -Y join backup_bootdg
  ```

  where the `-Y` option indicates a silent operation, and *backup_bootdg* is the name of the backup boot disk group that you created during the upgrade.

# Reverting to the backup boot disk group after an unsuccessful upgrade

Perform this procedure if your upgrade was unsuccessful and you split the mirrored boot disk to back it up during upgrade. You can revert to the backup that you created when you upgraded.

See "Performing a rolling upgrade using the installer" on page 272.

**To revert the backup boot disk group after an unsuccessful upgrade**

1. To determine the boot disk groups, look for the *rootvol* volume in the output of the `vxprint` command.

   ```
   # vxprint
   ```

2. Use the `vxdg` command to find the boot disk group where you are currently booted.

   ```
   # vxdg bootdg
   ```

3. Boot the operating system from the backup boot disk group.
4. Join the original boot disk group to the backup disk group.

   ```
   # /etc/vx/bin/vxrootadm -Y join original_bootdg
   ```

   where the `-Y` option indicates a silent operation, and *original_bootdg* is the boot disk group that you no longer need.

Section 8

# Post-installation tasks


- Chapter 29. Performing post-installation tasks
- Chapter 30. Verifying the SFCFSHA installation

Chapter 29

# Performing post-installation tasks

This chapter includes the following topics:


- Changing root user into root role
- About enabling LDAP authentication for clusters that run in secure mode
- Starting and stopping processes for the Veritas products


## Changing root user into root role

On Oracle Solaris 11, to perform installation, you need to create root user. This means that a local user cannot assume the root role. After installation, you may want to turn root user into root role for a local user, who can log in as root.

1. Log in as root user.
2. Change the root account into role:

```
# rolemod -K type=role root
# getent user_attr root

root::::type=role;auths=solaris.*;profiles=All;audit_flags=lo\
:no;lock_after_retries=no;min_label=admin_low;clearance=admin_high
```

3. Assign the root role to a local user who was unassigned the role:

```
# usermod -R root admin
```

For more information, see the Oracle documentation on Oracle Solaris 11 operating system.

# 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 OpenLDAP and Windows Active Directory.

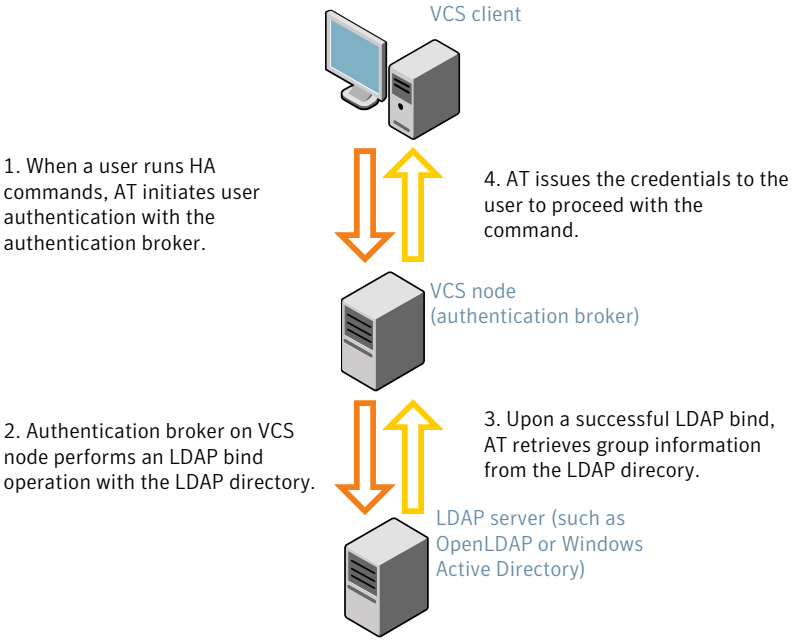
For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain.

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 29-1 depicts the SFCFSHA cluster communication with the LDAP servers when clusters run in secure mode.

**Figure 29-1** Client communication with LDAP servers




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 6.1.6.0 or later.

  ```
  # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showversion
  vssat version: 6.1.6.0
  ```

**To enable OpenLDAP 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/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
-d -s domain_controller_name_or_ipaddress -u domain_user

Attribute list file name not provided, using AttributeList.txt

Attribute file created.
```

You can use the `cat` command to view the entries in the attributes file.

2 Run the LDAP configuration tool `atldapconf` using the `-c` option. The `-c` option creates a CLI file to add the LDAP domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
-c -d windows_domain_name

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/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf -x

Using default broker port 2821

CLI file not provided, using default CLI.txt

Looking for AT installation...

AT found installed at ./vssat

Successfully added LDAP domain.
```

4 Check the AT version and list the LDAP domains to verify that the Windows Active Directory server integration is complete.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showversion

vssat version: 6.1.12.0

# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat listldapdomains

Domain Name : mydomain.com

Server URL : ldap://192.168.20.32:389

SSL Enabled : No

User Base DN : CN=people,DC=mydomain,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 Check the other domains in the cluster.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showdomains -p vx
```

The command output lists the number of domains that are found, with the domain names and domain types.

6 Generate credentials for the user.

```
# unset EAT_LOG

# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat authenticate \
-d ldap:windows_domain_name -p user_name -s user_password -b \
localhost:14149
```

7 Add non-root users as applicable.

```
# useradd user1

# passwd pw1

Changing password for "user1"

user1's New password:

Re-enter user1's new password:

# su user1

# bash

# id

uid=204(user1) gid=1(staff)

# pwd

# mkdir /home/user1

# chown user1 /home/ user1
```

8 Log in as non-root user and run `ha` commands as LDAP user.

```
# cd /home/user1

# ls

# cat .vcspwd

101 localhost mpise LDAP_SERVER ldap

# unset VCS_DOMAINTYPE

# unset VCS_DOMAIN

# /opt/VRTSvcs/bin/hasys -state

   #System        Attribute          Value

cluster1:sysA     SysState           FAULTED

cluster1:sysB     SysState           FAULTED

cluster2:sysC     SysState           RUNNING

cluster2:sysD     SysState           RUNNING
```

# Starting and stopping processes for the Veritas products

After the installation and configuration is complete, the Veritas product installer starts the processes that are used by the installed products. You can use the product installer to stop or start the processes, if required.

**To stop the processes**

- Use the `-stop` option to stop the product installation script.

  For example, to stop the product's processes, enter the following command:

  ```
  # ./installer -stop
  ```

  or

  ```
  # /opt/VRTS/install/installsfcfsha<version> -stop
  ```

  Where *<version>* is the specific release version.

  See "About the Veritas installer" on page 44.

**To start the processes**

- Use the `-start` option to start the product installation script.

  For example, to start the product's processes, enter the following command:

  ```
  # ./installer -start
  ```

  or

  ```
  # /opt/VRTS/install/installsfcfsha<version> -start
  ```

  Where `<version>` is the specific release version.

  See "About the Veritas installer" on page 44.

Chapter 30

# Verifying the SFCFSHA installation

This chapter includes the following topics:


- Performing a postcheck on a node
- Verifying that the products were installed
- Installation log files
- Checking Veritas Volume Manager processes
- Checking Veritas File System installation
- Verifying agent configuration for Storage Foundation Cluster File System High Availability
- Configuring VCS for Storage Foundation Cluster File System High Availability
- About the cluster UUID
- Verifying the LLT, GAB, and VCS configuration files
- Verifying LLT, GAB, and cluster operation


## Performing a postcheck on a node

The installer's `postcheck` command can help you to determine installation-related problems and provide troubleshooting information.

See “About using the postcheck option” on page 434.

**To run the postcheck command on a node**

1 Run the installer with the `-postcheck` option.

```
# ./installer -postcheck system_name
```

2 Review the output for installation-related information.

# Verifying that the products were installed

Verify that the SFCFSHA products are installed.

Use the pkginfo (Solaris 10) or pkg info (Solaris 11) command to check which packages have been installed.

Solaris 10:

```
# pkginfo -l VRTSvlic package_name package_name ...
```

Solaris 11:

```
# pkg info -| VRTSvlic package_name package_name
```

You can verify the version of the installed product. Use the following command:

```
# /opt/VRTS/install/installsfcfsha<version>
```

Where `<version>` is the specific release version.

See "About the Veritas installer" on page 44.

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.

# Checking Veritas Volume Manager processes

Use the following procedure to verify that Volume Manager processes are running.

**To confirm that key Volume Manager processes are running**

- Type the following command:

  ```
  # ps -ef | grep vx
  ```

  Entries for the `vxconfigd`, `vxnotify`, `vxesd`, `vxrelocd`, `vxcached`, and `vxconfigbackupd` processes should appear in the output from this command. If you disable hot-relocation, the `vxrelocd` and `vxnotify` processes are not displayed.

  For more details on hot relocation, see *Veritas Veritas Storage Foundation Cluster File System High Availability Administrator's Guide.*

# Checking Veritas File System installation

The Veritas File System package consists of a kernel component and administrative commands.

## Verifying Veritas File System kernel installation

To ensure that the file system driver is loaded, enter:

```
# modinfo | grep vxfs
```

The `modinfo` command displays information about all modules loaded on the system. If the `vxfs` module is loaded, you will see an entry corresponding to `vxfs`. If not,

follow the instructions load and then unload the file system module to complete the process.

See "Loading and unloading the file system module" on page 219.

## Verifying command installation

Table 30-1 lists the directories with Veritas File System commands.

**Table 30-1** VxFS command locations

| Location | Contents |
|---|---|
| `/etc/fs/vxfs` | Contains the Veritas `mount` command and QuickLog commands required to mount file systems. |
| `/usr/lib/fs/vxfs/bin` | Contains the VxFS type-specific switch-out commands. |
| `/opt/VRTSvxfs/sbin` | Contains the Veritas-specific commands. |
| `/opt/VRTS/bin` | Contains symbolic links to all Veritas-specific commands installed in the directories listed above. |

Determine whether these subdirectories are present:

```
# ls /etc/fs/vxfs
# ls /usr/lib/fs/vxfs/bin
# ls /opt/VRTSvxfs/sbin
# ls /opt/VRTS/bin
```

Make sure you have adjusted the environment variables accordingly.

See "Setting environment variables" on page 63.

# Verifying agent configuration for Storage Foundation Cluster File System High Availability

This section describes how to verify the agent configuration.

**To verify the agent configuration**

- Enter the cluster status command from any node in the cluster:

```
# cfscluster status
```

Output resembles:

```
Node             :  system01
Cluster Manager  :  running
CVM state        :  running
No mount point registered with cluster configuration

Node             :  system02
Cluster Manager  :  running
CVM state        :  running
No mount point registered with cluster configuration
```

# Configuring VCS for Storage Foundation Cluster File System High Availability

Configuring VCS means conveying to the VCS engine the definitions of the cluster, service groups, resources, and resource dependencies. VCS uses two configuration files in a default configuration:

- The `main.cf` file defines the entire cluster.
- The `types.cf` file defines the resource types.

By default, both files reside in the directory `/etc/VRTSvcs/conf/config`. Additional files similar to `types.cf` may be present if agents have been added, such as `OracleTypes.cf`.

In a VCS cluster, the first system to be brought online reads the configuration file and creates an internal (in-memory) representation of the configuration. Systems brought online after the first system derive their information from systems running in the cluster. You must stop the cluster while you are modifying the files from the command line. Changes made by editing the configuration files take effect when the cluster is restarted. The node on which the changes were made should be the first node to be brought back online.

## main.cf file

The VCS configuration file `main.cf` is created during the installation procedure. After installation, the `main.cf` file contains the base definitions of the cluster and

its nodes. Additionally, the file `types.cf` listed in the include statement defines the bundled agents for VCS resources.

See the *Veritas Cluster Server User's Guide*.

A typical VCS configuration file for SFCFSHA file resembles:

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleASMTypes.cf"
include "Db2udbTypes.cf"
include "OracleTypes.cf"
include "SybaseTypes.cf"

cluster sfcfs_1 (
        HacliUserLevel = COMMANDROOT
        )

system thor150 (
        )

system thor151 (
        )

group cvm (
        SystemList = { thor150 = 0, thor151 = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { thor150, thor151 }
        )
CFSfsckd vxfsckd (
        )
        CVMCluster cvm_clus (
                CVMClustName = sfcfs_1
                CVMNodeId = { thor150 = 0, thor151 = 1 }
                CVMTransport = gab
                CVMTimeout = 200
                )

        CVMVxconfigd cvm_vxconfigd (
                Critical = 0
                CVMVxconfigdArgs = { syslog }
                )
```

```
cvm_clus requires cvm_vxconfigd
vxfsckd requires cvm_clus

// resource dependency tree
//
//      group cvm
//      {
//      CVMCluster cvm_clus
//          {
//          CVMVxconfigd cvm_vxconfigd
//          }
//      }
```

## Storage Foundation Cluster File System HA Only

If you configured VCS Cluster Manager (Web Console), a service group, "ClusterService," was created that includes IP, Process, and Notifier resources. These resources were configured according to information you provided during the installation procedure. A resource dependency was also created.

## Veritas Cluster Server application failover services

If you installed SFCFS HA, you can begin implementing the application monitoring failover services provided by the Veritas Cluster Server. Information about setting up VCS services is beyond the scope of this document.

See the *Veritas Cluster Server* documentation.

## Configuring the cluster UUID when creating a cluster manually

You need to configure the cluster UUID when you manually create a cluster.

**To configure the cluster UUID when you create a cluster manually**

- On one node in the cluster, perform the following command to populate the cluster UUID on each node in the cluster.

  ```
  # /opt/VRTSvcs/bin/uuidconfig.pl -clus -configure nodeA
        nodeB ... nodeN
  ```

  Where *nodeA*, *nodeB*, through *nodeN* are the names of the cluster nodes.

# About the cluster UUID

You can verify the existence of the cluster UUID.

**To verify the cluster UUID exists**

- From the prompt, run a cat command.

```
cat /etc/vx/.uuids/clusuuid
```

# 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/lltab
   - 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 449.

# 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 351.
4. Verify GAB operation.

   See "Verifying GAB" on page 353.

5 Verify the cluster operation.

See "Verifying the cluster" on page 355.

# 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 sys1.

2 Run the `lltstat` command on the node sys1 to view the status of LLT.

```
lltstat -n
```

The output on sys1 resembles:

```
LLT node information:
    Node             State           Links
    *0 sys1          OPEN           2
     1 sys2          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 sys1             OPEN       2
     1 sys2             OPEN       2
     2 sys5             OPEN       1
```

3 Log in as superuser on the node sys2.

4 Run the `lltstat` command on the node sys2 to view the status of LLT.

```
lltstat -n
```

The output on sys2 resembles:

```
LLT node information:
    Node             State           Links
     0 sys1          OPEN            2
    *1 sys2          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 sys1 in a two-node cluster:

```
lltstat -nvv active
```

The output on sys1 resembles the following:

- For Solaris SPARC:

```
Node          State      Link    Status      Address
*0 sys1       OPEN
                         bge1 UP      08:00:20:93:0E:34
                         bge2 UP      08:00:20:93:0E:38
1 sys2        OPEN
                         bge1 UP      08:00:20:8F:D1:F2
                         bge2 DOWN
```

- For Solaris x64:

```
Node          State      Link    Status      Address
*0 sys1       OPEN
                         e1000g:1 UP      08:00:20:93:0E:34
                         e1000g:2 UP      08:00:20:93:0E:38
1 sys2        OPEN
                         e1000g:1 UP      08:00:20:8F:D1:F2
                         e1000g:2 DOWN
```

The command reports the status on the two active nodes in the cluster, sys1 and sys2.

For each correctly configured node, the information must show the following:

- A state of OPEN
- A status for each link of UP
- An address for each link

However, the output in the example shows different details for the node sys2. 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 sys1 in a two-node cluster:

```
lltstat -p
```

The output resembles:

```
LLT port information:
  Port  Usage       Cookie
  0     gab          0x0
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
  7     gab          0x7
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
  31    gab          0x1F
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
```

# Verifying GAB

Verify the GAB operation using the `gabconfig -a` command. This command returns the GAB port membership information.

The ports indicate the following:

| | |
|---|---|
| a | GAB |
| b | I/O fencing |
| d | Oracle Disk Manager (ODM) |
| f | Cluster File System (CFS) |
| h | Veritas Cluster Server (VCS: High Availability Daemon) |
| u | Cluster Volume Manager (CVM)<br>(to ship commands from slave node to master node)<br>Port u in the `gabconfig` output is visible with CVM protocol version >= 100. |

| | |
|---|---|
| v | Cluster Volume Manager (CVM) |
| w | vxconfigd (module for CVM) |
| y | Cluster Volume Manager (CVM) I/O shipping |

For more information on GAB, refer to the *Veritas Cluster Server Administrator's Guide*.

**To verify GAB**

1 To verify that GAB operates, type the following command on each node:

```
/sbin/gabconfig -a
```

2 Review the output of the command:

- If GAB operates, the following GAB port membership information is returned:

```
GAB Port Memberships
===================================
Port a gen  ada401 membership 01
Port b gen  ada40d membership 01
Port d gen  ada409 membership 01
Port f gen  ada41c membership 01
Port h gen  ada40f membership 01
Port o gen  ada406 membership 01
Port u gen  ada41a membership 01
Port v gen  ada416 membership 01
Port w gen  ada418 membership 01
Port y gen  ada42a membership 0
```

  Note that port b in the `gabconfig` command output may not indicate that I/O fencing feature is configured. After you configure SFCFSHA using the installer, the installer starts I/O fencing in disabled mode. You can use the `vxfenadm -d` command to verify the I/O fencing configuration.

- If GAB does not operate, the command does not return any GAB port membership information:

```
GAB Port Memberships
===================================
```

# Verifying the cluster

Verify the status of the cluster using the `hastatus` command. This command returns the system state and the group state.

Refer to the `hastatus(1M)` manual page.

Refer to the *Veritas Cluster Server Administrator's Guide* for a description of system states and the transitions between them.

**To verify the cluster**

1 To verify the status of the cluster, type the following command:

```
# hastatus -summary
```

The output resembles:

```
-- SYSTEM STATE
-- System               State                Frozen

A  sys1                 RUNNING              0
A  sys2                 RUNNING              0

-- GROUP STATE
-- Group           System        Probed  AutoDisabled   State

B  cvm             sys1          Y       N              ONLINE
B  cvm             sys2          Y       N              ONLINE
```

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 sys1. The list continues with similar information for sys2 (not shown) and any other nodes in the cluster.

---

**Note:** The following example is for SPARC. x64 clusters have different command output.

---

```
#System    Attribute             Value

sys1       AgentsStopped         0

sys1       AvailableCapacity     100

sys1       CPUBinding            BindTo None CPUNumber 0

sys1       CPUUsage              0

sys1       CPUUsageMonitoring    Enabled 0 ActionThreshold 0
                                 ActionTimeLimit 0 Action NONE
                                 NotifyThreshold 0 NotifyTimeLimit 0

sys1       Capacity              100

sys1       ConfigBlockCount      130

sys1       ConfigCheckSum        46688

sys1       ConfigDiskState       CURRENT

sys1       ConfigFile            /etc/VRTSvcs/conf/config

sys1       ConfigInfoCnt         0

sys1       ConfigModDate         Wed 14 Oct 2009 17:22:48

sys1       ConnectorState        Down

sys1       CurrentLimits

sys1       DiskHbStatus

sys1       DynamicLoad           0

sys1       EngineRestarted       0

sys1       EngineVersion         5.1.00.0
```

```
#System    Attribute             Value

sys1       Frozen                0

sys1       GUIIPAddr

sys1       HostUtilization       CPU 0 Swap 0

sys1       LLTNodeId             0

sys1       LicenseType           DEMO

sys1       Limits

sys1       LinkHbStatus

sys1       LoadTimeCounter       0

sys1       LoadTimeThreshold     600

sys1       LoadWarningLevel      80

sys1       NoAutoDisable         0

sys1       NodeId                0

sys1       OnGrpCnt              1

sys1       ShutdownTimeout

sys1       SourceFile            ./main.cf

sys1       SysInfo               Solaris:sys1,Generic_
                                 118558-11,5.9,sun4u

sys1       SysName               sys1

sys1       SysState              RUNNING

sys1       SystemLocation

sys1       SystemOwner

sys1       TFrozen               0

sys1       TRSE                  0

sys1       UpDownState           Up

sys1       UserInt               0

sys1       UserStr
```

```
#System    Attribute             Value

sys1       VCSFeatures           DR

sys1       VCSMode               VCS_CFS_VRTS
```

Section 9

# Configuration of disaster recovery environments


- Chapter 31. Configuring disaster recovery environments

Chapter 31

# Configuring disaster recovery environments

This chapter includes the following topics:


- Disaster recovery options for SFCFSHA
- About setting up a campus cluster for disaster recovery
- About setting up a global cluster environment for SFCFSHA
- About configuring a parallel global cluster using Veritas Volume Replicator (VVR) for replication


## Disaster recovery options for SFCFSHA

SFCFSHA supports configuring a disaster recovery environment using:

- Campus cluster
- Global clustering option (GCO) with replication
- Global clustering using Veritas Volume Replicator (VVR) for replication

For more about planning for disaster recovery environments:

You can install and configure clusters for your disaster recovery environment as you would for any cluster using the procedures in this installation guide.

For a high level description of the tasks for implementing disaster recovery environments:

See “About setting up a campus cluster for disaster recovery” on page 361.

See “About setting up a global cluster environment for SFCFSHA” on page 363.

See "About configuring a parallel global cluster using Veritas Volume Replicator (VVR) for replication" on page 364.

For complete details for configuring your disaster recovery environment once clusters are installed and configured:

See the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide*.

# About setting up a campus cluster for disaster recovery

Campus clusters:

- Are connected using a high speed cable that guarantees network access between the nodes
- Provide local high availability and disaster recovery functionality in a single cluster
- Employ shared disk groups mirrored across sites with Veritas Volume Manager (VxVM)
- Are supported by Veritas Storage Foundation Cluster File System High Availability (SFCFSHA)

The following high-level tasks illustrate the setup steps for a campus cluster in a parallel cluster database environment. The example values are given for SF for Oracle RAC and should be adapted for an SFCFS HA cluster using another database application.

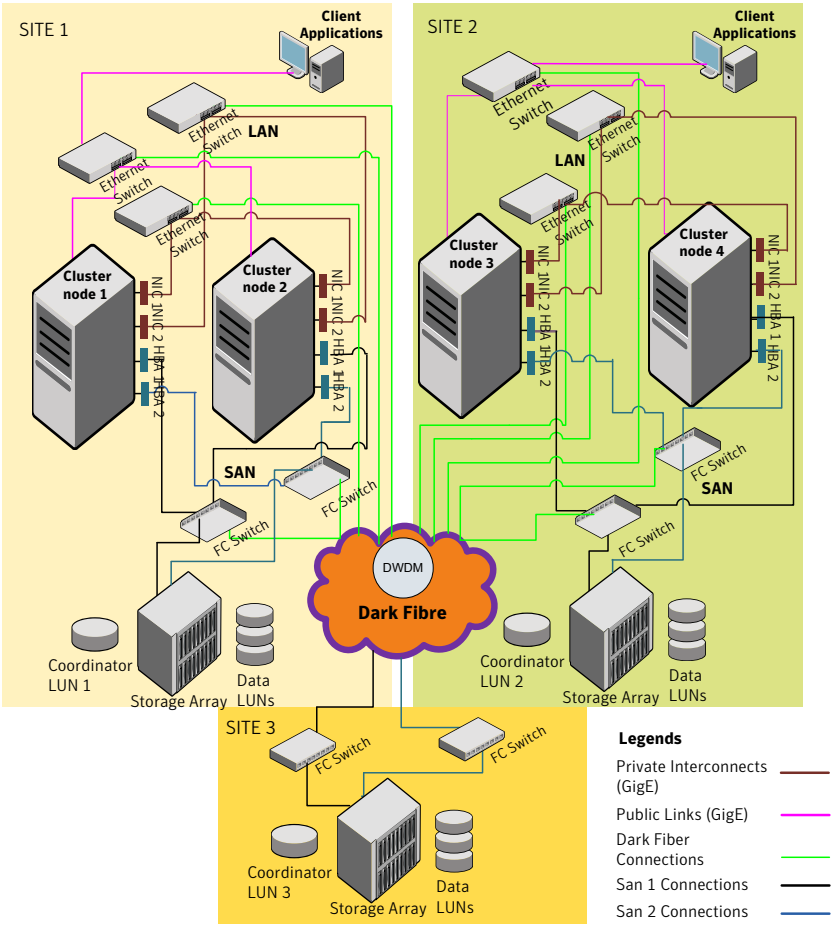
**Table 31-1** Tasks for setting up a parallel campus cluster for disaster recovery

| Task | Description |
|---|---|
| Prepare to set up campus cluster configuration | See the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Implementations Guide*. |
| Configure I/O fencing to prevent data corruption | See the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Implementations Guide*. |
| Prepare to install Oracle RAC Clusterware and database binaries | See the *Veritas Storage Foundation for Oracle RAC Installation and Configuration Guide*. |
| Prepare to install your database software. | See your database documentation. |

**Table 31-1** Tasks for setting up a parallel campus cluster for disaster recovery *(continued)*

| Task | Description |
|---|---|
| Configure VxVM disk groups for campus cluster | See the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Implementations Guide*. |
| Install Oracle RAC Clusterware and database binaries | For Oracle RAC, see the *Veritas Storage Foundation for Oracle RAC Installation and Configuration Guide*.<br>For SFCFS HA, see your database documentation. |
| Install your database software. | See your database documentation. |
| Configure VCS service groups | See the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Implementations Guide*. |

**Figure 31-1** Sample SF Oracle RAC configuration




Although a Coordination Point (CP) server is not used in the current example, it can also be used instead of a third site for a coordinator disk.

# About setting up a global cluster environment for SFCFSHA

Configuring a global cluster for environment with parallel clusters requires the coordination of many component setup tasks. The procedures provided here are guidelines. You will need this guide to install and configure SFCFSHA on each

cluster. Refer to the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Guide* to configure a global cluster environment and replication between the two clusters.

- Configure a SFCFSHA cluster at the primary site
- Configure an SFCFSHA cluster at the secondary site
- Configure a global cluster environment
- Test the HA/DR configuration

Upon successful testing, you can bring the environment into production

For global cluster configuration details:

See the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Guide*.

# About configuring a parallel global cluster using Veritas Volume Replicator (VVR) for replication

Configuring a global cluster for environment with SFCFSHA and Veritas Volume Replicator requires the coordination of many component setup tasks. The tasks listed below are guidelines.

Before configuring two clusters for global clustering, you must verify that:

- You have the correct installation options enabled for SFCFSHA, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster and VVR enabled.
  Review SFCFSHA requirements and licensing information.
- Both clusters have SFCFSHA software installed and configured.

---

**Note:** You can install and configure both clusters at the same time, or you can configure the second cluster at a later time than the first.

---

You can use this guide to install and configure SFCFSHA on each cluster. For details for configuring a global cluster environment and replication between the the clusters using VVR:

See the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide*.

With two clusters installed and configured , you are ready to configure a global cluster environment using VVR. You must perform the following tasks to modify both cluster configurations to support replication in the global cluster environment.

**Table 31-2** Tasks for configuring a parallel global cluster with VVR

| Task | Description |
|---|---|
| Setting up replication on the primary site | ■ Create the Storage Replicator Log (SRL) in the disk group for the database.<br>■ Create the Replicated Volume Group (RVG) on the primary site. |
| Setting up replication on the secondary site | ■ Create a disk group to hold the data volume, SRL, and RVG on the storage on the secondary site. You must match the names and sizes of these volumes with the names and sizes of the volumes on the primary site.<br>■ Edit the /etc/vx/vras/.rdg file on the secondary site.<br>■ Use resolvable virtual IP addresses that set network RLINK connections as host names of the primary and secondary sites.<br>■ Create the replication objects on the secondary site. |
| Starting replication of the database. | You can use either of the following methods to start replication:<br>■ Automatic synchronization<br>■ Full synchronization with Storage Checkpoint |
| Configuring VCS for replication on clusters at both sites. | Configure Veritas Cluster Server (VCS) to provide high availability for the database:<br>■ Modify the VCS configuration on the primary site<br>■ Modify the VCS configuration on the secondary site |

Once the global clusters and replication with VVR are configured, the following replication use cases are supported for it:

- Migration of the role of the primary site to the remote site
- Takeover of the primary site role by the secondary site
- Migrate the role of primary site to the secondary site
- Migrate the role of new primary site back to the original primary site
- Take over after an outage
- Resynchronize after an outage
- Update the rlink to reflect changes

For details on the replication use cases:

See the *Veritas Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide*.

Section 10

# Uninstallation of SFCFSHA


- Chapter 32. Uninstalling Storage Foundation Cluster File System High Availability
- Chapter 33. Uninstalling using response files

Chapter 32

# Uninstalling Storage Foundation Cluster File System High Availability

This chapter includes the following topics:


- About removing Veritas Storage Foundation Cluster File System High Availability
- Shutting down cluster operations
- Disabling the agents on a system
- Removing the Replicated Data Set
- Uninstalling SFCFSHA packages using the script-based installer
- Uninstalling SFCFSHA with the Veritas Web-based installer
- Uninstalling Storage Foundation using the pkgrm command
- Removing the CP server configuration using the installer program
- Removing the Storage Foundation for Databases (SFDB) repository after removing the product


## About removing Veritas Storage Foundation Cluster File System High Availability

This section covers uninstallation requirements and steps to uninstall the Veritas software.

Only users with superuser privileges can uninstall Veritas Storage Foundation Cluster File System High Availability.

**Warning:** Failure to follow the instructions in the following sections may result in unexpected behavior.

# Preparing to uninstall

Review the following removing the Veritas software.

## Remote uninstallation

You must configure remote communication to uninstall SFCFSHA on remote systems. In a High Availability environment, you must meet the prerequisites to uninstall on all nodes in the cluster at one time.

The following prerequisites are required for remote uninstallation:

- Communication protocols must exist between systems.By default, the uninstall scripts use ssh.
- You must be able to execute ssh or rsh commands as superuser on all systems.
- The ssh or rsh must be configured to operate without requests for passwords or passphrases.

See "About configuring secure shell or remote shell communication modes before installing products" on page 467.

## Preparing to remove Veritas Volume Manager

This section describes the steps you need to take before removing Veritas Volume Manager (VxVM) to preserve the contents of the volumes.

**Warning:** Failure to follow the preparations in this section might result in unexpected behavior.

### Moving volumes from an encapsulated root disk

Use the following procedure to move volumes from an encapsulated root disk.

**To uninstall VxVM if root, swap, usr, or var is a volume under Volume Manager control**

1 Ensure that the `rootvol`, `swapvol`, `usr`, and `var` volumes have only one associated plex each.

The plex must be contiguous, non-striped, non-spanned, and non-sparse. To obtain this information, enter the following:

```
# vxprint -ht rootvol swapvol usr var
```

If any of these volumes have more than one associated plex, remove the unnecessary plexes using the following command:

```
# vxplex -o rm dis plex_name
```

2 Run the `vxunroot` command:

```
# /etc/vx/bin/vxunroot
```

The `vxunroot` command changes the volume entries in `/etc/vfstab` to the underlying disk partitions for `rootvol`, `swapvol`, `usr`, and `var`. It also modifies `/etc/system` and prompts for a reboot so that disk partitions are mounted instead of volumes for `root`, `swap`, `usr`, and `var`.

3 Once you have changed the `root`, `swap`, `usr`, and `var` volumes, move all remaining volumes to disk partitions.

You can do this using one of the following procedures:

- Back up the entire system to tape and then recover from tape.
- Back up each file system individually and then recover them all after creating new file systems on disk partitions.
- Move volumes incrementally to disk partitions.
  See "Moving volumes to disk partitions" on page 370.
  Otherwise, shut down VxVM.

### Moving volumes to disk partitions

Use the following procedure to move volumes incrementally to disk partitions.

**To move volumes incrementally to disk partitions**

1. Evacuate disks using `vxdiskadm`, the VOM GUI, or the `vxevac` utility.

   Evacuation moves subdisks from the specified disks to target disks. The evacuated disks provide the initial free disk space for volumes to be moved to disk partitions.

2. Remove the evacuated disks from VxVM control by entering:

   ```
   # vxdg rmdisk diskname
   # vxdisk rm devname
   ```

3. Decide which volume to move first, and if the volume is mounted, unmount it.

4. If the volume is being used as a raw partition for database applications, make sure that the application is not updating the volume and that you have applied the `sync` command to the data on the volume.

5. Create a partition on free disk space of the same size as the volume using the `format` command.

   If there is not enough free space for the partition, add a new disk to the system for the first volume removed. Subsequent volumes can use the free space generated by the removal of this first volume.

6. Copy the data on the volume onto the newly created disk partition using a command such as `dd`.

   ```
   # dd if=/dev/vx/dsk/diskgroup/lhome of=/dev/dsk/c2t2d2s7
   ```

   where `c2t2d2` is the disk outside of Volume Manager and `s7` is the newly created partition.

7. Replace the entry for that volume (if present) in `/etc/vfstab` with an entry for the newly created partition.

8. Mount the disk partition if the corresponding volume was previously mounted.

9. Stop and remove the volume from VxVM using the commands.

   ```
   # vxvol -g diskgroup stop volume_name
   # vxedit -rf rm volume_name
   ```

10 Remove any free disks (those having no subdisks defined on them) by removing the volumes from VxVM control.

To check if there are still some subdisks remaining on a particular disk, use the `vxprint` command.

```
# vxprint -g diskgroup -F '%sdnum' diskname
```

If the output is not 0, there are still some subdisks on this disk that you need to remove. If the output is 0, remove the disk from VxVM control.

```
# vxdg rmdisk diskname
# vxdisk rm devname
```

Use the free space created for adding the data from the next volume you want to remove.

11 After you successfully convert all volumes into disk partitions, reboot the system.

12 After the reboot, make sure none of the volumes are open by using the `vxprint` command.

```
# vxprint -Aht -e v_open
```

13 If any volumes remain open, repeat the steps listed above.

### Example of moving volumes to disk partitions on Solaris

This example shows how to move the data on a volume to a disk partition. In the example, there are three disks: `disk1` and `disk2` are subdisks on volume `vol01` and `disk3` is a free disk. The data on `vol01` is copied to `disk3` using `vxevac`.

These are the contents of the disk group `voldg` before the data on `vol01` is copied to `disk3`.

```
# vxprint -g voldg -ht
DG NAME   NCONFIG   NLOG     MINORS    GROUP-ID
DM NAME   DEVICE    TYPE     PRIVLEN   PUBLEN    STATE
RV NAME   RLINK_CNT KSTATE   STATE     PRIMARY   DATAVOLS  SRL
RL NAME   RVG       KSTATE   STATE     REM_HOST  REM_DG    REM_RLNK
V  NAME   RVG       KSTATE   STATE     LENGTH    READPOL   PREFPLEX UTYPE
PL NAME   VOLUME    KSTATE   STATE     LENGTH    LAYOUT    NCOL/WID MODE
SD NAME   PLEX      DISK     DISKOFFS  LENGTH    [COL/]OFF DEVICE   MODE
SV NAME   PLEX      VOLNAME  NVOLLAYR  LENGTH    [COL/]OFF AM/NM    MODE
DC NAME   PARENTVOL LOGVOL
SP NAME   SNAPVOL   DCO

dg voldg default   default 115000
```

```
1017856044.1141.hostname.veritas.com

dm disk1 c1t12d0s2 sliced  2591     17900352 -
dm disk2 c1t14d0s2 sliced  2591     17899056 -
dm disk3 c1t3d0s2  sliced  2591     17899056 -

v  vol1  -         ENABLED ACTIVE   4196448  ROUND     -        fsgen
pl pl1   vol1      ENABLED ACTIVE   4196448  CONCAT    -        RW
sd sd1   pl1       disk1   0        2098224  0         c1t12d0  ENA
sd sd2   pl1       disk2   0        2098224  2098224   c1t14d0  ENA
```

Evacuate `disk1` to `disk3`.

```
# /etc/vx/bin/vxevac -g voldg disk1 disk3
# vxprint -g voldg -ht

DG NAME  NCONFIG    NLOG     MINORS   GROUP-ID
DM NAME  DEVICE     TYPE     PRIVLEN  PUBLEN   STATE
RV NAME  RLINK_CNT  KSTATE   STATE    PRIMARY  DATAVOLS  SRL
RL NAME  RVG        KSTATE   STATE    REM_HOST REM_DG    REM_RLNK
V  NAME  RVG        KSTATE   STATE    LENGTH   READPOL   PREFPLEX  UTYPE
PL NAME  VOLUME     KSTATE   STATE    LENGTH   LAYOUT    NCOL/WID  MODE
SD NAME  PLEX       DISK     DISKOFFS LENGTH   [COL/]OFF DEVICE    MODE
SV NAME  PLEX       VOLNAME  NVOLLAYR LENGTH   [COL/]OFF AM/NM     MODE
DC NAME  PARENTVOL  LOGVOL
SP NAME  SNAPVOL    DCO

dg voldg default    default  115000
1017856044.1141.hostname.veritas.com

dm disk1 c1t12d0s2  sliced   2591     17900352 -
dm disk2 c1t14d0s2  sliced   2591     17899056 -
dm disk3 c1t3d0s2   sliced   2591     17899056 -

v  vol1  -          ENABLED  ACTIVE   4196448  ROUND     -         fsgen
pl pl1   vol1       ENABLED  ACTIVE   4196448  CONCAT    -         RW
sd disk3-01l1       disk3    0        2098224  0         c1t3d0    ENA
sd sd2   pl1        disk2    0        2098224  2098224   c1t14d0   ENA
```

Evacuate `disk2` to `disk3`.

```
# /etc/vx/bin/vxevac -g voldg disk2 disk3
# vxprint -g voldg -ht
```

```
DG NAME     NCONFIG   NLOG    MINORS   GROUP-ID
DM NAME     DEVICE    TYPE    PRIVLEN  PUBLEN   STATE
RV NAME     RLINK_CNT KSTATE  STATE    PRIMARY  DATAVOLS  SRL
RL NAME     RVG       KSTATE  STATE    REM_HOST REM_DG    REM_RLNK
V  NAME     RVG       KSTATE  STATE    LENGTH   READPOL   PREFPLEX UTYPE
PL NAME     VOLUME    KSTATE  STATE    LENGTH   LAYOUT    NCOL/WID MODE
SD NAME     PLEX      DISK    DISKOFFS LENGTH   [COL/]OFF DEVICE   MODE
SV NAME     PLEX      VOLNAME NVOLLAYR LENGTH   [COL/]OFF AM/NM    MODE
DC NAME     PARENTVOL LOGVOL
SP NAME     SNAPVOL   DCO

dg voldg    default   default 115000
1017856044.1141.hostname.veritas.com

dm disk1    c1t12d0s2 sliced  2591    17900352 -
dm disk2    c1t14d0s2 sliced  2591    17899056 -
dm disk3    c1t3d0s2  sliced  2591    17899056 -

v  vol1     -         ENABLED ACTIVE  4196448  ROUND   -      fsgen
pl pl1      vol1      ENABLED ACTIVE  4196448  CONCAT  -      RW
sd disk3-01 pl1       disk3   0       2098224  0       c1t3d0 ENA
sd disk3-02 pl1       disk3   2098224 2098224  2098224 c1t3d0 ENA
```

Remove the evacuated disks from VxVM control.

```
# vxdisk -g voldg list
DEVICE      TYPE      DISK         GROUP        STATUS
c1t3d0s2    sliced    disk3        voldg        online
c1t12d0s2   sliced    disk1        voldg        online
c1t14d0s2   sliced    disk2        voldg        online

# vxdg rmdisk disk1
# vxdg rmdisk disk2
# vxdisk rm c1t12d0
# vxdisk rm c1t14d0
```

Verify that the evacuated disks have been removed from VxVM control.

```
# vxdisk -g voldg list
DEVICE       TYPE      DISK         GROUP        STATUS
c1t3d0s2     sliced    disk3        voldg        online
```

Check to see whether the volume you want to move first is mounted.

```
# mount | grep vol1
/vol1 on /dev/vx/dsk/voldg/vol1
read/write/setuid/log/nolargefiles/dev=12dc138 on Wed Apr
3 10:13:11 2002
```

Create a partition on free disk space of the same size as the volume. In this example, a 2G partition is created on `disk1` (`c1t12d0s1`).

```
# format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
     0. c0t0d0 <SUN9.0G cyl 4924 alt 2 hd 27 sec 133>
        /sbus@1f,0/SUNW,fas@e,8800000/sd@0,0
     1. c1t3d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@3,0
     2. c1t9d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@9,0
     3. c1t10d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@a,0
     4. c1t11d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@b,0
     5. c1t12d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@c,0
     6. c1t14d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@e,0
     7. c1t15d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@f,0
Specify disk (enter its number): 5
selecting c1t12d0
[disk formatted]

FORMAT MENU:
        disk       - select a disk
        type       - select (define) a disk type
        partition  - select (define) a partition table
        current    - describe the current disk
        format     - format and analyze the disk
        repair     - repair a defective sector
        label      - write label to the disk
        analyze    - surface analysis
        defect     - defect list management
        backup     - search for backup labels
        verify     - read and display labels
```

```
        save       - save new disk/partition definitions
        inquiry    - show vendor, product and revision
        volname    - set 8-character volume name
        !<cmd>     - execute <cmd>, then return
        quit
format> p

PARTITION MENU:
        0      - change '0' partition
        1      - change '1' partition
        2      - change '2' partition
        3      - change '3' partition
        4      - change '4' partition
        5      - change '5' partition
        6      - change '6' partition
        7      - change '7' partition
        select - select a predefined table
        modify - modify a predefined partition table
        name   - name the current table
        print  - display the current table
        label  - write partition map and label to the disk
        !<cmd> - execute <cmd>, then return
        quit
partition> 1
Part      Tag    Flag    Cylinders     Size          Blocks
  1 unassigned    wm      0            0       (0/0/0)            0
Enter partition id tag[unassigned]:
Enter partition permission flags[wm]:
Enter new starting cyl[0]:
Enter partition size[0b, 0c, 0.00mb, 0.00gb]: 2.00gb
partition> l
Ready to label disk, continue? y

partition> p
Current partition table (unnamed):
Total disk cylinders available: 13814 + 2 (reserved cylinders)
Part      Tag    Flag    Cylinders     Size          Blocks
  0 unassigned    wm      0            0       (0/0/0)            0
  1 unassigned    wm      0 -  3236    2.00GB  (3237/0/0)   4195152
partition> q
```

Copy the data on `vol01` to the newly created disk partition.

```
# dd if=/dev/vx/dsk/voldg/vol01 of=/dev/dsk/c1t12d0s1
```

In the `/etc/vfstab` file, remove the following entry.

```
/dev/vx/dsk/voldg/vol1 /dev/vx/rdsk/voldg/vol1 /vol1 vxfs 4 yes rw
```

Replace it with an entry for the newly created partition.

```
/dev/dsk/c1t12d0s1 /dev/rdsk/c1t12d0s1 /vol01 vxfs 4  yes rw
```

Mount the disk partition.

```
# mount -F vxfs /dev/dsk/c1t12d0s1 /vol01
```

Remove `vol01` from VxVM.

```
# vxedit -rf rm /dev/vx/dsk/voldg/vol01
```

To complete the procedure, follow the remaining steps.

## Preparing to remove Veritas File System

The `VRTSvxfs` package cannot be removed if there are any mounted VxFS file systems or Storage Checkpoints. Unmount the VxFS file systems and Storage Checkpoints before uninstalling Veritas Storage Foundation. After you remove the `VRTSvxfs` package, VxFS file systems are not mountable or accessible until another `VRTSvxfs` package is installed.

### To unmount a file system

1 Check if any VxFS file systems are mounted.

```
# cat /etc/mnttab | grep vxfs
```

2 Unmount any file systems.

```
# umount special | mount_point
```

Specify the file system to be unmounted as a *mount_point* or *special* (the device on which the file system resides). See the `umount_vxfs`(1M) manual page for more information about this command and its available options.

You can use the `-a` option to unmount all file systems except `/`, `/usr`, `/usr/kvm`, `/var`, `/proc`, `/dev/fd`, and `/tmp`.

**To unmount a Storage Checkpoint**

1 Check if any Storage Checkpoints are mounted.

```
# cat /etc/mnttab | grep vxfs
```

2 Unmount any Storage Checkpoints.

```
# umount /checkpoint_name
```

# Shutting down cluster operations

If the systems are running as an HA cluster, you have to take all service groups offline and shutdown VCS.

**To take all service groups offline and shutdown VCS**

- Use the `hastop` command as follows:

```
# /opt/VRTSvcs/bin/hastop -all
```

**Warning:** Do not use the `-force` option when executing `hastop`. This will leave all service groups online and shut down VCS, causing undesired results during uninstallation of the packages.

# Disabling the agents on a system

This section explains how to disable a VCS agent for VVR on a system. To disable an agent, you must change the service group containing the resource type of the agent to an OFFLINE state. Then, you can stop the application or switch the application to another system.

**To disable the agents**

1. Check whether any service group containing the resource type of the agent is online by typing the following command:

   ```
   # hagrp -state service_group -sys system_name
   ```

   If none of the service groups is online, skip to 3.

2. If the service group is online, take it offline.

   To take the service group offline without bringing it online on any other system in the cluster, enter:

   ```
   # hagrp -offline service_group -sys system_name
   ```

3. Stop the agent on the system by entering:

   ```
   # haagent -stop agent_name -sys system_name
   ```

   When you get the message `Please look for messages in the log file`, check the file `/var/VRTSvcs/log/engine_A.log` for a message confirming that each agent has stopped.

   You can also use the `ps` command to confirm that the agent is stopped.

4. Remove the system from the `SystemList` of the service group. If you disable the agent on all the systems in the `SystemList`, you can also remove the service groups and resource types from the VCS configuration.

   Read information on administering VCS from the command line.

   Refer to the *Veritas Cluster Server User's Guide*.

# Removing the Replicated Data Set

If you use VVR, you need to perform the following steps. This section gives the steps to remove a Replicated Data Set (RDS) when the application is either active or stopped.

**To remove the Replicated Data Set**

1 Verify that all RLINKs are up-to-date:

```
# vxrlink -g diskgroup status rlink_name
```

If the Secondary is not required to be up-to-date, proceed to 2 and stop replication using the `-f` option with the `vradmin stoprep` command.

2 Stop replication to the Secondary by issuing the following command on any host in the RDS:

The `vradmin stoprep` command fails if the Primary and Secondary RLINKs are not up-to-date. Use the `-f` option to stop replication to a Secondary even when the RLINKs are not up-to-date.

```
# vradmin -g diskgroup stoprep local_rvgname sec_hostname
```

The argument `local_rvgname` is the name of the RVG on the local host and represents its RDS.

The argument `sec_hostname` is the name of the Secondary host as displayed in the output of the `vradmin printrvg` command.

3 Remove the Secondary from the RDS by issuing the following command on any host in the RDS:

```
# vradmin -g diskgroup delsec local_rvgname sec_hostname
```

The argument local_rvgname is the name of the RVG on the local host and represents its RDS.

The argument sec_hostname is the name of the Secondary host as displayed in the output of the `vradmin printrvg` command.

4 Remove the Primary from the RDS by issuing the following command on the Primary:

```
# vradmin -g diskgroup delpri local_rvgname
```

When used with the `-f` option, the `vradmin delpri` command removes the Primary even when the application is running on the Primary.

The RDS is removed.

5 If you want to delete the SRLs from the Primary and Secondary hosts in the RDS, issue the following command on the Primary and all Secondaries:

```
# vxedit -r -g diskgroup rm srl_name
```

# Uninstalling SFCFSHA packages using the script-based installer

Use the following procedure to remove SFCFSHA products.

Not all packages may be installed on your system depending on the choices that you made when you installed the software.

---

**Note:** After you uninstall the product, you cannot access any file systems you created using the default disk layout version in SFCFSHA 6.0.1 with a previous version of SFCFSHA.

---

Language packages are uninstalled when you uninstall the English language packages.

**To shut down and remove the installed SFCFSHA packages**

1. Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/vfstab`. Failing to remove these entries could result in system boot problems later.
2. Unmount all mount points for VxFS file systems.

   ```
   # umount /mount_point
   ```

3. If the VxVM package (`VRTSvxvm`) is installed, read and follow the uninstallation procedures for VxVM.

   See "Preparing to remove Veritas Volume Manager" on page 369.
4. Make sure you have performed all of the prerequisite steps.
5. 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
   ```

6. Move to the `/opt/VRTS/install` directory and run the uninstall script.

   ```
   # cd /opt/VRTS/install

   # ./uninstallsfcfsha<version>
   ```

Where *<version>* is the specific release version.

Or, if you are using ssh or rsh, use one of the following:

- `# ./uninstallsfcfsha<version> -rsh`
- `# ./uninstallsfcfsha<version> -ssh`

See "About the Veritas installer" on page 44.

7 The uninstall script prompts for the system name. Enter one or more system names, separated by a space, from which to uninstall SFCFSHA, for example, `sys1`:

```
Enter the system names separated by spaces: [q?] sys1 sys2
```

8 The uninstall script prompts you to stop the product processes. If you respond yes, the processes are stopped and the packages are uninstalled.

The uninstall script creates log files and displays the location of the log files.

9 Most packages have kernel components. In order to ensure complete removal, a system reboot is recommended after all packages have been removed.

10 To verify the removal of the packages, use the `pkginfo` command.

```
# pkginfo | grep VRTS
```

# Uninstalling SFCFSHA with the Veritas Web-based installer

This section describes how to uninstall using the Veritas Web-based installer.

**Note:** After you uninstall the product, you cannot access any file systems you created using the default disk layout Version in SFCFSHA 6.0.1 with a previous version of SFCFSHA.

### To uninstall SFCFSHA

1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 144.

3 On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.

4 Select **Storage Foundation Cluster File System High Availability** from the Product drop-down list, and click **Next**.

5 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Next**.

6 After the validation completes successfully, click **Next** to uninstall SFCFSHA on the selected system.

7 If there are any processes running on the target system, the installer stops the processes. Click **Next**.

8 After the installer stops the processes, the installer removes the products from the specified system.

Click **Next**.

9 After the uninstall completes, the installer displays the location of the summary, response, and log files. If required, view the files to confirm the status of the removal.

10 Click **Finish**.

Most packages have kernel components. In order to ensure their complete removal, a system reboot is recommended after all the packages have been removed.

# Uninstalling Storage Foundation using the pkgrm command

Use the following procedure to uninstall Storage Foundation using the pkgrm command.

If you are uninstalling Veritas Storage Foundation using the pkgrm command, the packages must be removed in a specific order, or else the uninstallation will fail. Removing the packages out of order will result in some errors, including possible core dumps, although the packages will still be removed.

**To uninstall Storage Foundation**

1. Unmount all VxFS file systems and Storage Checkpoints, and close all VxVM volumes.

   Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/vfstab`. Failing to remove these entries could result in system boot problems later.

2. Unmount all mount points for VxFS file systems and Storage Checkpoints.

   ```
   # umount /mount_point
   ```

3. Stop all applications from accessing VxVM volumes, and close all VxVM volumes.

4. Stop various daemons, if applicable.

   ```
   # /opt/VRTS/bin/vxsvcctrl stop
   ```

5. Remove the packages in the following order:

   Solaris 10:

   ```
   # # pkgrm VRTSodm VRTSgms VRTScavf VRTSglm VRTSdbed \
   VRTSvcsea VRTSvcsag VRTScps VRTSvcs VRTSamf \
   VRTSvxfen VRTSgab VRTSllt VRTSfssdk VRTSfsadv \
   VRTSvxfs VRTSsfmh VRTSob VRTSaslapm VRTSvxvm \
   VRTSspt VRTSsfcpi60 VRTSperl VRTSvlic
   ```

   Solaris 11:

   ```
   # pkg uninstall VRTSodm VRTSgms VRTScavf VRTSglm VRTSdbed \
   VRTSvcsea VRTSvcsag VRTScps VRTSvcs VRTSamf \
   VRTSvxfen VRTSgab VRTSllt VRTSfssdk VRTSfsadv \
   VRTSvxfs VRTSsfmh VRTSob VRTSaslapm VRTSvxvm \
   VRTSspt VRTSsfcpi60 VRTSperl VRTSvlic
   ```

# Uninstalling the language packages using the pkgrm command

If you would like to remove only the language packages, you can do so with the `pkgrm` command.

If you use the product installer menu or the uninstallation script, you can remove the language packages along with the English packages.

**To remove the language packages**

- Use the `pkgrm` command to remove the appropriate packages.

  See "Chinese language packages" on page 479.

  See "Japanese language packages" on page 480.

  ```
  # pkgrm package_name package_name ...
  ```

  Because the packages do not contain any dependencies, you can remove them in any order.

# Removing the CP server configuration using the installer program

This section describes how to remove the CP server configuration from a node or a cluster that hosts the CP server.

---

**Warning:** Ensure that no SFCFSHA cluster (application cluster) uses the CP server that you want to unconfigure.

---

**To remove the CP server configuration**

1 To run the configuration removal script, enter the following command on the node where you want to remove the CP server configuration:

```
root@cps1.symantecexample.com
# /opt/VRTS/install/installvcsversion  -configcps
```

2 Select option 3 from the menu to unconfigure the CP server.

```
VERITAS COORDINATION POINT SERVER CONFIGURATION UTILITY
=======================================================

Select one of the following:

[1] Configure Coordination Point Server on single node VCS system

[2] Configure Coordination Point Server on SFHA cluster

[3] Unconfigure Coordination Point Server
```

3 Review the warning message and confirm that you want to unconfigure the CP server.

```
WARNING: Unconfiguring Coordination Point Server stops the
vxcpserv process. VCS clusters using this server for
coordination purpose will have one less coordination point.

Are you sure you want to bring down the cp server? (y/n)
(Default:n) :y
```

4 Review the screen output as the script performs the following steps to remove the CP server configuration:

- Stops the CP server
- Removes the CP server from VCS configuration
- Removes resource dependencies
- Takes the the CP server service group (CPSSG) offline, if it is online
- Removes the CPSSG service group from the VCS configuration
- Successfully unconfigured the Veritas Coordination Point Server

```
The CP server database is not being deleted on the shared storage.
It can be re-used if CP server is reconfigured on the cluster.
The same database location can be specified during CP server
configuration.
```

5 Decide if you want to delete the CP server configuration file.

```
Do you want to delete the CP Server configuration file
(/etc/vxcps.conf) and log files
(in /var/VRTScps)? [y,n,q] (n) y

Deleting /etc/vxcps.conf and log files on sys1.... Done
Deleting /etc/vxcps.conf and log files on sys2... Done
```

6 Confirm if you want to send information about this installation to Symantec to help improve installation in the future.

```
Would you like to send the information about this installation
to Symantec to help improve installation in the future? [y,n,q,?] (y)
```

Upload completed successfully.

# 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 disables the SFDB tools.

**To remove the SFDB repository**

1 Identify the SFDB repositories created on the host.

```
# cat /var/vx/vxdba/rep_loc
```

Oracle:

```
{
   "sfae_rept_version" : 1,
   "oracle" : {
      "SFAEDB" : {
         "location" : "/data/sfaedb/.sfae",
         "old_location" : "",
         "alias" : [
            "sfaedb"
         ]
      }
   }
}
```

DB2:

```
{
  "db2" : {
     "db2inst1_sfaedb2" : {
        "location" : "/db2data/db2inst1/NODE0000/SQL00001/.sfae",
        "old_location" : "",
        "alias" : [
           "db2inst1_sfaedb2"
        ]
     }
  },
  "sfae_rept_version" : 1
}
```

2 Remove the directory identified by the `location` key.

Oracle:

```
# rm -rf /data/sfaedb/.sfae
```

DB2:

```
# rm -rf /db2data/db2inst1/NODE0000/SQL00001/.sfae
```

3 Remove the repository location file.

```
# rm -rf /var/vx/vxdba/rep_loc
```

This completes the removal of the SFDB repository.

Chapter 33

# Uninstalling using response files

This chapter includes the following topics:


- Uninstalling SFCFSHA using response files
- Response file variables to uninstall Veritas Storage Foundation Cluster File System High Availability
- Sample response file for Veritas Storage Foundation Cluster File System High Availability uninstallation


## Uninstalling SFCFSHA using response files

Typically, you can use the response file that the installer generates after you perform SFCFSHA uninstallation on one cluster to uninstall SFCFSHA on other clusters.

**To perform an automated uninstallation**

1. Make sure that you meet the prerequisites to uninstall SFCFSHA.
2. Copy the response file to the system where you want to uninstall SFCFSHA.
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/uninstallsfcfsha<version>
 -responsefile /tmp/response_file
```

Where <version> is the specific release version, and /tmp/*response_file* is the response file's full path name.

See "About the Veritas installer" on page 44.

# Response file variables to uninstall Veritas Storage Foundation Cluster File System High Availability

Table 33-1 lists the response file variables that you can define to configure SFCFSHA.

**Table 33-1** Response file variables for uninstalling SFCFSHA

| Variable | Description |
|---|---|
| CFG{systems} | List of systems on which the product is to be installed or uninstalled.<br>List or scalar: list<br>Optional or required: required |
| CFG{prod} | Defines the product to be installed or uninstalled.<br>List or scalar: scalar<br>Optional or required: required |
| CFG{opt}{keyfile} | Defines the location of an ssh keyfile that is used to communicate with all remote systems.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{tmppath} | Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp.<br>List or scalar: scalar<br>Optional or required: optional |

**Table 33-1** Response file variables for uninstalling SFCFSHA *(continued)*

| Variable | Description |
|---|---|
| CFG{opt}{logpath} | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.<br>List or scalar: scalar<br>Optional or required: optional |
| CFG{opt}{uninstall} | Uninstalls SFCFSHA packages.<br>List or scalar: scalar<br>Optional or required: optional |

# Sample response file for Veritas Storage Foundation Cluster File System High Availability uninstallation

The following example shows a response file for uninstalling Veritas Storage Foundation Cluster File System High Availability.

```
our %CFG;

$CFG{opt}{redirect}=1;
$CFG{opt}{uninstall}=1;
$CFG{prod}="SFCFSHA60";
$CFG{systems}=[ qw(sol90118 sol90119) ];

1;
```

Section 11

# Adding and removing nodes


- Chapter 34. Adding a node to SFCFSHA clusters
- Chapter 35. Removing a node from SFCFSHA clusters

Chapter 34

# Adding a node to SFCFSHA clusters

This chapter includes the following topics:


- About adding a node to a cluster
- Before adding a node to a cluster
- Adding a node to a cluster using the SFCFSHA installer
- Adding a node using the Web-based installer
- Adding the node to a cluster manually
- Configuring server-based fencing on the new node
- Updating the Storage Foundation for Databases (SFDB) repository after adding a node
- Sample configuration file for adding a node to the cluster


## About adding a node to a cluster

After you install SFCFSHA 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 following table provides a summary of the tasks required to add a node to an existing SFCFSHA cluster.

**Table 34-1** Tasks for adding a node to a cluster

| Step | Description |
|---|---|
| Complete the prerequisites and preparatory tasks before adding a node to the cluster. | See "Before adding a node to a cluster" on page 395. |
| Add a new node to the cluster. | See "Adding a node to a cluster using the SFCFSHA installer" on page 398.<br>See "Adding a node using the Web-based installer" on page 401.<br>See "Adding the node to a cluster manually" on page 402. |
| Complete the configuration of the new node after adding it to the cluster. | See "Configuring Cluster Volume Manager (CVM) and Cluster File System (CFS) on the new node" on page 409. |
| If you are using the Storage Foundation for Databases (SFDB) tools, you must update the repository database. | See "Updating the Storage Foundation for Databases (SFDB) repository after adding a node" on page 413. |

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 SFCFSHA cluster, perform the required preparations.

- Verify hardware and software requirements are met.
- Set up the hardware.
- Prepare the new node.

**To verify hardware and software requirements are met**

1 Review hardware and software requirements for SFCFSHA.

See "Assessing the system for installation readiness" on page 64.

2 Verify the new system has the same identical operating system versions and patch levels as that of the existing cluster

3 Verify the existing cluster is an SFCFSHA cluster and that SFCFSHA is running on the cluster.

4 If the cluster is upgraded from the previous version, you must check the cluster protocol version to make sure it has the same version as the node to be added. If there is a protocol mismatch, the node is unable to join the existing cluster.

Check the cluster protocal version using:

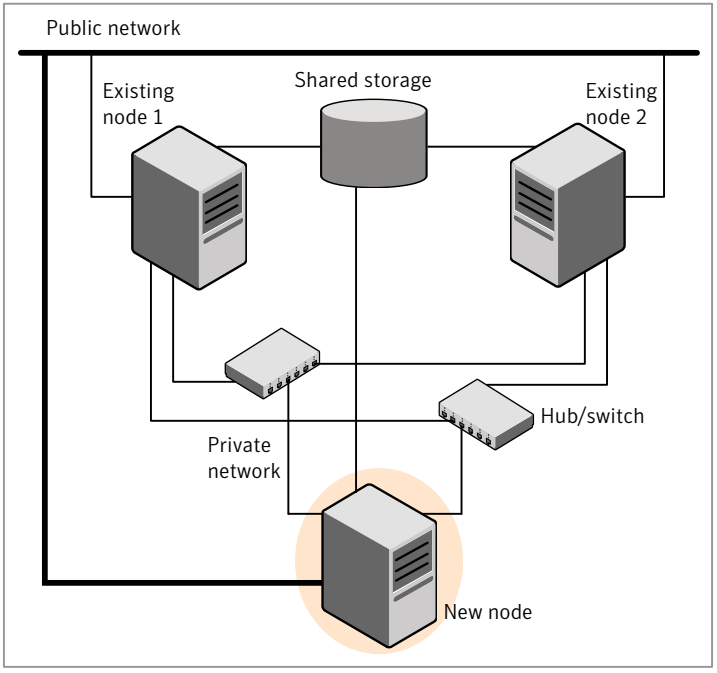
```
# vxdctl protocolversion
Cluster running at protocol 120
```

5 If the cluster protocol on the master node is below 120, upgrade it using:

```
# vxdctl upgrade [version]
```

Before you configure a new system on an existing cluster, you must physically add the system to the cluster as illustrated in Figure 34-1.

**Figure 34-1** Adding a node to a two-node cluster using two switches




**To set up the hardware**

1 Connect the SFCFSHA private Ethernet controllers.

Perform the following tasks as necessary:

- When you add nodes to a cluster, use independent switches or hubs for the private network connections. You can only use crossover cables for a two-node cluster, so you might have to swap out the cable for a switch or hub.
- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

Figure 34-1 illustrates a new node being added to an existing two-node cluster using two independent hubs.

2 Make sure that you meet the following requirements:

- The node must be connected to the same shared storage devices as the existing nodes.
- The node must have private network connections to two independent switches for the cluster.
  For more information, see the *Veritas Cluster Server Installation Guide*.
- The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster.

Complete the following preparatory steps on the new node before you add it to an existing SFCFSHA cluster.

**To prepare the new node**

1 Verify that the new node meets installation requirements.

```
# ./installsfcfsha -precheck
```

You can also use the Web-based installer for the precheck.

2 Install SFCFSHA on the new system. Make sure all the VRTS packages available on the existing nodes are also available on the new node.

```
# cd /opt/VRTS/install

# ./installsfcfsha<version>
```

Where `<version>` is the specific release version.

Do not configure SFCFSHA when prompted.

3 You can restart the new node after installation is complete. Configure the new node using the configuration from the existing cluster nodes.

See "About installation and configuration methods" on page 42.

# Adding a node to a cluster using the SFCFSHA installer

You can add a node to a cluster using the `-addnode` option with the SFCFSHA installer.

The SFCFSHA installer performs the following tasks:

- Verifies that the node and the existing cluster meet communication requirements.
- Verifies the products and packages installed but not configured on the new node.
- Discovers the network interfaces on the new node and checks the interface settings.
- Creates the following files on the new node:

  `/etc/llttab`

  `/etc/VRTSvcs/conf/sysname`
- Copies the following files on the new node:

  `/etc/llthosts`

  `/etc/gabtab`

  `/etc/VRTSvcs/conf/config/main.cf`
- Copies the following files from the existing cluster to the new node:

  `/etc/vxfenmode`

  `/etc/vxfendg`

  `/etc/vcsmmtab`

  `/etc/vx/.uuids/clusuuid`

  `/etc/default/llt`

  `/etc/default/gab`
- Generate security credentials on the new node if the CPS server of existing cluster is secure
- Configures disk-based or server-based fencing depending on the fencing mode in use on the existing cluster.
- Adds the new node to the CVM, ClusterService, and VxSS service groups in the VCS configuration.

  **Note:** For other service groups configured under VCS, update the configuration for the new node manually.
- Starts SFCFSHA processes and configures CVM and CFS on the new node.

At the end of the process, the new node joins the SFCFSHA 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 SFCFSHA installer with the -addnode option.

   ```
   # cd /opt/VRTS/install

   # ./installsfcfsha<version> -addnode
   ```

   Where `<version>` is the specific release version.

   See "About the Veritas installer" on page 44.

   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 SFCFSHA cluster.

   The installer uses the node information to identify the existing cluster.

   ```
   Enter one node of the SFCFSHA cluster to which
   you would like to add one or more new nodes: sys1
   ```
4. Review and confirm the cluster information.
5. Enter the name of the systems that you want to add as new nodes to the cluster.

   ```
   Enter the system names separated by spaces
   to add to the cluster: sys5
   ```

   Confirm if the installer prompts if you want to add the node to the cluster.

   The installer checks the installed products and packages on the nodes and discovers the network interfaces.

6 Enter the name of the network interface that you want to configure as the first private heartbeat link.

**Note:** The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster. The LLT configuration for the new node must be the same as that of the existing cluster.

```
Enter the NIC for the first private heartbeat
link on sys5: [b,q,?] bge1

Enter the NIC for the second private heartbeat
link on sys5: [b,q,?] bge2
```

**Note:** At least two private heartbeat links must be configured for high availability of the cluster.

7 Depending on the number of LLT links configured in the existing cluster, configure additional private heartbeat links for the new node.

The installer verifies the network interface settings and displays the information.

8 Review and confirm the information.

9 If you have configured SMTP, SNMP, or the global cluster option in the existing cluster, you are prompted for the NIC information for the new node.

```
Enter the NIC for VCS to use on sys5: bge3

SFCFSHA is configured on the cluster. Do you want to
configure it on the new node(s)? [y,n,q] (y) n
```

10 The installer prompts you with an option to mount the shared volumes on the new node. Select **y** to mount them.

When completed, the installer confirms the volumes are mounted. The installer indicates the location of the log file, summary file, and response file with details of the actions performed.

11 If the existing cluster uses server-based fencing in secure mode, the installer will configure server-based fencing in secure mode on the new nodes.

The installer then starts all the required Veritas processes and joins the new node to cluster.

The installer indicates the location of the log file, summary file, and response file with details of the actions performed.

12 Confirm that the new node has joined the SFCFSHA cluster using `lltstat -n` and `gabconfig -a` commands.

If the new node has not joined the cluster, verify if it has been added to the SystemList.

# Adding a node using the Web-based installer

You can use the Web-based installer to add a node to a cluster.

**To add a node to a cluster using the Web-based installer**

1 From the Task pull-down menu, select **Add a Cluster node**.

From the product pull-down menu, select the product.

Click the **Next** button.

2 Click **OK** to confirm the prerequisites to add a node.

3 In the System Names field enter a name of a node in the cluster where you plan to add the node and click **OK**.

The installer program checks inter-system communications and compatibility. If the node fails any of the checks, review the error and fix the issue.

If prompted, review the cluster's name, ID, and its systems. Click the **Yes** button to proceed.

4 In the System Names field, enter the names of the systems that you want to add to the cluster as nodes. Separate system names with spaces. Click the **Next** button.

The installer program checks inter-system communications and compatibility. If the system fails any of the checks, review the error and fix the issue.

Click the **Next** button. If prompted, click the **Yes** button to add the system and to proceed.

5 From the heartbeat NIC pull-down menus, select the heartbeat NICs for the cluster. Click the **Next** button.

6 Once the addition is complete, review the log files. Optionally send installation information to Symantec. Click the **Finish** button to complete the node's addition to the cluster.

# Adding the node to a cluster manually

Perform this procedure after you install SFCFSHA only if you plan to add the node to the cluster manually.

**Table 34-2** Procedures for adding a node to a cluster manually

| Step | Description |
|---|---|
| Start the Veritas Volume Manager (VxVM) on the new node. | See "Starting Veritas Volume Manager (VxVM) on the new node" on page 403. |
| Configure the cluster processes on the new node. | See "Configuring cluster processes on the new node" on page 403. |
| If the CPS server of existing cluster is secure, generate security credentials on the new node. | See "Setting up the node to run in secure mode" on page 405. |
| Configure fencing for the new node to match the fencing configuration on the existing cluster.<br>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 408. |
| Start VCS. | See "To start VCS on the new node" on page 409. |
| Configure CVM and CFS. | See "Configuring Cluster Volume Manager (CVM) and Cluster File System (CFS) on the new node" on page 409. |
| 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 410. |

## Starting Veritas Volume Manager (VxVM) on the new node

Veritas Volume Manager (VxVM) uses license keys to control access. As you run the `vxinstall` utility, answer **n** to prompts about licensing. You installed the appropriate license when you ran the `installsfcfsha` program.

**To start VxVM on the new node**

1. To start VxVM on the new node, use the vxinstall utility:

   ```
   # vxinstall
   ```

2. Enter **n** when prompted to set up a system wide disk group for the system.

   The installation completes.

3. Verify that the daemons are up and running. Enter the command:

   ```
   # vxdisk list
   ```

   Make sure the output displays the shared disks without errors.

## Configuring cluster processes on the new node

Perform the steps in the following procedure to configure cluster processes on the new node.

1. Edit the /etc/llthosts file on the existing nodes. Using vi or another text editor, add the line for the new node to the file. The file resembles:

   ```
   0 sys1
   1 sys2
   2 sys5
   ```

2. Copy the `/etc/llthosts` file from one of the existing systems over to the new system. The `/etc/llthosts` file must be identical on all nodes in the cluster.

3. Create an `/etc/lltab` file on the new system. For example:

   ```
   set-node sys5
   set-cluster 101

   link bge1 /dev/bge:1 - ether - -
   link bge2 /dev/bge:2 - ether - -
   ```

   Except for the first line that refers to the node, the file resembles the /etc/lltab files on the existing nodes. The second line, the cluster ID, must be the same as in the existing nodes.

4 Use vi or another text editor to create the file `/etc/gabtab` on the new node. This file must contain a line that resembles the following example:

```
/sbin/gabconfig -c -nN
```

Where N represents the number of systems in the cluster including the new node. For a three-system cluster, N would equal 3.

5 Edit the /etc/gabtab file on each of the existing systems, changing the content to match the file on the new system.

6 For the following files on the new node:

```
/etc/default/llt
/etc/default/gab
/etc/default/vxfen
/etc/default/vcs
```

Verify if the attributes in each file are set as follows before using smf on Solaris 10 to start the related processes and to load drivers:

```
LLT_START/LLT_STOP=1
GAB_START/GAB_STOP=1
VXFEN_START/VXFEN_STOP=1
VCS_START/VCS_STOP=1
```

7 Use vi or another text editor to create the file `/etc/VRTSvcs/conf/sysname` on the new node. This file must contain the name of the new node added to the cluster.

For example:

```
sys5
```

8 Create the Unique Universal Identifier file `/etc/vx/.uuids/clusuuid` on the new node:

```
# /opt/VRTSvcs/bin/uuidconfig.pl -rsh -clus -copy \
-from_sys sys1 -to_sys sys5
```

9 Start the LLT, GAB, and ODM drivers on the new node:

```
# svcadm enable llt

# svcadm enable gab

# svcadm restart vxodm
```

10 On the new node, verify that the GAB port memberships are a and d:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen df204 membership 012
Port b gen df20a membership 012
Port d gen df207 membership 012
```

## Setting up the node to run in secure mode

You must follow this procedure only if you are adding a node to a cluster that is running in secure mode. If you are adding a node to a cluster that is not running in a secure mode, proceed with configuring LLT and GAB.

Table 34-3 uses the following information for the following command examples.

**Table 34-3** The command examples definitions

| Name | Fully-qualified host name (FQHN) | Function |
|---|---|---|
| sys5 | sys5.nodes.example.com | The new node that you are adding to the cluster. |

## Configuring the authentication broker on node sys5

**To configure the authentication broker on node sys5**

1 Extract the embedded authentication files and copy them to temporary directory:

```
# mkdir -p /var/VRTSvcs/vcsauth/bkup

# cd /tmp; gunzip -c /opt/VRTSvcs/bin/VxAT.tar.gz | tar xvf -
```

2 Edit the setup file manually:

```
# cat /etc/vx/.uuids/clusuuid 2>&1
```

The output is a string denoting the UUID. This UUID (without { and }) is used as the ClusterName for the setup file.

```
{UUID}

# cat /tmp/eat_setup 2>&1
```

The file content must resemble the following example:

```
AcceptorMode=IP_ONLY

BrokerExeName=vcsauthserver

ClusterName=UUID

DataDir=/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER

DestDir=/opt/VRTSvcs/bin/vcsauth/vcsauthserver

FipsMode=0

IPPort=14149

RootBrokerName=vcsroot_uuid

SetToRBPlusABorNot=0

SetupPDRs=1

SourceDir=/tmp/VxAT/version
```

3 Set up the embedded authentication file:

```
# cd /tmp/VxAT/version/bin/edition_number; \
./broker_setup.sh/tmp/eat_setup

# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssregctl -s -f
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER/root/.VRTSat/profile \
/VRTSatlocal.conf -b 'Security\Authentication \
\Authentication Broker' -k UpdatedDebugLogFileName \
-v /var/VRTSvcs/log/vcsauthserver.log -t string
```

4 Copy the broker credentials from one node in the cluster to sys5 by copying the entire `bkup` directory.

The `bkup` directory content resembles the following example:

```
# cd /var/VRTSvcs/vcsauth/bkup/

# ls

CMDSERVER  CPSADM CPSERVER  HAD  VCS_SERVICES  WAC
```

5 Import the VCS_SERVICES domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atutil import -z \
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER -f /var/VRTSvcs/vcsauth/bkup \
/VCS_SERVICES -p password
```

6 Import the credentials for HAD, CMDSERVER, CPSADM, CPSERVER, and WAC.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atutil import -z \
/var/VRTSvcs/vcsauth/data/VCS_SERVICES -f /var/VRTSvcs/vcsauth/bkup \
/HAD -p password
```

7 Start the vcsauthserver process on sys5.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh
```

8 Perform the following tasks:

```
# mkdir /var/VRTSvcs/vcsauth/data/CLIENT

# mkdir /var/VRTSvcs/vcsauth/data/TRUST

# export EAT_DATA_DIR='/var/VRTSvcs/vcsauth/data/TRUST'

# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat setuptrust -b \
localhost:14149 -s high
```

9 Create the `/etc/VRTSvcs/conf/config/.secure` file:

```
# touch /etc/VRTSvcs/conf/config/.secure
```

## Starting fencing on the new node

Perform the following steps to start fencing on the new node.

**To start fencing on the new node**

1 For disk-based fencing on at least one node, copy the following files from one of the nodes in the existing cluster to the new node:

```
/etc/default/vxfen
/etc/vxfendg
/etc/vxfenmode
```

If you are using pure CP server-based fencing on the existing cluster, then only the /etc/vxfenmode file needs to be copied on the new node.

2 Start fencing on the new node:

```
# svcadm enable vxfen
```

3 On the new node, verify that the GAB port memberships are a, b, and d:

```
# gabconfig -a

GAB Port Memberships
===============================================================
Port a gen    df204 membership 012
Port b gen    df20d membership 012
Port d gen    df20a membership 012
```

## After adding the new node

Start VCS on the new node.

**To start VCS on the new node**

1. Start VCS on the new node:

```
# hastart
```

   VCS brings the CVM group online.

2. Verify that the CVM group is online:

```
# hagrp -state
```

## Configuring Cluster Volume Manager (CVM) and Cluster File System (CFS) on the new node

Modify the existing cluster configuration to configure Cluster Volume Manager (CVM) and Cluster File System (CFS) for the new node.

**To configure CVM and CFS on the new node**

1. Make a backup copy of the main.cf file on the existing node, if not backed up in previous procedures. For example:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.cf.2node
```

2. On one of the nodes in the existing cluster, set the cluster configuration to read-write mode:

```
# haconf -makerw
```

3. Add the new node to the VCS configuration, if not already added:

```
# hasys -add sys5
```

4 To enable the existing cluster to recognize the new node, run the following commands on one of the existing nodes:

```
# hagrp -modify cvm SystemList -add sys5 2
# hagrp -modify cvm AutoStartList -add sys5
# hares -modify cvm_clus CVMNodeId -add sys5 2
# haconf -dump -makero
# /etc/vx/bin/vxclustadm -m vcs reinit
# /etc/vx/bin/vxclustadm nidmap
```

5 On the remaining nodes of the existing cluster, run the following commands:

```
# /etc/vx/bin/vxclustadm -m vcs reinit
# /etc/vx/bin/vxclustadm nidmap
```

6 Copy the configuration files from one of the nodes in the existing cluster to the new node:

```
# rcp /etc/VRTSvcs/conf/config/main.cf \
sys5:/etc/VRTSvcs/conf/config/main.cf
# rcp /etc/VRTSvcs/conf/config/CFSTypes.cf \
sys5:/etc/VRTSvcs/conf/config/CFSTypes.cf
# rcp /etc/VRTSvcs/conf/config/CVMTypes.cf \
sys5:/etc/VRTSvcs/conf/config/CVMTypes.cf
```

7 The `/etc/vx/tunefstab` file sets non-default tunables for local-mounted and cluster-mounted file systems.

If you have configured a `/etc/vx/tunefstab` file to tune cluster-mounted file systems on any of the existing cluster nodes, you may want the new node to adopt some or all of the same tunables.

To adopt some or all tunables, review the contents of the file, and copy either the file, or the portions desired, into the `/etc/vx/tunefstab` file on the new cluster 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 sys1, write-enable the configuration:

```
# haconf -makerw
```

2 Add the node sys5 to the existing ClusterService group.

```
# hagrp -modify ClusterService SystemList -add sys5 2

# hagrp -modify ClusterService AutoStartList -add sys5
```

3 Modify the IP address and NIC resource in the existing group for the new node.

```
# hares -modify gcoip Device bge0 -sys sys5

# hares -modify gconic Device bge0 -sys sys5
```

4 Save the configuration by running the following command from any node.

```
# haconf -dump -makero
```

# Configuring server-based fencing on the new node

This section describes the procedures to configure server-based fencing on a new node. Depending on whether server-based fencing is configured in secure or non-secure mode on the existing cluster, perform the tasks in one of the following procedures:

- Server-based fencing in non-secure mode:
  To configure server-based fencing in non-secure mode on the new node
- Server-based fencing in secure mode:
  To configure server-based fencing with security on the new node

**To configure server-based fencing in non-secure mode on the new node**

1 Log in to each CP server as the root user.

2 Update each CP server configuration with the new node information:

```
# cpsadm -s cps1.symantecexample.com \
-a add_node -c clus1 -h sys5 -n2

Node 2 (sys5) successfully added
```

3 Verify that the new node is added to the CP server configuration:

```
# cpsadm -s cps1.symantecexample.com \
-a list_nodes
```

The new node must be listed in the command output.

4 Add the VCS user cpsclient@sys5 to each CP server:

```
# cpsadm -s cps1.symantecexample.com \
-a add_user -e cpsclient@sys5 \
-f cps_operator -g vx

User cpsclient@sys5 successfully added
```

**To configure server-based fencing with security on the new node**

1 Log in to each CP server as the root user.

2 Update each CP server configuration with the new node information:

```
# cpsadm -s cps1.symantecexample.com \
-a add_node -c clus1 -h sys5 -n2

Node 2 (sys5) successfully added
```

3 Verify that the new node is added to the CP server configuration:

```
# cpsadm -s cps1.symantecexample.com -a list_nodes
```

The new node must be listed in the output.

## Adding the new node to the vxfen service group

Perform the steps in the following procedure to add the new node to the vxfen service group.

**To add the new node to the vxfen group using the CLI**

1 On one of the nodes in the existing SFCFSHA cluster, set the cluster configuration to read-write mode:

```
# haconf -makerw
```

2 Add the node sys5 to the existing vxfen group.

```
# hagrp -modify vxfen SystemList -add sys5 2
```

3 Save the configuration by running the following command from any node in the SFCFSHA cluster:

```
# haconf -dump -makero
```

# Updating the Storage Foundation for Databases (SFDB) repository after adding a node

If you are using Database Storage Checkpoints, Database FlashSnap, or SmartTier for Oracle 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 Copy the `/var/vx/vxdba/rep_loc` file from one of the nodes in the cluster to the new node.

2 If the `/var/vx/vxdba/auth/user-authorizations` file exists on the existing cluster nodes, copy it to the new node.

If the `/var/vx/vxdba/auth/user-authorizations` file does not exist on any of the existing cluster nodes, no action is required.

This completes the addition of the new node to the SFDB repository.

For information on using SFDB tools features:

See *Veritas Storage Foundation: Storage and Availability Management for Oracle Databases*

See *Veritas Storage Foundation: Storage and Availability Management for DB2 Databases*

# Sample configuration file for adding a node to the cluster

You may use this sample file as reference information to understand the configuration changes that take place when you add a node to a cluster.

The existing sample configuration before adding the node `sys5` is as follows:

- The existing cluster `clus1` comprises two nodes `sys1` and `sys2` and hosts a single database.
- The Oracle database is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- Only one private IP address is configured for Oracle Clusterware. The private IP address is managed by the PrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.

The following sample configuration file shows the changes (in **bold**) effected in the configuration after adding a node "sys5" to the cluster.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"


cluster clus1 (
        UserNames = { admin = bopHo }
        Administrators = { admin }
        UseFence = SCSI3
        )


system clus1 (
        )
system sys2 (
        )
system sys5 (
       )
```

**Note:** In the following group oradb1_grp, the sys5 node has been added.

```
group oradb1_grp (
        SystemList = { clus1 = 0, sys2 = 1, sys5 = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { clus1, sys2, sys5 }
        )
```

**Note:** In the following Oracle resource, the sys5 node information has been added.

```
Oracle ora1 (
          Critical = 0
          Sid @clus1 = vrts1
          Sid @sys2 = vrts2
          Sid @sys5 = vrts3
          Owner = oracle
          Home = "/app/oracle/orahome"
          StartUpOpt = "SRVCTLSTART"
          ShutDownOpt = "SRVCTLSTOP"
          )

CFSMount oradata_mnt (
         Critical = 0
         MountPoint = "/oradata"
         BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
         )

CVMVolDg oradata_voldg (
         Critical = 0
         CVMDiskGroup = oradatadg
         CVMVolume = { oradatavol }
         CVMActivation = sw
         )

requires group cvm online local firm
ora1 requires oradata_mnt
oradata_mnt requires oradata_voldg
```

**Note:** In the following CVM and CVMCluster resources, the sys5 node information has been added.

```
group cvm (
        SystemList = { clus1 = 0, sys2 = 1, sys5 =2}
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { clus1, sys2, sys5 }
        )

        Application cssd (
                Critical = 0
                StartProgram = "/opt/VRTSvcs/rac/bin/cssd-online"
                StopProgram = "/opt/VRTSvcs/rac/bin/cssd-offline"
                CleanProgram = "/opt/VRTSvcs/rac/bin/cssd-clean"
                MonitorProgram = "/opt/VRTSvcs/rac/bin/cssd-monitor"
                OnlineRetryLimit = 20
                )

       CFSMount ocrvote_mnt (
                Critical = 0
                MountPoint = "/ocrvote"
                BlockDevice = "/dev/vx/dsk/ocrvotedg/ocrvotevol"
                MountOpt= "mincache=direct"
                )

      CVMVolDg ocrvote_voldg (
               Critical = 0
               CVMDiskGroup = ocrvotedg
               CVMVolume = { ocrvotevol }
               CVMActivation = sw
               )


      CFSfsckd vxfsckd (
               )



      CVMCluster cvm_clus (
              CVMClustName = clus1
              CVMNodeId = { clus1 = 0, sys2 = 1, sys5 =2 }
              CVMTransport = gab
              CVMTimeout = 200
              )
```

```
      CVMVxconfigd cvm_vxconfigd (
               Critical = 0
               CVMVxconfigdArgs = { syslog }
               )
```

**Note:** In the following PrivNIC resource, the sys5 node information has been added.

```
PrivNIC ora_priv (
              Critical = 0
              Device@clus1 = { bge1 = 0, bge2 = 1}
              Device@sys2 = { bge1 = 0, bge2 = 1}
              Device@sys5 = { bge1 = 0, bge2 = 1}
              Address@clus1 = "192.168.12.1"
              Address@sys2 = "192.168.12.2"
              Address@sys5 = "192.168.12.5"
              NetMask = "255.255.255.0"
              )


cssd requires ocrvote_mnt
cssd requires ora_priv
ocrvote_mnt requires ocrvote_voldg
ocrvote_mnt requires vxfsckd
ocrvote_voldg requires cvm_clus
vxfsckd requires cvm_clus
cvm_clus requires cvm_vxconfigd
```

Chapter 35

# Removing a node from SFCFSHA clusters

This chapter includes the following topics:


- About removing a node from a cluster
- Removing a node from a cluster
- Modifying the VCS configuration files on existing nodes
- Modifying the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node
- Removing the node configuration from the CP server
- Removing security credentials from the leaving node
- Updating the Storage Foundation for Databases (SFDB) repository after removing a node
- Sample configuration file for removing a node from the cluster


## About removing a node from a cluster

You can remove one or more nodes from an SFCFSHA cluster. The following table provides a summary of the tasks required to add a node to an existing SFCFSHA cluster.

**Table 35-1** Tasks for removing a node from a cluster

| Step | Description |
|---|---|
| Prepare to remove the node:<br>■ Back up the configuration file.<br>■ Check the status of the nodes and the service groups.<br>■ Take the service groups offline and removing the database instances. | See "Removing a node from a cluster" on page 419. |
| Remove the node from the cluster. | See "Removing a node from a cluster" on page 419. |
| Modify the cluster configuration on remaining nodes.<br>■ Edit the /etc/llthosts file.<br>■ Edit the /etc/gabtab file.<br>■ Modify the VCS configuration to remove the node.<br>■ Modify the CVM configuration to remove the node. | See "Modifying the VCS configuration files on existing nodes" on page 420.<br>See "Modifying the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node" on page 423. |
| If the existing cluster is configured to use server-based I/O fencing, remove the node configuration from the Coordination Point (CP) server. | See "Removing the node configuration from the CP server" on page 423. |
| 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 424. |
| Updating the Storage Foundation for Databases (SFDB) repository after removing a node | See "Updating the Storage Foundation for Databases (SFDB) repository after removing a node" on page 425. |

The Veritas product installer does not support removing a node. You must remove a node manually. The example procedures describe how to remove a node from a cluster with three nodes.

# Removing a node from a cluster

Perform the following steps to remove a node from a cluster. The procedure can be done from any node remaining in the cluster or from a remote host.

**To prepare to remove a node from a cluster**

1 Take your application service groups offline if they are under Veritas Cluster Server (VCS) control on the node you want to remove.

```
# hagrp -offline app_group -sys sys5
```

2 Stop the applications that use Veritas File System (VxFS) or Cluster File System (CFS) mount points and are not configured under VCS. Use native application commands to stop the applications.

**To remove a node from a cluster**

1 Unmount the VxFS/CFS file systems that are not configured under VCS.

```
# umount mount_point
```

2 Stop VCS on the node:

```
# hastop -local
```

3 Uninstall SFCFSHA from the node using the SFCFSHA installer.

```
# cd /opt/VRTS/install

# ./uninstallsfcfsha sys5
```

The installer stops all SFCFSHA processes and uninstalls the SFCFSHA packages.

4 Modify the VCS configuration files on the existing nodes to remove references to the deleted node.

See "Modifying the VCS configuration files on existing nodes" on page 420.

5 Modify the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node.

See "Modifying the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node" on page 423.

# Modifying the VCS configuration files on existing nodes

Modify the configuration files on the remaining nodes of the cluster to remove references to the deleted nodes.

Tasks for modifying the cluster configuration files:

- Edit the /etc/llthosts file
- Edit the /etc/gabtab file
- Modify the VCS configuration to remove the node

For an example main.cf:

See "Sample configuration file for removing a node from the cluster" on page 425.

**To edit the /etc/llthosts file**

- On each of the existing nodes, edit the `/etc/llthosts` file to remove lines that contain references to the removed nodes.

  For example, if sys5 is the node removed from the cluster, remove the line "2 sys5" from the file:

  ```
  0 sys1
  1 sys2
  2 sys5
  ```

  Change to:

  ```
  0 sys1
  1 sys2
  ```

**To edit the /etc/gabtab file**

- Modify the following command in the `/etc/gabtab` file to reflect the number of systems after the node is removed:

  ```
  /sbin/gabconfig -c -nN
  ```

  where N is the number of remaining nodes in the cluster.

  For example, with two nodes remaining, the file resembles:

  ```
  /sbin/gabconfig -c -n2
  ```

Modify the VCS configuration file main.cf to remove all references to the deleted node.

Use one of the following methods to modify the configuration:

- Edit the `/etc/VRTSvcs/conf/config/main.cf` file
  This method requires application down time.
- Use the command line interface
  This method allows the applications to remain online on all remaining nodes.

The following procedure uses the command line interface and modifies the sample VCS configuration to remove references to the deleted node. Run the steps in the procedure from one of the existing nodes in the cluster. The procedure allows you to change the VCS configuration while applications remain online on the remaining nodes.

**To modify the cluster configuration using the command line interface (CLI)**

1 Back up the `/etc/VRTSvcs/conf/config/main.cf` file.

```
# cd /etc/VRTSvcs/conf/config

# cp main.cf main.cf.3node.bak
```

2 Change the cluster configuration to read-write mode:

```
# haconf -makerw
```

3 Remove the node from the AutoStartList attribute of the service group by specifying the remaining nodes in the desired order:

```
# hagrp -modify cvm AutoStartList sys1 sys2
```

4 Remove the node from the SystemList attribute of the service group:

```
# hagrp -modify cvm SystemList -delete sys5
```

If the system is part of the SystemList of a parent group, it must be deleted from the parent group first.

5 Remove the node from the CVMNodeId attribute of the service group:

```
# hares -modify cvm_clus CVMNodeId -delete sys5
```

6 If you have the other service groups (such as the database service group or the ClusterService group) that have the removed node in their configuration, perform step 4 and step 5 for each of them.

7 Remove the deleted node from the NodeList attribute of all CFS mount resources:

```
# hares -modify CFSMount NodeList -delete sys5
```

8 Remove the deleted node from the system list of any other service groups that exist on the cluster. For example, to delete the node sys5:

```
# hagrp -modify appgrp SystemList -delete sys5
```

9 Remove the deleted node from the cluster system list:

```
# hasys -delete sys5
```

10 Save the new configuration to disk:

```
# haconf -dump -makero
```

11 Verify that the node is removed from the VCS configuration.

```
# grep -i sys5 /etc/VRTSvcs/conf/config/main.cf
```

If the node is not removed, use the VCS commands as described in this procedure to remove the node.

# Modifying the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node

**To modify the CVM configuration on the existing nodes to remove references to the deleted node**

- On the remaining nodes of the existing cluster, run the following commands:

```
# /etc/vx/bin/vxclustadm -m vcs reinit
# /etc/vx/bin/vxclustadm nidmap
```

# Removing the node configuration from the CP server

After removing a node from a SFCFSHA cluster, perform the steps in the following procedure to remove that node's configuration from the CP server.

---

**Note:** The `cpsadm` command is used to perform the steps in this procedure. For detailed information about the `cpsadm` command, see the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide*.

---

**To remove the node configuration from the CP server**

1. Log into the CP server as the root user.
2. View the list of VCS users on the CP server, using the following command:

   ```
   # cpsadm -s cp_server -a list_users
   ```

   Where *cp_server* is the virtual IP/ virtual hostname of the CP server.
3. Remove the VCS user associated with the node you previously removed from the cluster.

   For CP server in non-secure mode:

   ```
   # cpsadm -s cp_server  -a rm_user \
   -e cpsclient@sys5  -f cps_operator  -g vx
   ```

4. Remove the node entry from the CP server:

   ```
   # cpsadm -s cp_server -a rm_node  -h sys5 -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 sys5. Perform the following steps.

**To remove the security credentials**

1. Stop the AT process.

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh \
   stop
   ```

2. Remove the credentials.

   ```
   # rm -rf /var/VRTSvcs/vcsauth/data/
   ```

# Updating the Storage Foundation for Databases (SFDB) repository after removing a node

After removing a node from a cluster, you do not need to perform any steps to update the SFDB repository.

For information on removing the SFDB repository after removing the product:

See "Removing the Storage Foundation for Databases (SFDB) repository after removing the product" on page 387.

# Sample configuration file for removing a node from the cluster

You may use this sample file as reference information to understand the configuration changes involved when you remove a node from a cluster.

The existing sample configuration before removing the node *system3* is as follows:

- The existing cluster*cluster1*comprises three nodes *system1*, *system2*, and *system3* and hosts a single database.
- The database is stored on CFS.
- The database is managed by a VCS database agent.
  The agent starts, stops, and monitors the database.

---

**Note:** The following sample file shows in **bold** the configuration information that is removed when the node *system3* is removed from the cluster.

---

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"

cluster cluster1 (
        UserNames = { admin = bopHo }
        Administrators = { admin }
        UseFence = SCSI3
        )

cluster cluster1 (
        UserNames = { admin = bopHo }
        Administrators = { admin }
```

```
        UseFence = SCSI3
        )

system system1 (
        )
system system2 (
        )
system system3 (
       )
```

**Note:** In the following group *app_grp*, the *system3* node must be removed.

```
group app_grp (
        SystemList = { system1 = 0, system2 = 1, system3 = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { system1, system2, system3 }
        )
```

**Note:** In the following application resource, the *system3* node information must be removed.

```
App app1 (
          Critical = 0
          Sid @system1 = vrts1
          Sid @system2 = vrts2
          Sid @system3 = vrts3
          )

CFSMount appdata_mnt (
         Critical = 0
         MountPoint = "/oradata"
         BlockDevice = "/dev/vx/dsk/appdatadg/appdatavol"
         )

CVMVolDg appdata_voldg (
         Critical = 0
         CVMDiskGroup = appdatadg
         CVMVolume = { appdatavol }
         CVMActivation = sw
         )
```

```
requires group cvm online local firm
app1 requires appdata_mnt
appdata_mnt requires appdata_voldg
```

**Note:** In the following CVM and CVMCluster resources, the *system3* node information must be removed.

```
group cvm (
        SystemList = { system1 = 0, system2 = 1, system3 =2}
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { system1, system2, system3 }
        )

        CFSfsckd vxfsckd (
                )



        CVMCluster cvm_clus (
              CVMClustName = rac_cluster101
              CVMNodeId = { system1 = 0, system2 = 1, system3 =2 }
              CVMTransport = gab
              CVMTimeout = 200
              )


       CVMVxconfigd cvm_vxconfigd (
               Critical = 0
               CVMVxconfigdArgs = { syslog }
               )


vxfsckd requires cvm_clus
cvm_clus requires cvm_vxconfigd
```

Section 12

# Installation reference


- Appendix A. Installation scripts
- Appendix B. Tunable files for installation
- Appendix C. Configuration files
- Appendix D. Configuring the secure shell or the remote shell for communications
- Appendix E. Storage Foundation Cluster File System High Availability components
- Appendix F. High availability agent information
- Appendix G. Troubleshooting the SFCFSHA installation
- Appendix H. Sample SFCFSHA cluster setup diagrams for CP server-based I/O fencing
- Appendix I. Reconciling major/minor numbers for NFS shared disks
- Appendix J. Configuring LLT over UDP
- Appendix K. Compatability issues when installing Storage Foundation Cluster File System High Availability with other products

Appendix A

# Installation scripts

This appendix includes the following topics:


- Installation script options
- About using the postcheck option


## 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 the Veritas installer" on page 44.

**Table A-1** Available command line options

| Commandline Option | Function |
|---|---|
| -addnode | Adds a node to a high availability cluster. |
| -allpkgs | Displays all packages required for the specified product. The packages are listed in correct installation order. The output can be used to create scripts for command line installs, or for installations over a network. |
| -comcleanup | The `-comcleanup` option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated. |
| -configure | Configures the product after installation. |

**Table A-1** Available command line options *(continued)*

| Commandline Option | Function |
|---|---|
| -fencing | Configures I/O fencing in a running cluster. |
| –hostfile *full_path_to_file* | Specifies the location of a file that contains a list of hostnames on which to install. |
| -installallpkgs | The `-installallpkgs` option is used to select all packages. |
| -installrecpkgs | The `-installrecpkgs`option is used to select the recommended packages set. |
| –installminpkgs | The `-installminpkgs`option is used to select the minimum packages set. |
| -ignorepatchreqs | The `-ignorepatchreqs` option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system. |
| –jumpstart *dir_path* | Produces a sample finish file for Solaris JumpStart installation. The *dir_path* indicates the path to the directory in which to create the finish file. |
| –keyfile *ssh_key_file* | Specifies a key file for secure shell (SSH) installs. This option passes `-i ssh_key_file` to every SSH invocation. |
| -license | Registers or updates product licenses on the specified systems. |
| –logpath *log_path* | Specifies a directory other than `/opt/VRTS/install/logs` as the location where installer log files, summary files, and response files are saved. |
| -makeresponsefile | Use the `-makeresponsefile` option only to generate response files. No actual software installation occurs when you use this option. |
| -minpkgs | Displays the minimal packages required for the specified product. The packages are listed in correct installation order. Optional packages are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option. |

**Table A-1** Available command line options *(continued)*

| Commandline Option | Function |
|---|---|
| -nolic | Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified. |
| –pkginfo | Displays a list of packages and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the -pkginfo option with the installvcs script to display VCS packages. |
| –pkgpath *package_path* | Designates the path of a directory that contains all packages to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems. |
| –pkgset | Discovers and displays the package group (minimum, recommended, all) and packages that are installed on the specified systems. |
| -pkgtable | Displays product's packages in correct installation order by group. |
| –postcheck | Checks for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups. |
| -precheck | Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product. |
| –recpkgs | Displays the recommended packages required for the specified product. The packages are listed in correct installation order. Optional packages are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option. |
| -redirect | Displays progress details without showing the progress bar. |

**Table A-1** Available command line options *(continued)*

| Commandline Option | Function |
|---|---|
| -requirements | The `-requirements` option displays required OS version, required packages and patches, file system space, and other system requirements in order to install the product. |
| –responsefile *response_file* | Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. |
| -rolling_upgrade | Starts a rolling upgrade. Using this option, the installer detects the rolling upgrade status on cluster systems automatically without the need to specify rolling upgrade phase 1 or phase 2 explicitly. |
| -rollingupgrade_phase1 | The `-rollingupgrade_phase1` option is used to perform rolling upgrade Phase-I. In the phase, the product kernel packages get upgraded to the latest version. |
| -rollingupgrade_phase2 | The `-rollingupgrade_phase2` option is used to perform rolling upgrade Phase-II. In the phase, VCS and other agent packages upgrade to the latest version. Product kernel drivers are rolling-upgraded to the latest protocol version. |
| –rootpath *root_path* | Specifies an alternative root directory on which to install packages.<br>On Solaris operating systems, `-rootpath` passes `-R path` to `pkgadd` command. |
| -rsh | Specify this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.<br>See "About configuring secure shell or remote shell communication modes before installing products" on page 467. |

**Table A-1** Available command line options *(continued)*

| Commandline Option | Function |
|---|---|
| –serial | Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems. |
| -settunables | Specify this option when you want to set tunable parameters after you install and configure a product. You may need to restart processes of the product for the tunable parameter values to take effect. You must use this option together with the `-tunablesfile` option. |
| -start | Starts the daemons and processes for the specified product. |
| -stop | Stops the daemons and processes for the specified product. |
| -timeout | The `-timeout` option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the `-timeout` option overrides the default value of 1200 seconds. Setting the `-timeout` option to 0 prevents the script from timing out. The `-timeout` option does not work with the `-serial` option |
| –tmppath *tmp_path* | Specifies a directory other than `/var/tmp` as the working directory for the installation scripts. This destination is where initial logging is performed and where packages are copied on remote systems before installation. |
| -tunables | Lists all supported tunables and create a tunables file template. |
| -tunables_file *tunables_file* | Specify this option when you specify a tunables file. The tunables file should include tunable parameters. |
| -upgrade | Specifies that an existing version of the product exists and you plan to upgrade it. |

**Table A-1** Available command line options *(continued)*

| Commandline Option | Function |
|---|---|
| -upgrade_kernelpkgs | The `-upgrade_kernelpkgs` option has been renamed to `-rollingupgrade_phase1`. |
| -upgrade_nonkernelpkgs | The `-upgrade_nonkernelpkgs` option has been renamed to `-rollingupgrade_phase2`. |
| -version | Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available. |

# About using the postcheck option

You can use the installer's post-check to determine installation-related problems and to aid in troubleshooting.

**Note:** This command option requires downtime for the node.

When you use the `postcheck` option, it can help you troubleshoot the following VCS-related issues:

- The heartbeat link does not exist.
- The heartbeat link cannot communicate.
- The heartbeat link is a part of a bonded or aggregated NIC.
- A duplicated cluster ID exists (if LLT is not running at the check time).
- The VRTSllt pkg version is not consistent on the nodes.
- The llt-linkinstall value is incorrect.
- The llthosts(4) or lltttab(4) configuration is incorrect.
- the `/etc/gabtab` file is incorrect.
- The incorrect GAB linkinstall value exists.
- The VRTSgab pkg version is not consistent on the nodes.

- The `main.cf` file or the `types.cf` file is invalid.
- The `/etc/VRTSvcs/conf/sysname` file is not consistent with the hostname.
- The cluster UUID does not exist.
- The `uuidconfig.pl` file is missing.
- The VRTSvcs pkg version is not consistent on the nodes.
- The `/etc/vxfenmode` file is missing or incorrect.
- The `/etc/vxfendg file` is invalid.
- The vxfen link-install value is incorrect.
- The VRTSvxfen pkg version is not consistent.

The `postcheck` option can help you troubleshoot the following SFHA or SFCFSHA issues:

- Volume Manager cannot start because the `/etc/vx/reconfig.d/state.d/install-db` file has not been removed.
- Volume Manager cannot start because the `volboot` file is not loaded.
- Volume Manager cannot start because no license exists.
- Cluster Volume Manager cannot start because the CVM configuration is incorrect in the `main.cf` file. For example, the Autostartlist value is missing on the nodes.
- Cluster Volume Manager cannot come online because the node ID in the `/etc/llthosts` file is not consistent.
- Cluster Volume Manager cannot come online because Vxfen is not started.
- Cluster Volume Manager cannot start because gab is not configured.
- Cluster Volume Manager cannot come online because of a CVM protocol mismatch.
- Cluster Volume Manager group name has changed from "cvm", which causes CVM to go offline.

You can use the installer's post-check option to perform the following checks:

General checks for all products:

- All the required packages are installed.
- The versions of the required packages are correct.
- There are no verification issues for the required packages.

Checks for Volume Manager (VM):

- Lists the daemons which are not running (`vxattachd`, `vxconfigbackupd`, `vxesd`, `vxrelocd` ...).
- Lists the disks which are not in 'online' or 'online shared' state (`vxdisk list`).
- Lists the diskgroups which are not in 'enabled' state (`vxdg list`).
- Lists the volumes which are not in 'enabled' state (`vxprint -g <dgname>`).
- Lists the volumes which are in 'Unstartable' state (`vxinfo -g <dgname>`).
- Lists the volumes which are not configured in `(AIX) /etc/filesystems`, `(Linux/HP-UX)/etc/fstab`, or `(SunOS)/etc/vfstab`.

Checks for File System (FS):

- Lists the VxFS kernel modules which are not loaded (`vxfs/fdd/vxportal`.).
- Whether all VxFS file systems present in `(AIX) /etc/filesystems`, `(Linux/HP-UX)/etc/fstab`, or `(SunOS)/etc/vfstab` file are mounted.
- Whether all VxFS file systems present in `(AIX) /etc/filesystems`, `(Linux/HP-UX)/etc/fstab`, or `(SunOS)/etc/vfstab` are in disk layout 6 or higher.
- Whether all mounted VxFS file systems are in disk layout 6 or higher.

Checks for Cluster File System:

- Whether FS and ODM are running at the latest protocol level.
- Whether all mounted CFS file systems are managed by VCS.
- Whether cvm service group is online.

See "Performing a postcheck on a node" on page 343.

Appendix B

# Tunable files for installation

This appendix includes the following topics:


- About setting tunable parameters using the installer or a response file
- Setting tunables for an installation, configuration, or upgrade
- Setting tunables with no other installer-related operations
- Setting tunables with an un-integrated response file
- Preparing the tunables file
- Setting parameters for the tunables file
- Tunables value parameter definitions


## About setting tunable parameters using the installer or a response file

You can set non-default product and system tunable parameters using a tunables file. With the file, you can set tunables such as the I/O policy or toggle native multi-pathing. The tunables file passes arguments to the installer script to set tunables. With the file, you can set the tunables for the following operations:

- When you install, configure, or upgrade systems.

  ```
  # ./installer -tunablesfile tunables_file_name
  ```

  See "Setting tunables for an installation, configuration, or upgrade" on page 438.

- When you apply the tunables file with no other installer-related operations.

  ```
  # ./installer -tunablesfile tunables_file_name -settunables [
  system1 system2 ...]
  ```

See "Setting tunables with no other installer-related operations" on page 439.

- When you apply the tunables file with an un-integrated response file.

  ```
  # ./installer -responsefile response_file_name -tunablesfile
  tunables_file_name
  ```

  See "Setting tunables with an un-integrated response file" on page 440.

See "About response files" on page 43.

You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 442.

# Setting tunables for an installation, configuration, or upgrade

You can use a tunables file for installation procedures to set non-default tunables. You invoke the installation script with the `tunablesfile` option. The tunables file passes arguments to the script to set the selected tunables. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 442.

---

**Note:** Certain tunables only take effect after a system reboot.

---

**To set the non-default tunables for an installation, configuration, or upgrade**

1. Prepare the tunables file.

   See "Preparing the tunables file" on page 441.

2. Make sure the systems where you want to install SFCFSHA meet the installation requirements.

3. Complete any preinstallation tasks.

4. Copy the tunables file to one of the systems where you want to install, configure, or upgrade the product.

5. Mount the product disc and navigate to the directory that contains the installation program.

6. Start the installer for the installation, configuration, or upgrade. For example:

   ```
   # ./installer -tunablesfile /tmp/tunables_file
   ```

   Where /tmp/*tunables_file* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

# Setting tunables with no other installer-related operations

You can use the installer to set tunable parameters without any other installer-related operations. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 442.

**Note:** Certain tunables only take effect after a system reboot.

**To set tunables with no other installer-related operations**

1 Prepare the tunables file.

See "Preparing the tunables file" on page 441.

2 Make sure the systems where you want to install SFCFSHA meet the installation requirements.

3 Complete any preinstallation tasks.

4 Copy the tunables file to one of the systems that you want to tune.

5 Mount the product disc and navigate to the directory that contains the installation program.

6 Start the installer with the `-settunables` option.

```
# ./installer -tunablesfile tunables_file_name -settunables [
sys123 sys234 ...]
```

Where /tmp/*tunables_file* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

# Setting tunables with an un-integrated response file

You can use the installer to set tunable parameters with an un-integrated response file. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 442.

**Note:** Certain tunables only take effect after a system reboot.

**To set tunables with an un-integrated response file**

1 Make sure the systems where you want to install SFCFSHA meet the installation requirements.

2 Complete any preinstallation tasks.

3 Prepare the tunables file.

See "Preparing the tunables file" on page 441.

4 Copy the tunables file to one of the systems that you want to tune.

5 Mount the product disc and navigate to the directory that contains the installation program.

6 Start the installer with the `-responsefile` and `-tunablesfile` options.

```
# ./installer -responsefile response_file_name -tunablesfile
tunables_file_name
```

Where *response_file_name* is the full path name for the response file and *tunables_file_name* is the full path name for the tunables file.

7 Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

# Preparing the tunables file

A tunables file is a Perl module and consists of an opening and closing statement, with the tunables defined between. Use the hash symbol at the beginning of the line to comment out the line. The tunables file opens with the line "our %TUN;" and ends with the return true "1;" line. The final return true line only needs to appear once at the end of the file. Define each tunable parameter on its own line.

You can use the installer to create a tunables file template, or manually format tunables files you create.

**To create a tunables file template**

- Start the installer with the `-tunables` option. Enter the following:

  ```
  # ./installer -tunables
  ```

  You see a list of all supported tunables, and the location of the tunables file template.

**To manually format tunables files**

- Format the tunable parameter as follows:

  ```
  $TUN{"tunable_name"}{"system_name"|"*"}=value_of_tunable;
  ```

For the *system_name*, use the name of the system, its IP address, or a wildcard symbol. The *value_of_tunable* depends on the type of tunable you are setting. End the line with a semicolon.

The following is an example of a tunables file.

```
#
# Tunable Parameter Values:
#
our %TUN;

$TUN{"tunable1"}{"*"}=1024;
$TUN{"tunable3"}{"sys123"}="SHA256";

1;
```

# Setting parameters for the tunables file

Each tunables file defines different tunable parameters. The values that you can use are listed in the description of each parameter. Select the tunables that you want to add to the tunables file and then configure each parameter.

See "Tunables value parameter definitions" on page 442.

Each line for the parameter value starts with $TUN. The name of the tunable is in curly brackets and double-quotes. The system name is enclosed in curly brackets and double-quotes. Finally define the value and end the line with a semicolon, for example:

```
$TUN{"dmp_daemon_count"}{"node123"}=16;
```

In this example, you are changing the dmp_daemon_count value from its default of 10 to 16. You can use the wildcard symbol "*" for all systems. For example:

```
$TUN{"dmp_daemon_count"}{"*"}=16;
```

# Tunables value parameter definitions

When you create a tunables file for the installer you can only use the parameters in the following list.

Prior to making any updates to the tunables, refer to the *Veritas Storage Foundation and High Availability Solutions Tuning Guide* for detailed information on product tunable ranges and recommendations .

Table B-1 describes the supported tunable parameters that can be specified in a tunables file.

**Table B-1** Supported tunable parameters

| Tunable | Description |
|---|---|
| dmp_cache_open | (Veritas Dynamic Multi-Pathing) Whether the first open on a device performed by an array support library (ASL) is cached. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_daemon_count | (Veritas Dynamic Multi-Pathing) The number of kernel threads for DMP administrative tasks. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_delayq_interval | (Veritas Dynamic Multi-Pathing) The time interval for which DMP delays the error processing if the device is busy. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_fast_recovery | (Veritas Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |

**Table B-1** Supported tunable parameters *(continued)*

| Tunable | Description |
|---|---|
| dmp_health_time | (Veritas Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_log_level | (Veritas Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_low_impact_probe | (Veritas Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_lun_retry_timeout | (Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_monitor_fabric | (Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_monitor_osevent | (Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_monitor_ownership | (Veritas Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_native_multipathing | (Veritas Dynamic Multi-Pathing) Whether DMP will intercept the I/Os directly on the raw OS paths or not. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_native_support | (Veritas Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_path_age | (Veritas Dynamic Multi-Pathing) The time for which an intermittently failing path needs to be monitored before DMP marks it as healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |

**Table B-1** Supported tunable parameters *(continued)*

| Tunable | Description |
|---|---|
| dmp_pathswitch_blks_shift | (Veritas Dynamic Multi-Pathing) The default number of contiguous I/O blocks sent along a DMP path to an array before switching to the next available path. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_probe_idle_lun | (Veritas Dynamic Multi-Pathing) Whether the path restoration kernel thread probes idle LUNs. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_probe_threshold | (Veritas Dynamic Multi-Pathing) The number of paths will be probed by the restore daemon. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_restore_cycles | (Veritas Dynamic Multi-Pathing) The number of cycles between running the check_all policy when the restore policy is check_periodic. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_restore_interval | (Veritas Dynamic Multi-Pathing) The time interval in seconds the restore daemon analyzes the condition of paths. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_restore_policy | (Veritas Dynamic Multi-Pathing) The policy used by DMP path restoration thread. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_restore_state | (Veritas Dynamic Multi-Pathing) Whether kernel thread for DMP path restoration is started. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_retry_count | (Veritas Dynamic Multi-Pathing) The number of times a path reports a path busy error consecutively before DMP marks the path as failed. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_scsi_timeout | (Veritas Dynamic Multi-Pathing) The timeout value for any SCSI command sent via DMP. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| dmp_sfg_threshold | (Veritas Dynamic Multi-Pathing) The status of the subpaths failover group (SFG) feature. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |

**Table B-1** Supported tunable parameters *(continued)*

| Tunable | Description |
|---|---|
| dmp_stat_interval | (Veritas Dynamic Multi-Pathing) The time interval between gathering DMP statistics. This tunable must be set after Veritas Dynamic Multi-Pathing is started. |
| max_diskq | (Veritas File System) Specifies the maximum disk queue generated by a single file. The installer sets only the system default value of max_diskq. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |
| read_ahead | (Veritas File System) The 0 value disables read ahead functionality, the 1 value (default) retains traditional sequential read ahead behavior, and the 2 value enables enhanced read ahead for all reads. The installer sets only the system default value of read_ahead. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |
| read_nstream | (Veritas File System) The number of parallel read requests of size read_pref_io that can be outstanding at one time. The installer sets only the system default value of read_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |
| read_pref_io | (Veritas File System) The preferred read request size. The installer sets only the system default value of read_pref_io. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |
| vol_checkpt_default | (Veritas File System) Size of VxVM storage checkpoints (sectors). This tunable requires system reboot to take effect. |
| vol_cmpres_enabled | (Veritas Volume Manager) Allow enabling compression for VERITAS Volume Replicator. |
| vol_cmpres_threads | (Veritas Volume Manager) Maximum number of compression threads for VERITAS Volume Replicator. |
| vol_default_iodelay | (Veritas Volume Manager) Time to pause between I/O requests from VxVM utilities (10ms units). This tunable requires system reboot to take effect. |

**Table B-1** Supported tunable parameters *(continued)*

| Tunable | Description |
|---|---|
| vol_fmr_logsz | (Veritas Volume Manager) Maximum size of bitmap Fast Mirror Resync uses to track changed blocks (KBytes). This tunable requires system reboot to take effect. |
| vol_max_adminio_poolsz | (Veritas Volume Manager) Maximum amount of memory used by VxVM admin I/O's (bytes). This tunablle rquires system reboot to take effect. |
| vol_max_nmpool_sz | (Veritas Volume Manager) Maximum name pool size (bytes). |
| vol_max_rdback_sz | (Veritas Volume Manager) Storage Record readback pool maximum (bytes). |
| vol_max_wrspool_sz | (Veritas Volume Manager) Maximum memory used in clustered version of VERITAS Volume Replicator (bytes). |
| vol_maxio | (Veritas Volume Manager) Maximum size of logical VxVM I/O operations (sectors). This tunable requires system reboot to take effect. |
| vol_maxioctl | (Veritas Volume Manager) Maximum size of data passed into the VxVM ioctl calls (bytes). This tunable requires system reboot to take effect. |
| vol_maxparallelio | (Veritas Volume Manager) Number of I/O operations vxconfigd can request at one time. This tunable requires system reboot to take effect. |
| vol_maxspecialio | (Veritas Volume Manager) Maximum size of a VxVM I/O operation issued by an ioctl call (sectors). This tunable requires system reboot to take effect. |
| vol_min_lowmem_sz | (Veritas Volume Manager) Low water mark for memory (bytes). |
| vol_nm_hb_timeout | (Veritas Volume Manager) Veritas Volume Replicator timeout value (ticks). |
| vol_rvio_maxpool_sz | (Veritas Volume Manager) Maximum memory requested by VERITAS Volume Replicator (bytes). |
| vol_stats_enable | (Veritas Volume Manager) Enable VxVM I/O stat collection. |

**Table B-1** Supported tunable parameters *(continued)*

| Tunable | Description |
|---|---|
| vol_subdisk_num | (Veritas Volume Manager) Maximum number of subdisks attached to a single VxVM plex. This tunable requires system reboot to take effect. |
| voldrl_max_drtregs | (Veritas Volume Manager) Maximum number of dirty VxVM regions that can exist on a non-sequential DRL. This tunable requires system reboot to take effect. |
| voldrl_max_seq_dirty | (Veritas Volume Manager) Maximum number of dirty regions in sequential mode. This tunable requires system reboot to take effect. |
| voldrl_min_regionsz | (Veritas Volume Manager) Minimum size of a VxVM Dirty Region Logging (DRL) region (sectors). This tunable requires system reboot to take effect. |
| voldrl_volumemax_drtregs | (Veritas Volume Manager) Max per volume dirty regions in log-plex DRL. |
| voldrl_volumemax_drtregs_20 | (Veritas Volume Manager) Max per volume dirty regions in DCO version 20. |
| voldrl_dirty_regions | (Veritas Volume Manager) Number of regions cached for DCO version 30. |
| voliomem_chunk_size | (Veritas Volume Manager) Size of VxVM memory allocation requests (bytes). This tunable requires system reboot to take effect. |
| voliomem_maxpool_sz | (Veritas Volume Manager) Maximum amount of memory used by VxVM (bytes). This tunable requires system reboot to take effect. |
| voliot_errbuf_dflt | (Veritas Volume Manager) Size of a VxVM error trace buffer (bytes). This tunable requires system reboot to take effect. |
| voliot_iobuf_default | (Veritas Volume Manager) Default size of a VxVM I/O trace buffer (bytes). This tunable requires system reboot to take effect. |
| voliot_iobuf_limit | (Veritas Volume Manager) Maximum total size of all VxVM I/O trace buffers (bytes). This tunable requires system reboot to take effect. |

**Table B-1** Supported tunable parameters *(continued)*

| Tunable | Description |
|---|---|
| voliot_iobuf_max | (Veritas Volume Manager) Maximum size of a VxVM I/O trace buffer (bytes). This tunable requires system reboot to take effect. |
| voliot_max_open | (Veritas Volume Manager) Maximum number of VxVM trace channels available for vxtrace commands. This tunable requires system reboot to take effect. |
| volpagemod_max_memsz | (Veritas Volume Manager) Maximum paging module memory used by Instant Snapshots (Kbytes). |
| volraid_rsrtransmax | (Veritas Volume Manager) Maximum number of VxVM RAID-5 transient reconstruct operations in parallel. This tunable requires system reboot to take effect. |
| vx_era_nthreads | (Veritas File System) Maximum number of threads VxFS will detect read_ahead patterns on. This tunable requires system reboot to take effect. |
| vx_bc_bufhwm | (Veritas File System) VxFS metadata buffer cache high water mark. This tunable requires system reboot to take effect. |
| vxfs_ninode | (Veritas File System) Number of entries in the VxFS inode table. This tunable requires system reboot to take effect. |
| write_nstream | (Veritas File System) The number of parallel write requests of size write_pref_io that can be outstanding at one time. The installer sets only the system default value of write_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |
| write_pref_io | (Veritas File System) The preferred write request size. The installer sets only the system default value of write_pref_io. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |

Appendix C

# Configuration files

This appendix includes the following topics:


- About the LLT and GAB configuration files
- About the AMF 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/lltab files. GAB requires /etc/gabtab file.

Table C-1 lists the LLT configuration files and the information that these files contain.

**Table C-1** LLT configuration files

| File | Description |
|---|---|
| /etc/default/llt | This file stores the start and stop environment variables for LLT:<br>■ LLT_START—Defines the startup behavior for the LLT module after a system reboot. Valid values include:<br>1—Indicates that LLT is enabled to start up.<br>0—Indicates that LLT is disabled to start up.<br>■ LLT_STOP—Defines the shutdown behavior for the LLT module during a system shutdown. Valid values include:<br>1—Indicates that LLT is enabled to shut down.<br>0—Indicates that LLT is disabled to shut down.<br>The installer sets the value of these variables to 1 at the end of SFCFSHA configuration. |

**Table C-1** LLT configuration files *(continued)*

| File | Description |
|---|---|
| /etc/llthosts | The file `llthosts` is a database that contains one entry per system. This file links the LLT system ID (in the first column) with the LLT host name. This file must be identical on each node in the cluster. A mismatch of the contents of the file can cause indeterminate behavior in the cluster.<br>For example, the file /etc/llthosts contains the entries that resemble:<br>`0 sys1`<br>`1 sys2` |
| /etc/lltab | The file `lltab` contains the information that is derived during installation and used by the utility `lltconfig(1M)`. After installation, this file lists the private network links that correspond to the specific system. For example, the file /etc/lltab contains the entries that resemble the following:<br>■ For Solaris SPARC:<br>`set-node sys1`<br>`set-cluster 2`<br>`link bge0 /dev/bge0 - ether - -`<br>`link bge1 /dev/bge1 - ether - -`<br>■ For Solaris x64:<br>`set-node sys1`<br>`set-cluster 2`<br>`link e1000g1 /dev/e1000g:1 - ether - -`<br>`link e1000g2 /dev/e1000g:2 - ether - -`<br>The first line identifies the system. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines begin with the `link` command. These lines identify the two network cards that the LLT protocol uses.<br>If you configured a low priority link under LLT, the file also includes a "link-lowpri" line.<br>Refer to the `lltab(4)` manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the `lltab` file. |

Table C-2 lists the GAB configuration files and the information that these files contain.

**Table C-2** GAB configuration files

| File | Description |
|---|---|
| /etc/default/gab | This file stores the start and stop environment variables for GAB:<br>■ GAB_START—Defines the startup behavior for the GAB module after a system reboot. Valid values include:<br>1—Indicates that GAB is enabled to start up.<br>0—Indicates that GAB is disabled to start up.<br>■ GAB_STOP—Defines the shutdown behavior for the GAB module during a system shutdown. Valid values include:<br>1—Indicates that GAB is enabled to shut down.<br>0—Indicates that GAB is disabled to shut down.<br>The installer sets the value of these variables to 1 at the end of SFCFSHA configuration. |
| /etc/gabtab | After you install SFCFSHA, the file /etc/gabtab contains a `gabconfig(1)` command that configures the GAB driver for use.<br>The file /etc/gabtab contains a line that resembles:<br>`/sbin/gabconfig -c -nN`<br>The `-c` option configures the driver for use. The `-nN` specifies that the cluster is not formed until at least *N* nodes are ready to form the cluster. Symantec recommends that you set N to be the total number of nodes in the cluster.<br>**Note:** Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`. Using `-c -x` can lead to a split-brain condition. Use the `-c` option for `/sbin/gabconfig` to avoid a split-brain condition.<br>**Note:** |

# 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 C-3 lists the AMF configuration files.

**Table C-3** AMF configuration files

| File | Description |
|---|---|
| /etc/default/amf | This file stores the start and stop environment variables for AMF:<br>■ 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:<br>1—Indicates that AMF is enabled to start up. (default)<br>0—Indicates that AMF is disabled to start up.<br>■ 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:<br>1—Indicates that AMF is enabled to shut down. (default)<br>0—Indicates that AMF is disabled to shut down. |
| /etc/amftab | After you install VCS, the file `/etc/amftab` contains a `amfconfig`(1) command that configures the AMF driver for use.<br>The AMF init script uses this `/etc/amftab` file to configure the AMF driver. The `/etc/amftab` file contains the following line by default:<br>`/opt/VRTSamf/bin/amfconfig -c` |

# About I/O fencing configuration files

Table C-4 lists the I/O fencing configuration files.

**Table C-4** I/O fencing configuration files

| File | Description |
|---|---|
| /etc/default/vxfen | This file stores the start and stop environment variables for I/O fencing:<br>■ VXFEN_START—Defines the startup behavior for the I/O fencing module after a system reboot. Valid values include:<br>1—Indicates that I/O fencing is enabled to start up.<br>0—Indicates that I/O fencing is disabled to start up.<br>■ VXFEN_STOP—Defines the shutdown behavior for the I/O fencing module during a system shutdown. Valid values include:<br>1—Indicates that I/O fencing is enabled to shut down.<br>0—Indicates that I/O fencing is disabled to shut down.<br>The installer sets the value of these variables to 1 at the end of SFCFSHA configuration. |

**Table C-4** I/O fencing configuration files *(continued)*

| File | Description |
|---|---|
| /etc/vxfendg | This file includes the coordinator disk group information.<br>This file is not applicable for server-based fencing. |
| /etc/vxfenmode | This file contains the following parameters:<br>■ `vxfen_mode`<br>  ■ scsi3—For disk-based fencing<br>  ■ customized—For server-based fencing<br>  ■ disabled—To run the I/O fencing driver but not do any fencing operations.<br>■ vxfen_mechanism<br>  This parameter is applicable only for server-based fencing. Set the value as `cps`.<br>■ scsi3_disk_policy<br>  ■ dmp—Configure the vxfen module to use DMP devices<br>  The disk policy is dmp by default. If you use iSCSI devices, you must set the disk policy as dmp.<br>  ■ raw—Configure the vxfen module to use the underlying raw character devices<br>  **Note:** You must use the same SCSI-3 disk policy on all the nodes.<br>■ security<br>  This parameter is applicable only for server-based fencing.<br>  1—Indicates that communication with the CP server is in secure mode. This setting is the default.<br>  0—Indicates that communication with the CP server is in non-secure mode.<br>■ List of coordination points<br>  This list is required only for server-based fencing configuration.<br>  Coordination points in server-based fencing can include coordinator disks, CP servers, or both. If you use coordinator disks, you must create a coordinator disk group containing the individual coordinator disks.<br>  Refer to the sample file /etc/vxfen.d/vxfenmode_cps for more information on how to specify the coordination points and multiple IP addresses for each CP server.<br>■ single_cp<br>  This parameter is applicable for server-based fencing which uses a single highly available CP server as its coordination point. Also applicable for when you use a coordinator disk group with single disk.<br>■ autoseed_gab_timeout<br>  This parameter enables GAB automatic seeding of the cluster even when some cluster nodes are unavailable. This feature requires that I/O fencing is enabled.<br>  0—Turns the GAB auto-seed feature on. Any value greater than 0 indicates the number of seconds that GAB must delay before it automatically seeds the cluster.<br>  -1—Turns the GAB auto-seed feature off. This setting is the default. |

**Table C-4** I/O fencing configuration files *(continued)*

| File | Description |
|---|---|
| /etc/vxfentab | When I/O fencing starts, the `vxfen` startup script creates this `/etc/vxfentab` file on each node. The startup script uses the contents of the /etc/vxfendg and /etc/vxfenmode files. Any time a system is rebooted, the fencing driver reinitializes the vxfentab file with the current list of all the coordinator points.<br>**Note:** The /etc/vxfentab file is a generated file; do not modify this file.<br>For disk-based I/O fencing, the /etc/vxfentab file on each node contains a list of all paths to each coordinator disk along with its unique disk identifier. A space separates the path and the unique disk identifier. An example of the /etc/vxfentab file in a disk-based fencing configuration on one node resembles as follows:<br>■ Raw disk:<br>`/dev/rdsk/c1t1d0s2 HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6 00A0B8000215A5D000006804E795D075`<br>`/dev/rdsk/c2t1d0s2 HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6 00A0B8000215A5D000006814E795D076`<br>`/dev/rdsk/c3t1d2s2 HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6 00A0B8000215A5D000006824E795D077`<br>■ DMP disk:<br>`/dev/vx/rdmp/c1t1d0s2 HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6 00A0B8000215A5D000006804E795D075`<br>`/dev/vx/rdmp/c2t1d0s2 HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6 00A0B8000215A5D000006814E795D076`<br>`/dev/vx/rdmp/c3t1d0s2 HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6 00A0B8000215A5D000006824E795D077`<br>For server-based fencing, the /etc/vxfentab file also includes the security settings information.<br>For server-based fencing with single CP server, the /etc/vxfentab file also includes the single_cp settings information. |

# Sample configuration files for CP server

The `/etc/vxcps.conf` file determines the configuration of the coordination point server (CP server.)

See "Sample CP server configuration (/etc/vxcps.conf) file output" on page 466.

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 "CP server hosted on a single node main.cf file" on page 455.
  See "Sample main.cf file for CP server hosted on a single node that runs VCS" on page 461.
- The main.cf file for a CP server that is hosted on an SFHA cluster:
  See "CP server hosted on an SFHA cluster main.cf file" on page 457.
  See "Sample main.cf file for CP server hosted on a two-node SFHA cluster" on page 463.

**Note:** The CP server supports Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with SFCFSHA clusters (application clusters). The example main.cf files use IPv4 addresses.

## CP server hosted on a single node main.cf file

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: cps1

```
include "types.cf"

// cluster name:  cps1
// CP server: cps1

cluster cps1 (
     UserNames = { admin = bMNfMHmJNiNNlVNhMK, haris = fopKojNvpHouNn,
             "cps1.symantecexample.com@root@vx" = aj,
             "root@cps1.symantecexample.com" = hq }
     Administrators = { admin, haris,
             "cps1.symantecexample.com@root@vx",
             "root@cps1.symantecexample.com" }
     SecureClus = 1
     HacliUserLevel = COMMANDROOT
     )

system cps1 (
     )
```

```
group CPSSG (
      SystemList = { cps1 = 0 }
      AutoStartList = { cps1 }
      )

      IP cpsvip (
            Device @cps1 = bge0
            Address = "10.209.3.1"
            NetMask = "255.255.252.0"
            )

      NIC cpsnic (
            Device @cps1 = bge0
            )

     Process vxcpserv (
           PathName = "/opt/VRTScps/bin/vxcpserv"
           ConfInterval = 30
           RestartLimit = 3
           )

 cpsvip requires cpsnic
 vxcpserv requires cpsvip


 // resource dependency tree
 //
 // group CPSSG
 // {
 // Process vxcpserv
 //     {
 //     IP cpsvip
 //         {
 //         NIC cpsnic
 //         }
 //     }
 // }


group VxSS (
      SystemList = { cps1 = 0 }
      Parallel = 1
```

```
        AutoStartList = { cps1 }
        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
 //    }
```

## CP server hosted on an SFHA cluster main.cf file

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: cps1, cps2

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"


// cluster: cps1
// CP servers:
// cps1
// cps2

cluster cps1 (
```

```
        UserNames = { admin = ajkCjeJgkFkkIskEjh,
                "cps1.symantecexample.com@root@vx" = JK,
                "cps2.symantecexample.com@root@vx" = dl }
        Administrators = { admin, "cps1.symantecexample.com@root@vx",
                "cps2.symantecexample.com@root@vx" }
        SecureClus = 1
        )

system cps1 (
        )

system cps2 (
        )

group CPSSG (
        SystemList = { cps1 = 0, cps2 = 1 }
        AutoStartList = { cps1, cps2 } )

        DiskGroup cpsdg (
                DiskGroup = cps_dg
                )

        IP cpsvip (
                Device @cps1 = bge0
                Device @cps2 = bge0
                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 @cps1 = bge0
                Device @cps2 = bge0
                )

        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 = { cps1 = 0, cps2 = 1 }
      Parallel = 1
      AutoStartList = { cps1, cps2 }
      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
 // }


group cvm (
        SystemList = { cps1 = 0, cps2 = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { cps1, cps2 }
        )

        CFSfsckd vxfsckd (
        )

        CVMCluster cvm_clus (
                CVMClustName = cpsl
                CVMNodeId = { cps1 = 0, cps2 = 1 }
                CVMTransport = gab
                CVMTimeout = 200
                )

        CVMVxconfigd cvm_vxconfigd (
                Critical = 0
                CVMVxconfigdArgs = { syslog }
                )

 cvm_clus requires cvm_vxconfigd
 vxfsckd requires cvm_clus
```

```
// resource dependency tree
//
// group cvm
// {
// CFSfsckd vxfsckd
//     {
//     CVMCluster cvm_clus
//         {
//         CVMVxconfigd cvm_vxconfigd
//         }
//     }
// }
```

## 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: cps1

```
include "types.cf"
include "/opt/VRTScps/bin/Quorum/QuorumTypes.cf"

// cluster name:  cps1
// CP server: cps1

cluster cps1 (
     UserNames = { admin = bMNfMHmJNiNNlVNhMK, haris = fopKojNvpHouNn,
             "cps1.symantecexample.com@root@vx" = aj,
             "root@cps1.symantecexample.com" = hq }
     Administrators = { admin, haris,
             "cps1.symantecexample.com@root@vx",
             "root@cps1.symantecexample.com" }
     SecureClus = 1
     HacliUserLevel = COMMANDROOT
     )
```

```
system cps1 (
     )

group CPSSG (
      SystemList = { cps1 = 0 }
      AutoStartList = { cps1 }
      )

      IP cpsvip1 (
            Critical = 0
            Device @cps1 = bge0
            Address = "10.209.3.1"
            NetMask = "255.255.252.0"
            )

      IP cpsvip2 (
            Critical = 0
            Device @cps1 = bge1
            Address = "10.209.3.2"
            NetMask = "255.255.252.0"
            )

      NIC cpsnic1 (
           Critical = 0
           Device @cps1 = bge0
           PingOptimize = 0
           NetworkHosts @cps1 = { "10.209.3.10 }
           )

      NIC cpsnic2 (
           Critical = 0
           Device @cps1 = bge1
           PingOptimize = 0
           )

      Process vxcpserv (
           PathName = "/opt/VRTScps/bin/vxcpserv"
           ConfInterval = 30
           RestartLimit = 3
           )

      Quorum quorum (
```

```
            QuorumResources = { cpsvip1, cpsvip2 }
            )

cpsvip1 requires cpsnic1
cpsvip2 requires cpsnic2
vxcpserv requires quorum


// resource dependency tree
//
// group CPSSG
// {
// IP cpsvip1
//     {
//     NIC cpsnic1
//     }
// IP cpsvip2
//     {
//     NIC cpsnic2
//     }
// Process vxcpserv
//     {
//     Quorum quorum
//     }
// }
```

## 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: cps1, cps2

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "/opt/VRTScps/bin/Quorum/QuorumTypes.cf"


// cluster: cps1
// CP servers:
```

```
// cps1
// cps2

cluster cps1 (
     UserNames = { admin = ajkCjeJgkFkkIskEjh,
            "cps1.symantecexample.com@root@vx" = JK,
            "cps2.symantecexample.com@root@vx" = dl }
     Administrators = { admin, "cps1.symantecexample.com@root@vx",
            "cps2.symantecexample.com@root@vx" }
     SecureClus = 1
     )

system cps1 (
     )

system cps2 (
     )

group CPSSG (
      SystemList = { cps1 = 0, cps2 = 1 }
      AutoStartList = { cps1, cps2 } )

      DiskGroup cpsdg (
            DiskGroup = cps_dg
            )

      IP cpsvip1 (
            Critical = 0
            Device @cps1 = bge0
            Device @cps2 = bge0
            Address = "10.209.81.88"
            NetMask = "255.255.252.0"
            )

      IP cpsvip2 (
            Critical = 0
            Device @cps1 = bge1
            Device @cps2 = bge1
            Address = "10.209.81.89"
            NetMask = "255.255.252.0"
            )

      Mount cpsmount (
```

```
            MountPoint = "/etc/VRTScps/db"
            BlockDevice = "/dev/vx/dsk/cps_dg/cps_volume"
            FSType = vxfs
            FsckOpt = "-y"
            )

      NIC cpsnic1 (
            Critical = 0
            Device @cps1 = bge0
            Device @cps2 = bge0
            PingOptimize = 0
            NetworkHosts @cps1 = { "10.209.81.10 }
            )

      NIC cpsnic2 (
            Critical = 0
            Device @cps1 = bge1
            Device @cps2 = bge1
            PingOptimize = 0
            )

      Process vxcpserv (
             PathName = "/opt/VRTScps/bin/vxcpserv"
             )

      Quorum quorum (
             QuorumResources = { cpsvip1, cpsvip2 }
             )

      Volume cpsvol (
             Volume = cps_volume
             DiskGroup = cps_dg
             )

cpsmount requires cpsvol
cpsvip1 requires cpsnic1
cpsvip2 requires cpsnic2
cpsvol requires cpsdg
vxcpserv requires cpsmount
vxcpserv requires quorum


// resource dependency tree
```

```
//
// group CPSSG
// {
// IP cpsvip1
//     {
//     NIC cpsnic1
//     }
// IP cpsvip2
//     {
//     NIC cpsnic2
//     }
// Process vxcpserv
//     {
//     Quorum quorum
//     Mount cpsmount
//         {
//         Volume cpsvol
//             {
//             DiskGroup cpsdg
//             }
//         }
//     }
// }
```

## Sample CP server configuration (/etc/vxcps.conf) file output

The following is an example of a coordination point server (CP server) configuration file `/etc/vxcps.conf` output.

```
##  The vxcps.conf file determines the
## configuration for Veritas CP Server.
cps_name=cps1
vip=[10.209.81.88]
vip=[10.209.81.89]:56789
port=14250
security=1
db=/etc/VRTScps/db
```

Appendix D

# Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:


- About configuring secure shell or remote shell communication modes before installing products
- Manually configuring and passwordless ssh
- Restarting the ssh session
- Enabling and disabling rsh for Solaris


## About configuring secure shell or remote shell communication modes before installing products

Establishing communication between nodes is required to install Veritas software from a remote system, or to install and configure a cluster. The node from which the installer is run must have permissions to run `rsh` (remote shell) or `ssh` (secure shell) utilities. You need to run the installer with superuser privileges on the systems where you plan to install Veritas software.

You can install products to remote systems using either secure shell (ssh) or remote shell (rsh). Symantec recommends that you use ssh as it is more secure than rsh.

This section contains an example of how to set up ssh password free communication. The example sets up ssh between a source system (system1) that contains the installation directories, and a target system (system2). This procedure also applies to multiple target systems.

**Note:** The script- and Web-based installers support establishing passwordless communication for you.

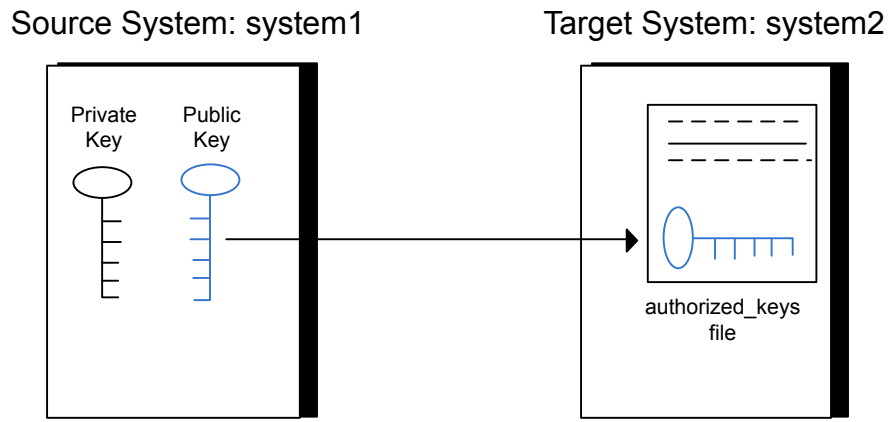
# Manually configuring and passwordless ssh

The ssh program enables you to log into and execute commands on a remote system. ssh enables encrypted communications and an authentication process between two untrusted hosts over an insecure network.

In this procedure, you first create a DSA key pair. From the key pair, you append the public key from the source system to the authorized_keys file on the target systems.

Figure D-1 illustrates this procedure.

**Figure D-1** Creating the DSA key pair and appending it to target systems




Read the ssh documentation and online manual pages before enabling ssh. Contact your operating system support provider for issues regarding ssh configuration.

Visit the OpenSSH website that is located at: http://openssh.org to access online manuals and other resources.

**To create the DSA key pair**

1 On the source system (system1), log in as root, and navigate to the root directory.

```
system1 # cd /
```

2 Make sure the `/.ssh` directory is on all the target installation systems (system2 in this example). If that directory is not present, create it on all the target systems and set the write permission to root only:

Solaris 10:

```
system2 # mkdir /.ssh
```

Solaris 11:

```
system2 # mkdir /root/.ssh
```

Change the permissions of this directory, to secure it.

Solaris 10:

```
system2 # chmod go-w /.ssh
```

Solaris 11:

```
system2 # chmod go-w /root/.ssh
```

3 To generate a DSA key pair on the source system, type the following command:

```
system1 # ssh-keygen -t dsa
```

System output similar to the following is displayed:

```
Generating public/private dsa key pair.
Enter file in which to save the key (//.ssh/id_dsa):
```

For Solaris 11:

```
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
```

4 Press Enter to accept the default location of `/.ssh/id_dsa`.

5 When the program asks you to enter the passphrase, press the Enter key twice.

```
Enter passphrase (empty for no passphrase):
```

Do not enter a passphrase. Press Enter.

```
Enter same passphrase again:
```

Press Enter again.

**To append the public key from the source system to the authorized_keys file on the target system, using secure file transfer**

1 Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems (system2 in this example).

To enable SFTP, the `/etc/ssh/sshd_config` file must contain the following two lines:

```
PermitRootLogin           yes
  Subsystem          sftp      /usr/lib/ssh/sftp-server
```

2 If the lines are not there, add them and restart ssh.

To restart ssh on Solaris 10 and Solaris 11, type the following command:

```
system1 # svcadm restart ssh
```

3 From the source system (system1), move the public key to a temporary file on the target system (system2).

Use the secure file transfer program.

In this example, the file name `id_dsa.pub` in the root directory is the name for the temporary file for the public key.

Use the following command for secure file transfer:

```
system1 # sftp system2
```

If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

```
Connecting to system2 ...
The authenticity of host 'system2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

4 Enter `yes`.

Output similar to the following is displayed:

```
Warning: Permanently added 'system2,10.182.00.00'
(DSA) to the list of known hosts.
root@system2 password:
```

5 Enter the root password of system2.

6 At the `sftp` prompt, type the following command:

```
sftp> put /.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /.ssh/id_dsa.pub to /id_dsa.pub
```

7 To quit the SFTP session, type the following command:

```
sftp> quit
```

8 To begin the `ssh` session on the target system (system2 in this example), type the following command on system1:

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

9 After you log in to system2, enter the following command to append the `id_dsa.pub` file to the `authorized_keys` file:

```
system2 # cat /id_dsa.pub >> /.ssh/authorized_keys
```

10 After the `id_dsa.pub` public key file is copied to the target system (system2), and added to the authorized keys file, delete it. To delete the `id_dsa.pub` public key file, enter the following command on system2:

```
system2 # rm /id_dsa.pub
```

11 To log out of the `ssh` session, enter the following command:

```
system2 # exit
```

12 When you install from a source system that is also an installation target, also add the local system `id_dsa.pub` key to the local `authorized_keys` file. The installation can fail if the installation source system is not authenticated.

To add the local system `id_dsa.pub` key to the local `authorized_keys` file, enter the following command:

```
system1 # cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys
```

13 Run the following commands on the source installation system. If your ssh session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and make the key globally available to the user `root`:

```
system1 # exec /usr/bin/ssh-agent $SHELL
system1 # ssh-add

  Identity added: //.ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

**To verify that you can connect to a target system**

1 On the source system (system1), enter the following command:

```
system1 # ssh -l root system2 uname -a
```

where system2 is the name of the target system.

2 The command should execute from the source system (system1) to the target system (system2) without the system requesting a passphrase or password.

3 Repeat this procedure for each target system.

# Restarting the ssh session

After you complete this procedure, ssh can be restarted in any of the following scenarios:

- After a terminal session is closed
- After a new terminal session is opened
- After a system is restarted
- After too much time has elapsed, to refresh ssh

**To restart ssh**

1 On the source installation system (system1), bring the private key into the shell environment.

```
system1 # exec /usr/bin/ssh-agent $SHELL
```

2 Make the key globally available for the user `root`

```
system1 # ssh-add
```

# Enabling and disabling rsh for Solaris

The following section describes how to enable remote shell on Solaris system.

Veritas recommends configuring a secure shell environment for Veritas product installations.

See "Manually configuring and passwordless ssh" on page 468.

See the operating system documentation for more information on configuring remote shell.

**To enable rsh**

1 To determine the current status of `rsh` and `rlogin`, type the following command:

```
# inetadm | grep -i login
```

If the service is enabled, the following line is displayed:

```
enabled online svc:/network/login:rlogin
```

If the service is not enabled, the following line is displayed:

```
disabled disabled svc:/network/login:rlogin
```

2 To enable a disabled `rsh`/`rlogin` service, type the following command:

```
# inetadm -e rlogin
```

3 To disable an enabled `rsh`/`rlogin` service, type the following command:

```
# inetadm -d rlogin
```

4 Modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. This file must be modified for each user who remotely accesses the system using rsh. Each line of the `.rhosts` file contains a fully qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access `system1` from `system2`, you must add an entry for `system2.`*`companyname`*`.com` in the `.rhosts` file on `system1`.

```
# echo "system2.companyname.com" >> $HOME/.rhosts
```

5 After you complete an installation procedure, delete the `.rhosts` file from each user's `$HOME` directory to ensure security:

```
# rm -f $HOME/.rhosts
```

Appendix E

# Storage Foundation Cluster File System High Availability components

This appendix includes the following topics:


- Veritas Storage Foundation Cluster File System High Availability installation packages
- Veritas Cluster Server installation packages
- Veritas Cluster File System installation packages
- Chinese language packages
- Japanese language packages
- Veritas Storage Foundation obsolete and reorganized installation packages


## Veritas Storage Foundation Cluster File System High Availability installation packages

Table E-1 shows the package name and contents for each English language package for Veritas Storage Foundation Cluster File System High Availability. The table also gives you guidelines for which packages to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Veritas Storage Foundation Cluster File System High Availability and Veritas Cluster Server (VCS) packages, the combined functionality is called Veritas Storage Foundation Cluster File System High Availability and High Availability.

See "Veritas Cluster Server installation packages" on page 478.

**Table E-1** Veritas Storage Foundation Cluster File System High Availability packages

| packages | Contents | Configuration |
|---|---|---|
| VRTSaslapm | Veritas Array Support Library (ASL) and Array Policy Module(APM) binaries<br>Required for the support and compatibility of various storage arrays. | Minimum |
| VRTSperl | Perl 5.14.2 for Veritas | Minimum |
| VRTSvlic | Veritas License Utilities<br>Installs the license key layout files required to decode the Storage Foundation license keys. Provides the standard license key utilities vxlicrep, vxlicinst, and vxlictest. | Minimum |
| VRTSvxfs | Veritas File System binaries<br>Required for VxFS file system support. | Minimum |
| VRTSvxvm | Veritas Volume Manager binaries, scripts, and utilities. Required for VxVM volume manager support. | Minimum |
| VRTSdbed | Veritas Storage Foundation for Databases | Recommended |
| VRTSob | Veritas Enterprise Administrator | Recommended |
| VRTSodm | Veritas ODM Driver for VxFS<br>Veritas Extension for Oracle Disk Manager is a custom storage interface designed specifically for Oracle9i and 10g. Oracle Disk Manager allows Oracle 9i and 10g to improve performance and manage system bandwidth. | Recommended |

**Table E-1** Veritas Storage Foundation Cluster File System High Availability packages *(continued)*

| packages | Contents | Configuration |
|---|---|---|
| VRTSsfcpi601 | Veritas Storage Foundation Common Product Installer<br><br>The Storage Foundation Common Product installer package contains the installer libraries and product scripts that perform the following:<br><br>■ installation<br>■ configuration<br>■ upgrade<br>■ uninstallation<br>■ adding nodes<br>■ removing nodes<br>■ etc.<br><br>You can use these script to simplify the native operating system installations, configurations, and upgrades. | Minimum |
| VRTSsfmh | Veritas Storage Foundation Managed Host<br><br>Veritas Storage Foundation Managed Host is now called Veritas Operations Manager (VOM).<br><br>Discovers configuration information on a Storage Foundation managed host. If you want a central server to manage and monitor this managed host, download and install the VRTSsfmcs package on a server, and add this managed host to the Central Server. The VRTSsfmcs package is not part of this release. You can download it separately from:<br><br>http://www.symantec.com/veritas-operations-manager | Recommended |
| VRTSspt | Veritas Software Support Tools | Recommended |
| VRTSfsadv | Minimum Veritas File System Advanced Solutions by Symantec (Solaris SPARC only). | Minimum |

**Table E-1** Veritas Storage Foundation Cluster File System High Availability packages *(continued)*

| packages | Contents | Configuration |
|---|---|---|
| VRTSfssdk | Veritas File System Software Developer Kit<br><br>For VxFS APIs, the package contains the public Software Developer Kit (headers, libraries, and sample code). It is required if some user programs use VxFS APIs. | All |

# Veritas Cluster Server installation packages

Table E-2 shows the package name and contents for each English language package for Veritas Cluster Server (VCS). The table also gives you guidelines for which packages to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Storage Foundation and VCS packages, the combined functionality is called Storage Foundation and High Availability.

See "Veritas Storage Foundation Cluster File System High Availability installation packages" on page 475.

**Table E-2** VCS installation packages

| package | Contents | Configuration |
|---|---|---|
| VRTSgab | Veritas Cluster Server group membership and atomic broadcast services | Minimum |
| VRTSllt | Veritas Cluster Server low-latency transport | Minimum |
| VRTSamf | Veritas Cluster Server Asynchronous Monitoring Framework | Minimum |
| VRTSvcs | Veritas Cluster Server | Minimum |
| VRTSvcsag | Veritas Cluster Server Bundled Agents | Minimum |
| VRTSvxfen | Veritas I/O Fencing | Minimum |
| VRTSvcsea | Consolidated database and enterprise agent packages | Recommended |

**Table E-2** VCS installation packages *(continued)*

| package | Contents | Configuration |
|---|---|---|
| VRTScps | Veritas Coordination Point Server<br><br>The Coordination Point Server is an alternate mechanism for I/O fencing. It implements I/O fencing through a client/server architecture and can provide I/O fencing for multiple VCS clusters. | All |

# Veritas Cluster File System installation packages

Table E-3 shows the package name and contents for each English language package for Veritas Cluster File System (CFS). The table also gives you guidelines for which packages to install based whether you want the minimum, recommended, or advanced configuration.

When you install all CFS packages and all the packages that comprise Storage Foundation and Veritas Cluster Server, the resulting functionality is called Storage Foundation Cluster File System.

See "Veritas Storage Foundation Cluster File System High Availability installation packages" on page 475.

See "Veritas Cluster Server installation packages" on page 478.

**Table E-3** CFS installation packages

| package | Contents | Configuration |
|---|---|---|
| VRTScavf | Veritas Cluster Server Agents for Storage Foundation Cluster File System | Minimum |
| VRTSglm | Veritas Group Lock Manager for Storage Foundation Cluster File System | Minimum |
| VRTSgms | Veritas Group Messaging Services for Storage Foundation Cluster File System | Recommended |

# Chinese language packages

The following table shows the package name and contents for each Chinese language package.

**Table E-4** Chinese language packages

| package | Contents |
|---|---|
| VRTSzhvm | Chinese Veritas Volume Manager by Symantec – Message Catalogs and Manual Pages |

# Japanese language packages

The following table show the package name and contents for each Japanese language package.

**Table E-5** Japanese language packages

| package | Contents |
|---|---|
| VRTSjacav | Japanese Veritas Cluster Server Agents for Storage Foundation Cluster File System – Manual Pages and Message Catalogs by Symantec |
| VRTSjacs | Veritas Cluster Server Japanese Message Catalogs by Symantec |
| VRTSjacse | Japanese Veritas High Availability Enterprise Agents by Symantec |
| VRTSjadba | Japanese Veritas Oracle Real Application Cluster Support package by Symantec |
| VRTSjadbe | Japanese Veritas Storage Foundation for Oracle from Symantec – Message Catalogs |
| VRTSjafs | Japanese Veritas File System – Message Catalog and Manual Pages |
| VRTSjaodm | Veritas Oracle Disk Manager Japanese Message Catalog and Manual Pages by Symantec |
| VRTSjavm | Japanese Veritas Volume Manager by Symantec – Message Catalogs and Manual Pages |
| VRTSmulic | Multi-language Symantec License Utilities |

# Veritas Storage Foundation obsolete and reorganized installation packages

Table E-6 lists the packages that are obsolete or reorganized for Veritas Storage Foundation Cluster File System High Availability.

**Table E-6** Veritas Storage Foundation obsolete and reorganized packages

| package | Description |
|---|---|
| Obsolete and reorganized for 6.0.1 | |
| VRTSat | Obsolete |
| VRTSatZH | Obsolete |
| VRTSatJA | Obsolete |
| Obsolete and reorganized for 5.1 | |
| Infrastructure | |
| SYMClma | Obsolete |
| VRTSaa | Included in VRTSsfmh |
| VRTSccg | Included in VRTSsfmh |
| VRTSdbms3 | Obsolete |
| VRTSicsco | Obsolete |
| VRTSjre | Obsolete |
| VRTSjre15 | Obsolete |
| VRTSmh | Included in VRTSsfmh |
| VRTSobc33 | Obsolete |
| VRTSobweb | Obsolete |
| VRTSobgui | Obsolete |
| VRTSpbx | Obsolete |
| VRTSsfm | Obsolete |
| VRTSweb | Obsolete |
| Product packages | |

**Table E-6** Veritas Storage Foundation obsolete and reorganized packages *(continued)*

| package | Description |
|---|---|
| VRTSacclib | Obsolete<br>The following information is for installations, upgrades, and uninstallations using the script- or Web-based installer.<br>■ For fresh installations VRTSacclib is not installed.<br>■ For upgrades, the existing VRTSacclib is uninstalled and a new VRTSacclib is installed.<br>■ For uninstallation, VRTSacclib is not uninstalled. |
| VRTSalloc | Obsolete |
| VRTScmccc | Obsolete |
| VRTScmcm | Obsolete |
| VRTScmcs | Obsolete |
| VRTScscm | Obsolete |
| VRTScscw | Obsolete |
| VRTScsocw | Obsolete |
| VRTScssim | Obsolete |
| VRTScutil | Obsolete |
| VRTSd2gui | Included in VRTSdbed |
| VRTSdb2ed | Included in VRTSdbed |
| VRTSdbcom | Included in VRTSdbed |
| VRTSdbed | Included in VRTSdbed |
| VRTSdcli | Obsolete |
| VRTSddlpr | Obsolete |
| VRTSdsa | Obsolete |
| VRTSfas | Obsolete |

**Table E-6** Veritas Storage Foundation obsolete and reorganized packages *(continued)*

| package | Description |
|---|---|
| VRTSfasag | Obsolete |
| VRTSfsman | Included in the product's main package. |
| VRTSfsmnd | Included in the product's main package. |
| VRTSfspro | Included in VRTSsfmh |
| VRTSgapms | Obsolete |
| VRTSmapro | Included in VRTSsfmh |
| VRTSorgui | Obsolete |
| VRTSsybed | Included in VRTSdbed |
| VRTSvail | Obsolete |
| VRTSvcsdb | Included in VRTSvcsea |
| VRTSvcsmn | Included in VRTSvcs |
| VRTSvcsor | Included in VRTSvcsea |
| VRTSvcssy | Included in VRTSvcsea |
| VRTSvcsvr | Included in VRTSvcs |
| VRTSvdid | Obsolete |
| VRTSvmman | Included in the product's main package. |
| VRTSvmpro | Included in VRTSsfmh |
| VRTSvrpro | Included in VRTSob |
| VRTSvrw | Obsolete |
| VRTSvxmsa | Obsolete |
| Documentation | All Documentation packages obsolete |

Appendix F

# High availability agent information

This appendix includes the following topics:


- About agents
- Enabling and disabling intelligent resource monitoring for agents manually
- CVMCluster agent
- CVMVxconfigd agent
- CVMVolDg agent
- CFSMount agent
- CFSfsckd agent


## About agents

An agent is defined as a process that starts, stops, and monitors all configured resources of a type, and reports their status to Veritas Cluster Server (VCS). Agents have both entry points and attributes. Entry points are also known as agent functions and are referred to as "agent functions" throughout the document.

Attributes contain data about the agent. An attribute has a definition and a value. You change attribute values to configure resources, which are defined as the individual components that work together to provide application services to the public network. For example, a resource may be a physical component such as a disk or a network interface card, a software component such as Oracle or a Web server, or a configuration component such as an IP address or mounted file system.

Attributes are either optional or required, although sometimes the attributes that are optional in one configuration may be required in other configurations. Many optional attributes have predefined or default values, which you should change as required. A variety of internal use only attributes also exist. Do not modify these attributes—modifying them can lead to significant problems for your clusters. Attributes have type and dimension. Some attribute values can accept numbers, others can accept alphanumeric values or groups of alphanumeric values, while others are simple boolean on/off values.

The entry points and attributes for each SFCFSHA agent are described in this appendix.

## VCS agents included within SFCFSHA

SFCFSHA includes the following VCS agents:

- CVMCluster agent
- CVMVxconfigd agent
- CVMVolDg agent
- CFSMount agent
- CFSfsckd
- Coordination Point agent

An SFCFSHA installation automatically configures the CVMCluster resource and the CVMVxconfigd resource.

You must configure the CVMVolDg agent for each shared disk group. If the database uses cluster file systems, configure the CFSMount agent for each volume in the disk group.

Use the information in this appendix about the entry points and attributes of the listed agents to make necessary configuration changes. For information on how to modify the VCS configuration:

See the *Veritas Cluster Server Administrator's Guide*

# Enabling and disabling intelligent resource monitoring for agents manually

Review the following procedures to enable or disable intelligent resource monitoring manually. The intelligent resource monitoring feature is enabled by default. The IMF resource type attribute determines whether an IMF-aware agent must perform intelligent resource monitoring.

**To enable intelligent resource monitoring**

1 Make the VCS configuration writable.

```
# haconf -makerw
```

2 Run the following command to enable intelligent resource monitoring.

- To enable intelligent monitoring of offline resources:

```
# hatype -modify resource_type IMF -update Mode 1
```

- To enable intelligent monitoring of online resources:

```
# hatype -modify resource_type IMF -update Mode 2
```

- To enable intelligent monitoring of both online and offline resources:

```
# hatype -modify resource_type IMF -update Mode 3
```

3 If required, change the values of the MonitorFreq key and the RegisterRetryLimit key of the IMF attribute.

Review the agent-specific recommendations in the attribute definition tables to set these attribute key values.

See "Attribute definition for CVMVxconfigd agent" on page 492.

See "Attribute definition for CFSMount agent" on page 498.

See "Attribute definition for CFSfsckd agent" on page 502.

4 Save the VCS configuration.

```
# haconf -dump -makero
```

5 Restart the agent. Run the following commands on each node.

```
# haagent -stop agent_name -force -sys sys_name
# haagent -start agent_name -sys sys_name
```

**To disable intelligent resource monitoring**

1 Make the VCS configuration writable.

```
# haconf -makerw
```

2 To disable intelligent resource monitoring for all the resources of a certain type, run the following command:

```
# hatype -modify resource_type IMF -update Mode 0
```

3 To disable intelligent resource monitoring for a specific resource, run the following command:

```
# hares -override resource_name IMF
# hares -modify resource_name IMF -update Mode 0
```

4 Save the VCS configuration.

```
# haconf -dump -makero
```

---

**Note:** VCS provides haimfconfig script to enable or disable the IMF functionality for agents. You can use the script with VCS in running or stopped state. Use the script to enable or disable IMF for the IMF-aware bundled agents, enterprise agents, and custom agents.

---

# Administering the AMF kernel driver

Review the following procedures to start, stop, or unload the AMF kernel driver.

**To start the AMF kernel driver**

1 Set the value of the AMF_START variable to 1 in the following file, if the value is not already 1:

```
# /etc/default/amf
```

2 Start the AMF kernel driver. Run the following command:

```
# svcadm enable amf
```

**To stop the AMF kernel driver**

1 Set the value of the AMF_START variable to 0 in the following file, if the value is not already 0:

```
# /etc/default/amf
```

2 Stop the AMF kernel driver. Run the following command:

```
# svcadm disable amf
```

**To unload the AMF kernel driver**

1 If agent downtime is not a concern, use the following steps to unload the AMF kernel driver:

- Stop the agents that are registered with the AMF kernel driver.
  The `amfstat` command output lists the agents that are registered with AMF under the Registered Reapers section.
  See the `amfstat` manual page.
- Stop the AMF kernel driver.
  See "To stop the AMF kernel driver" on page 488.
- Start the agents.

2 If you want minimum downtime of the agents, use the following steps to unload the AMF kernel driver:

- Run the following command to disable the AMF driver even if agents are still registered with it.

  ```
  # amfconfig -Uof
  ```

- Stop the AMF kernel driver.
  See "To stop the AMF kernel driver" on page 488.

# CVMCluster agent

The CVMCluster agent controls system membership on the cluster port that is associated with Veritas Volume Manager (VxVM).

The CVMCluster agent performs the following functions:

- Joins a node to the CVM cluster port.
- Removes a node from the CVM cluster port.
- Monitors the node's cluster membership state.

# Entry points for CVMCluster agent

Table F-1 describes the entry points used by the CVMCluster agent.

**Table F-1** CVMCluster agent entry points

| Entry Point | Description |
|---|---|
| Online | Joins a node to the CVM cluster port. Enables the Volume Manager cluster functionality by automatically importing the shared disk groups. |
| Offline | Removes a node from the CVM cluster port. |
| Monitor | Monitors the node's CVM cluster membership state. |

# Attribute definition for CVMCluster agent

Table F-2 describes the user-modifiable attributes of the CVMCluster resource type.

**Table F-2** CVMCluster agent attributes

| Attribute | Description |
|---|---|
| CVMClustName | Name of the cluster.<br>■ Type and dimension: string-scalar |
| CVMNodeAddr | List of host names and IP addresses.<br>■ Type and dimension: string-association |
| CVMNodeId | Associative list. The first part names the system; the second part contains the LLT ID number for the system.<br>■ Type and dimension: string-association |
| CVMTransport | Specifies the cluster messaging mechanism.<br>■ Type and dimension: string-scalar<br>■ Default = gab<br>**Note:** Do not change this value. |
| PortConfigd | The port number that is used by CVM for vxconfigd-level communication.<br>■ Type and dimension: integer-scalar |
| PortKmsgd | The port number that is used by CVM for kernel-level communication.<br>■ Type and dimension: integer-scalar |

**Table F-2** CVMCluster agent attributes *(continued)*

| Attribute | Description |
|---|---|
| CVMTimeout | Timeout in seconds used for CVM cluster reconfiguration.<br>■ Type and dimension: integer-scalar<br>■ Default = 200 |

# CVMCluster agent type definition

The following type definition is included in the file, `CVMTypes.cf`:

```
type CVMCluster (
        static keylist RegList = { CVMNodePreference }
        static int NumThreads = 1
        static int OnlineRetryLimit = 2
        static int OnlineTimeout = 400
        static str ArgList[] = { CVMTransport, CVMClustName,
                                 CVMNodeAddr, CVMNodeId, PortConfigd,
                                 PortKmsgd, CVMTimeout }
        str CVMClustName
        str CVMNodeAddr{}
        str CVMNodeId{}
        str CVMTransport
        str CVMNodePreference
        int PortConfigd
        int PortKmsgd
        int CVMTimeout
)
```

**Note:** The attributes `CVMNodeAddr`, `PortConfigd`, and `PortKmsgd` are not used in an SFCFSHA environment. GAB, the required cluster communication messaging mechanism, does not use them.

# CVMCluster agent sample configuration

The following is an example definition for the CVMCluster service group:

```
CVMCluster cvm_clus (
        Critical = 0
        CVMClustName = clus1
        CVMNodeId = { sys1 = 0, sys2 = 1 }
        CVMTransport = gab
```

```
CVMTimeout = 200
 )
```

# CVMVxconfigd agent

The CVMVxconfigd agent starts and monitors the vxconfigd daemon. The vxconfigd daemon maintains disk and disk group configurations, communicates configuration changes to the kernel, and modifies the configuration information that is stored on disks. CVMVxconfigd must be present in the CVM service group.

The CVMVxconfigd agent is an OnOnly agent; the agent starts the resource when the cluster starts up and VCS restarts the resource when necessary. The Operations attribute specifies these default aspects of startup.

Symantec recommends starting the vxconfigd daemon with the `syslog` option, which enables logging of debug messages. Note that the SFCFSHA installation configures the `syslog` option for the CVMVxconfigd agent.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

## Entry points for CVMVxconfigd agent

Table F-3 describes the entry points for the CVMVxconfigd agent.

**Table F-3** CVMVxconfigd entry points

| Entry Point | Description |
|---|---|
| Online | Starts the `vxconfigd` daemon |
| Offline | N/A |
| Monitor | Monitors whether `vxconfigd` daemon is running |
| imf_init | Initializes the agent to interface with the AMF kernel module. This function runs when the agent starts up. |
| imf_getnotification | Gets notification about the `vxconfigd` process state. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification. If the `vxconfigd` process fails, the function initiates a traditional CVMVxconfigd monitor entry point. |

**Table F-3** CVMVxconfigd entry points *(continued)*

| Entry Point | Description |
|---|---|
| imf_register | Registers or unregisters the `vxconfigd` process id (pid) with the AMF kernel module. This function runs after the resource goes into steady online state. |

# Attribute definition for CVMVxconfigd agent

Table F-4 describes the modifiable attributes of the CVMVxconfigd resource type.

**Table F-4** CVMVxconfigd agent attribute

| Attribute | Description |
|---|---|
| CVMVxconfigdArgs | List of the arguments that are sent to the `online` entry point.<br>Symantec recommends always specifying the `syslog` option.<br>■ Type and dimension: keylist |

**Table F-4** CVMVxconfigd agent attribute *(continued)*

| Attribute | Description |
|---|---|
| IMF | This resource-type level attribute determines whether the CVMVxconfigd agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level.<br>This attribute includes the following keys:<br>■ Mode: Define this attribute to enable or disable intelligent resource monitoring.<br>Valid values are as follows:<br>■ 0—Does not perform intelligent resource monitoring<br>■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources<br>Default: 0<br>■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer.<br>Default: 1<br>You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring.<br>After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows:<br>■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources<br>■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources<br>■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes.<br>Default: 3.<br>■ Type and dimension: integer-association<br>For more details of IMF attribute for the agent type, refer to the *Veritas Cluster Server Administrator's Guide*. |

# CVMVxconfigd agent type definition

The following type definition is included in the CVMTypes.cf file:

```
type CVMVxconfigd (
        static int IMF{} = { Mode=2, MonitorFreq=1, RegisterRetryLimit=3 }
        static int FaultOnMonitorTimeouts = 2
```

```
        static int RestartLimit = 5
        static str ArgList[] = { CVMVxconfigdArgs }
        static str Operations = OnOnly
        keylist CVMVxconfigdArgs
)
```

## CVMVxconfigd agent sample configuration

The following is an example definition for the `CVMVxconfigd` resource in the CVM service group:

```
CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )
```

# CVMVolDg agent

The CVMVolDg agent manages the CVM disk groups and CVM volumes and volume sets within the disk groups by performing the following functions:

- Imports the shared disk group from the CVM master node
- Starts the volumes and volume sets in the disk group
- Monitors the disk group, volumes, and volume sets
- Optionally, deports the disk group when the dependent applications are taken offline. The agent deports the disk group only if the appropriate attribute is set.

Configure the CVMVolDg agent for each disk group used by a Oracle service group. A disk group must be configured to only one Oracle service group.If cluster file systems are used for the database, configure the CFSMount agent for each volume or volume set in the disk group.

## Entry points for CVMVolDg agent

Table F-5 describes the entry points used by the CVMVolDg agent.

**Table F-5** CVMVolDg agent entry points

| Entry Point | Description |
|---|---|
| Online | Imports the shared disk group from the CVM master node, if the disk group is not already imported.<br>Starts all volumes and volume sets in the shared disk group specified by the CVMVolume attribute.<br>Sets the disk group activation mode to shared-write if the value of the CVMActivation attribute is sw. You can set the activation mode on both slave and master systems. |
| Offline | Removes the temporary files created by the online entry point.<br>If the `CVMDeportOnOffline` attribute is set to 1 and if the shared disk group does not contain open volumes on any node in the cluster, the disk group is deported from the CVM master node. |
| Monitor | Determines whether the disk group, the volumes, and the volume sets are online.<br>The agent takes a volume set offline if the file system metadata volume of a volume set is discovered to be offline in a monitor cycle.<br>**Note:** If the CFSMount resource goes offline and the file system on the volume set is unmounted, the agent retains the online state of the volume set even if the file system metadata volume in the volume set is offline. This is because the CVMVolDg agent is unable to determine whether or not the volumes that are offline are metadata volumes. |
| Clean | Removes the temporary files created by the online entry point. |

# Attribute definition for CVMVolDg agent

Table F-6 describes the user-modifiable attributes of the CVMVolDg resource type.

**Table F-6** CVMVolDg agent attributes

| Attribute | Description |
|---|---|
| CVMDiskGroup (required) | Shared disk group name.<br>■ Type and dimension: string-scalar |

**Table F-6** CVMVolDg agent attributes *(continued)*

| Attribute | Description |
|---|---|
| CVMVolume (required) | Name of shared volumes or volume sets. This list is used to check that the volumes or volume sets are in the correct state before allowing the resource to come online, and that the volumes remain in an enabled state.<br>■ Type and dimension: string-keylist |
| CVMActivation (required) | Activation mode for the disk group.<br>■ Type and dimension: string-scalar<br>■ Default = `sw (shared-write)`<br>This is a localized attribute. |
| CVMVolumeIoTest(optional) | List of volumes and volume sets that will be periodically polled to test availability. The polling is in the form of 4 KB reads every monitor cycle to a maximum of 10 of the volumes or volume sets in the list. For volume sets, reads are done on a maximum of 10 component volumes in each volume set.<br>■ Type and dimension: string-keylist |
| CVMDeportOnOffline (optional) | Indicates whether or not the shared disk group must be deported when the last online CVMVolDg resource for a disk group is taken offline.<br>The value 1 indicates that the agent will deport the shared disk group from the CVM master node, if not already deported, when the last online CVMVolDg resource for the disk group is taken offline.<br>The value 0 indicates that the agent will not deport the shared disk group when the CVMVolDg resource is taken offline.<br>■ Type and dimension: integer-scalar<br>■ Default = 0<br>**Note:** If multiple CVMVolDg resources are configured for a shared disk group, set the value of the attribute to either 1 or 0 for all of the resources.<br>The CVM disk group is deported based on the order in which the CVMVolDg resources are taken offline. If the CVMVolDg resources in the disk group contain a mixed setting of 1 and 0 for the `CVMDeportOnOffline` attribute, the disk group is deported only if the attribute value is 1 for the last CVMVolDg resource taken offline. If the attribute value is 0 for the last CVMVolDg resource taken offline, the disk group is not deported.<br>The deport operation fails if the shared disk group contains open volumes. |

# CVMVolDg agent type definition

The CVMTypes.cf file includes the CVMVolDg type definition:

```
type CVMVolDg (
        static keylist RegList = { CVMActivation, CVMVolume }
        static int OnlineRetryLimit = 2
        static int OnlineTimeout = 400
        static keylist ExternalStateChange = { OnlineGroup }
        static str ArgList[] = { CVMDiskGroup, CVMVolume, CVMActivation,
                                 CVMVolumeIoTest, CVMDGAction, CVMDeportOnOff
                                 CVMDeactivateOnOffline, State }
        str CVMDiskGroup
        str CVMDGAction
        keylist CVMVolume
        str CVMActivation
        keylist CVMVolumeIoTest
        int CVMDeportOnOffline
        int CVMDeactivateOnOffline
        temp int voldg_stat
)
```

## CVMVolDg agent sample configuration

Each Oracle service group requires a CVMVolDg resource type to be defined. The following is a sample configuration:

```
CVMVolDg cvmvoldg1 (
 Critical = 0
 CVMDiskgroup = testdg
 CVMVolume = { vol1, vol2, mvol1, mvol2, snapvol, vset1 }
 CVMVolumeIoTest = { snapvol, vset1 }
 CVMActivation @system1 = sw
 CVMActivation @system2 = sw
 CVMDeportOnOffline = 1
)
```

# CFSMount agent

The CFSMount agent brings online, takes offline, and monitors a cluster file system mount point.

The agent executable is located in /opt/VRTSvcs/bin/CFSMount/CFSMountAgent.

The CFSMount type definition is described in the /etc/VRTSvcs/conf/config/CFSTypes.cf file.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring

Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

## Entry points for CFSMount agent

Table F-7 provides the entry points for the CFSMount agent.

**Table F-7** CFSMount agent entry points

| Entry Point | Description |
|---|---|
| Online | Mounts a block device in cluster mode. |
| Offline | Unmounts the file system, forcing unmount if necessary, and sets primary to secondary if necessary. |
| Monitor | Determines if the file system is mounted. Checks mount status using the `fsclustadm` command. |
| Clean | Generates a null operation for a cluster file system mount. |
| imf_init | Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for the agent. This function runs when the agent starts up. |
| imf_getnotification | Gets notification about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification. |
| imf_register | Registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into steady state (online or offline). |

## Attribute definition for CFSMount agent

Table F-8 lists user-modifiable attributes of the CFSMount Agent resource type.

**Table F-8** CFSMount Agent attributes

| Attribute | Description |
|---|---|
| MountPoint | Directory for the mount point.<br>■ Type and dimension: string-scalar |
| BlockDevice | Block device for the mount point.<br>■ Type and dimension: string-scalar |

**Table F-8** CFSMount Agent attributes *(continued)*

| Attribute | Description |
|---|---|
| NodeList | List of nodes on which to mount. If NodeList is NULL, the agent uses the service group system list.<br>■ Type and dimension: string-keylist |
| IMF | Resource-type level attribute that determines whether the CFSMount agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level.<br>This attribute includes the following keys:<br>■ Mode: Define this attribute to enable or disable intelligent resource monitoring.<br>Valid values are as follows:<br>■ 0—Does not perform intelligent resource monitoring<br>■ 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources<br>■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources<br>■ 3—Performs intelligent resource monitoring for both online and for offline resources<br>Default: 0<br>■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer.<br>Default: 1<br>You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring.<br>After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows:<br>■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources<br>■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources<br>■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes.<br>Default: 3.<br>■ Type and dimension: integer-association<br>See "Enabling and disabling intelligent resource monitoring for agents manually" on page 485. |

**Table F-8** CFSMount Agent attributes *(continued)*

| Attribute | Description |
|---|---|
| MountOpt<br><br>(optional) | Options for the mount command. To create a valid MountOpt attribute string:<br>■ Use the VxFS type-specific options only.<br>■ Do not use the -o flag to specify the VxFS-specific options.<br>■ Do not use the `-F` vxfs file system type option.<br>■ Be aware the cluster option is not required.<br>■ Specify options in comma-separated list:<br>`ro`<br>`ro,cluster`<br>`blkclear,mincache=closesync`<br>■ Type and dimension: string-scalar |
| Policy (optional) | List of nodes to assume the primaryship of the cluster file system if the primary fails. If set to NULL or if none of the hosts specified in the list is active when the primary fails, a node is randomly selected from the set of active nodes to assume primaryship.<br>■ Type and dimension: string-scalar |

# CFSMount agent type definition

The `CFSTypes.cf` file includes the CFSMount agent type definition:

```
type CFSMount (
        static int IMF{} = { Mode=3, MonitorFreq=1, RegisterRetryLimit=3 }
        static keylist RegList = { MountOpt, Policy, NodeList, ForceOff, SetPrimary }
        static keylist SupportedActions = { primary }
        static int FaultOnMonitorTimeouts = 1
        static int OnlineWaitLimit = 1
        static str ArgList[] = { MountPoint, BlockDevice, MountOpt, Primary, AMFMountType }
        str MountPoint
        str MountType
        str BlockDevice
        str MountOpt
        keylist NodeList
        keylist Policy
        temp str Primary
        str SetPrimary
        temp str RemountRes
        temp str AMFMountType
```

```
        str ForceOff
)
```

## CFSMount agent sample configuration

Each Oracle service group requires a CFSMount resource type to be defined:

```
CFSMount ora_mount (
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol1"
        Primary = sys2;
        )
```

To see CFSMount defined in a more extensive example:

# CFSfsckd agent

The CFSfsckd agent starts, stops, and monitors the `vxfsckd` process. The CFSfsckd agent executable is `/opt/VRTSvcs/bin/CFSfsckd/CFSfsckdAgent`. The type definition is in the `/etc/VRTSvcs/conf/config/CFSTypes.cf` file. The configuration is added to the `main.cf` file after running the `cfscluster config` command.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

## Entry points for CFSfsckd agent

Table F-9 describes the CFSfsckd agent entry points.

**Table F-9** CFSfsckd agent entry points

| Entry Points | Description |
|---|---|
| Online | Starts the vxfsckd process. |
| Offline | Kills the vxfsckd process. |
| Monitor | Checks whether the vxfsckd process is running. |
| Clean | A null operation for a cluster file system mount. |
| imf_init | Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for the agent. This function runs when the agent starts up. |

**Table F-9** CFSfsckd agent entry points *(continued)*

| Entry Points | Description |
|---|---|
| imf_getnotification | Gets notification about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification. |
| imf_register | Registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into steady state (online or offline). |

## Attribute definition for CFSfsckd agent

Table F-10 lists user-modifiable attributes of the CFSfsckd Agent resource type.

**Table F-10** CFSfsckd Agent attributes

| Attribute | Description |
|---|---|
| IMF | Resource-type level attribute that determines whether the CFSfsckd agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level.<br>This attribute includes the following keys:<br>■ Mode: Define this attribute to enable or disable intelligent resource monitoring.<br>Valid values are as follows:<br>■ 0—Does not perform intelligent resource monitoring<br>■ 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources<br>■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources<br>■ 3—Performs intelligent resource monitoring for both online and for offline resources<br>Default: 0<br>■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer.<br>Default: 1<br>You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring.<br>After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows:<br>■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources<br>■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources<br>■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes.<br>Default: 3.<br>■ Type and dimension: integer-association<br>See "Enabling and disabling intelligent resource monitoring for agents manually" on page 485. |

# CFSfsckd agent type definition

The CFSfsckd type definition:

```
type CFSfsckd (
        static int IMF{} = { Mode=3, MonitorFreq=1, RegisterRetryLimit=3 }
        static int RestartLimit = 1
```

```
        str ActivationMode{}
)
```

# CFSfsckd agent sample configuration

This is a sample of CFSfsckd configuration:

```
CFSfsckd vxfsckd (
)
```

Appendix G

# Troubleshooting the SFCFSHA installation

This appendix includes the following topics:


- Restarting the installer after a failed connection
- What to do if you see a licensing reminder
- Storage Foundation Cluster File System High Availability installation issues
- Storage Foundation Cluster File System High Availability problems
- Installer cannot create UUID for the cluster
- The vxfentsthdw utility fails when SCSI TEST UNIT READY command fails
- Troubleshooting CP server
- Troubleshooting server-based fencing on the SFCFSHA cluster nodes
- Troubleshooting the webinstaller


## 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 54.
  After you install the license key, you must validate the license key using the following command:

  ```
  # /opt/VRTS/bin/vxlicrep
  ```

- 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

# Storage Foundation Cluster File System High Availability installation issues

If you encounter any issues installing SFCFSHA, refer to the following paragraphs for typical problems and their solutions:

## Incorrect permissions for root on remote system

The permissions are inappropriate. Make sure you have remote root access permission on each system to which you are installing.

```
Failed to setup rsh communication on 10.198.89.241:
'rsh 10.198.89.241 <command>' failed
Trying to setup ssh communication on 10.198.89.241.
Failed to setup ssh communication on 10.198.89.241:
Login denied

Failed to login to remote system(s) 10.198.89.241.
Please make sure the password(s) are correct and superuser(root)
can login to the remote system(s) with the password(s).
If you want to setup rsh on remote system(s), please make sure
rsh with command argument ('rsh <host> <command>') is not
denied by remote system(s).

Either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication

Would you like the installer to setup ssh/rsh communication
automatically between the nodes?
Superuser passwords for the systems will be asked. [y,n,q] (y) n

System verification did not complete successfully

The following errors were discovered on the systems:

The ssh permission denied on 10.198.89.241
rsh exited 1 on 10.198.89.241
either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication
```

Suggested solution: You need to set up the systems to allow remote access using `ssh` or `rsh`.

See "About configuring secure shell or remote shell communication modes before installing products" on page 467.

---

**Note:** Remove remote shell permissions after completing the SFCFSHA installation and configuration.

---

## Inaccessible system

The system you specified is not accessible. This could be for a variety of reasons such as, the system name was entered incorrectly or the system is not available over the network.

```
 Verifying systems: 12% .....................................
 Estimated time remaining: 0:10 1 of 8
 Checking system communication ............................. Done
System verification did not complete successfully
The following errors were discovered on the systems:
cannot resolve hostname host1
Enter the  system names separated by spaces: q,? (host1)
```

Suggested solution: Verify that you entered the system name correctly; use the `ping`(1M) command to verify the accessibility of the host.

# Storage Foundation Cluster File System High Availability problems

If there is a device failure or controller failure to a device, the file system may become disabled cluster-wide. To address the problem, unmount file system on all the nodes, then run a full `fsck`. When the file system check completes, mount all nodes again.

## Unmount failures

The `umount` command can fail if a reference is being held by an NFS server. Unshare the mount point and try the unmount again.

## Mount failures

Mounting a file system can fail for the following reasons:

- The file system is not using disk layout Version 7 or later.
- The mount options do not match the options of already mounted nodes.
- A cluster file system is mounted by default with the `qio` option enabled if the node has a Quick I/O for Databases license installed, even if the `qio` mount option was not explicitly specified. If the Quick I/O license is not installed, a cluster file system is mounted without the `qio` option enabled. So if some nodes in the cluster have a Quick I/O license installed and others do not, a cluster mount can succeed on some nodes and fail on others due to different mount options. To avoid this situation, ensure that Quick I/O licensing is uniformly

applied, or be careful to mount the cluster file system with the `qio/noqio` option appropriately specified on each node of the cluster.
See the `mount`(1M) manual page.

- A shared CVM volume was not specified.
- The device is still mounted as a local file system somewhere on the cluster. Unmount the device.
- The `fsck` or `mkfs` command is being run on the same volume from another node, or the volume is mounted in non-cluster mode from another node.
- The `vxfsckd` daemon is not running. This typically happens only if the `CFSfsckd` agent was not started correctly.
- If `mount` fails with an error message:

  ```
  vxfs mount: cannot open mnttab
  ```

  `/etc/mnttab` is missing or you do not have `root` privileges.
- If `mount` fails with an error message:

  ```
  vxfs mount: device already mounted, ...
  ```

  The device is in use by `mount`, `mkfs` or `fsck` on the same node. This error cannot be generated from another node in the cluster.
- If this error message displays:

  ```
  mount: slow
  ```

  The node may be in the process of joining the cluster.
- If you try to mount a file system that is already mounted without `-o cluster` option (that is, not in shared mode) on another cluster node,

  ```
  # mount -F vxfs /dev/vx/dsk/share/vol01 /vol01
  ```

  The following error message displays:

  ```
  vxfs mount: /dev/vx/dsk/share/vol01 is already mounted,
    /vol01 is busy, allowable number of mount points exceeded,
    or cluster reservation failed for the volume
  ```

# Command failures

This section describes command failures.

- Manual pages not accessible with the `man` command. Set the MANPATH environment variable appropriately.
  See "Setting environment variables" on page 63.
- The `mount`, `fsck`, and `mkfs` utilities reserve a shared volume. They fail on volumes that are in use. Be careful when accessing shared volumes with other utilities such as `dd`, it is possible for these commands to destroy data on the disk.
- Running some commands, such as `vxupgrade -n 7 /vol02`, can generate the following error message:

  ```
  vxfs vxupgrade: ERROR: not primary in a cluster file system
  ```

  This means that you can run this command only on the primary, that is, the system that mounted this file system first.

# Performance issues

Quick I/O File system performance is adversely affected if a cluster file system is mounted with the `qio` option enabled, but the file system is not used for Quick I/O files. Because `qio` is enabled by default, if you do not intend to use a shared file system for Quick I/O, explicitly specify the `noqio` option when mounting.

# High availability issues

This section describes high availability issues.

## Network partition and jeopardy

Network partition (or split brain) is a condition where a network failure can be misinterpreted as a failure of one or more nodes in a cluster. If one system in the cluster incorrectly assumes that another system failed, it may restart applications already running on the other system, thereby corrupting data. CFS tries to prevent this by having redundant heartbeat links.

At least one link must be active to maintain the integrity of the cluster. If all the links go down, after the last network link is broken, the node can no longer communicate with other nodes in the cluster. Thus the cluster is in one of two possible states. Either the last network link is broken (called a network partition condition), or the last network link is okay, but the node crashed, in which case it is not a network partition problem. It is not possible to identify whether it is the first or second state, so a kernel message is issued to indicate that a network partition may exist and there is a possibility of data corruption.

Jeopardy is a condition where a node in the cluster has a problem connecting to other nodes. In this situation, the link or disk heartbeat may be down, so a jeopardy warning may be displayed. Specifically, this message appears when a node has only one remaining link to the cluster and that link is a network link. This is considered a critical event because the node may lose its only remaining connection to the network.

**Warning:** Do not remove the communication links while shared storage is still connected.

### Low memory

Under heavy loads, software that manages heartbeat communication links may not be able to allocate kernel memory. If this occurs, a node halts to avoid any chance of network partitioning. Reduce the load on the node if this happens frequently.

A similar situation may occur if the values in the `/etc/llttab` files on all cluster nodes are not correct or identical.

# 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 SFCFSHA configuration, upgrade, or when you add a node to the cluster using the installer.

Workaround: To start SFCFSHA, you must run the uuidconfig.pl script manually to configure the UUID on each cluster node.

**To configure the cluster UUID when you create a cluster manually**

- On one node in the cluster, perform the following command to populate the cluster UUID on each node in the cluster.

  ```
  # /opt/VRTSvcs/bin/uuidconfig.pl -clus -configure nodeA
  nodeB ... nodeN
  ```

  Where nodeA, nodeB, through nodeN are the names of the cluster nodes.

# The vxfentsthdw utility fails when SCSI TEST UNIT READY command fails

While running the vxfentsthdw utility, you may see a message that resembles as follows:

```
Issuing SCSI TEST UNIT READY to disk reserved by other node
FAILED.
Contact the storage provider to have the hardware configuration
fixed.
```

The disk array does not support returning success for a `SCSI TEST UNIT READY` command when another host has the disk reserved using SCSI-3 persistent reservations. This happens with the Hitachi Data Systems 99XX arrays if bit 186 of the system mode option is not enabled.

# Troubleshooting CP server

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/VRTSvcs/log/vcsauthserver.log (Security related)
- If the vxcpserv process fails on the CP server, then review the following diagnostic files:
  - /var/VRTScps/diag/FFDC_CPS_*pid*_vxcpserv.log
  - /var/VRTScps/diag/stack_*pid*_vxcpserv.txt

**Note:** If the vxcpserv process fails on the CP server, these files are present in addition to a core file. VCS restarts vxcpserv process automatically in such situations.

The file /var/VRTSvcs/log/vxfen/vxfend_[ABC].log contains logs that may be useful in understanding and troubleshooting fencing-related issues on a SFCFSHA cluster (client cluster) node.

See "Troubleshooting issues related to the CP server service group" on page 513.

See "Checking the connectivity of CP server" on page 513.

See "Issues during fencing startup on SFCFSHA cluster nodes set up for server-based fencing" on page 514.

See "Issues during online migration of coordination points" on page 514.

## 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 SFCFSHA 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 SFCFSHA cluster nodes

The file /var/VRTSvcs/log/vxfen/vxfend_[ABC].log contains logs files that may be useful in understanding and troubleshooting fencing-related issues on a SFCFSHA cluster (application cluster) node.

# Issues during fencing startup on SFCFSHA cluster nodes set up for server-based fencing

**Table G-1** Fencing startup issues on SFCFSHA cluster (client cluster) nodes

| Issue | Description and resolution |
|---|---|
| `cpsadm` command on the SFCFSHA cluster gives connection error | If you receive a connection error message after issuing the `cpsadm` command on the SFCFSHA cluster, perform the following actions:<br>■ Ensure that the CP server is reachable from all the SFCFSHA cluster nodes.<br>■ Check that the SFCFSHA cluster nodes use the correct CP server virtual IP or virtual hostname and the correct port number.<br>Check the /etc/vxfenmode file.<br>■ Ensure that the running CP server is using the same virtual IP/virtual hostname and port number. |
| Authorization failure | Authorization failure occurs when the CP server's nodes or users are not added in the CP server configuration. Therefore, fencing on the SFCFSHA 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.<br>To resolve this issue, add the CP server node and user in the CP server configuration and restart fencing.<br>See "Preparing the CP servers manually for use by the SFCFSHA cluster" on page 227. |
| Authentication failure | If you had configured secure communication between the CP server and the SFCFSHA cluster (client cluster) nodes, authentication failure can occur due to the following causes:<br>■ Symantec Product Authentication Services (AT) is not properly configured on the CP server and/or the SFCFSHA cluster.<br>■ The CP server and the SFCFSHA cluster nodes use different root brokers, and trust is not established between the authentication brokers: |

# Issues during online migration of coordination points

During online migration of coordination points using the vxfenswap utility, the operation is automatically rolled back if a failure is encountered during validation of coordination points from any of the cluster nodes.

Validation failure of the new set of coordination points can occur in the following circumstances:

- The /etc/vxfenmode.test file is not updated on all the SFCFSHA cluster nodes, because new coordination points on the node were being picked up from an old /etc/vxfenmode.test file. The /etc/vxfenmode.test file must be updated with the

current details. If the /etc/vxfenmode.test file is not present, vxfenswap copies configuration for new coordination points from the /etc/vxfenmode file.

- The coordination points listed in the /etc/vxfenmode file on the different SFCFSHA 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 SFCFSHA cluster nodes to the CP server(s).
- Cluster, nodes, or users for the SFCFSHA cluster nodes have not been added on the new CP servers, thereby causing authorization failure.

### Vxfen service group activity 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.

Thus, 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 reflected 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 the webinstaller

This section provides possible solutions to problems that may occur when using the `webinstaller` script:

- Issue: The `webinstaller` script may report an error.

  You may receive a similar error message when using the webinstaller:

  ```
  Error: could not get hostname and IP address
  ```

Solution: Check whether `/etc/hosts` and `/etc/resolv.conf` file are correctly configured.

- Issue: The hostname is not a fully qualified domain name.
  You must have a fully qualified domain name for the hostname in https://<*hostname*>:<*port*>/.
  Solution: Check whether the `domain` section is defined in `/etc/resolv.conf` file.
- Issue: FireFox 3 may report an error.
  You may receive a similar error message when using FireFox 3:

  ```
  Certificate contains the same serial number as another certificate.
  ```

  Solution: Visit FireFox knowledge base website:

http://support.mozilla.com/en-US/kb/Certificate+contains+the+same+serial+number+as+another+certificate

Appendix H

# Sample SFCFSHA 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:

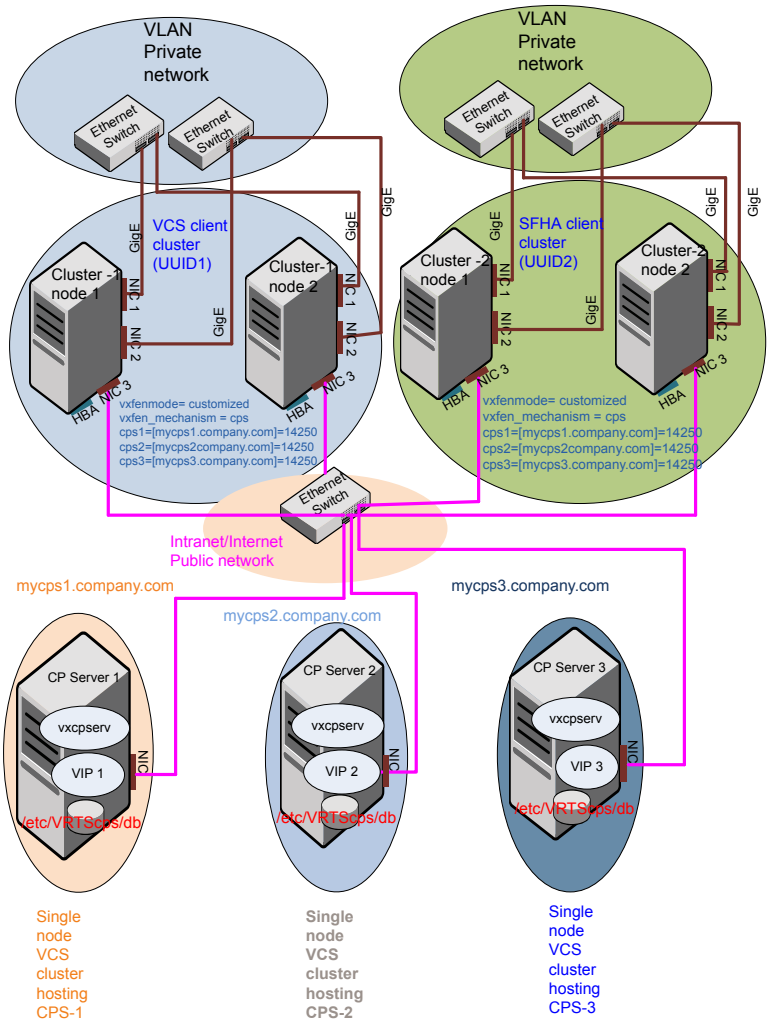
- Two unique client clusters that are served by 3 CP servers:
  See Figure H-1 on page 518.
- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:
- Two node campus cluster that is served be remote CP server and 2 SCSI-3 disks:
- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:

### Two unique client clusters served by 3 CP servers

Figure H-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 H-1** Two unique client clusters served by 3 CP servers



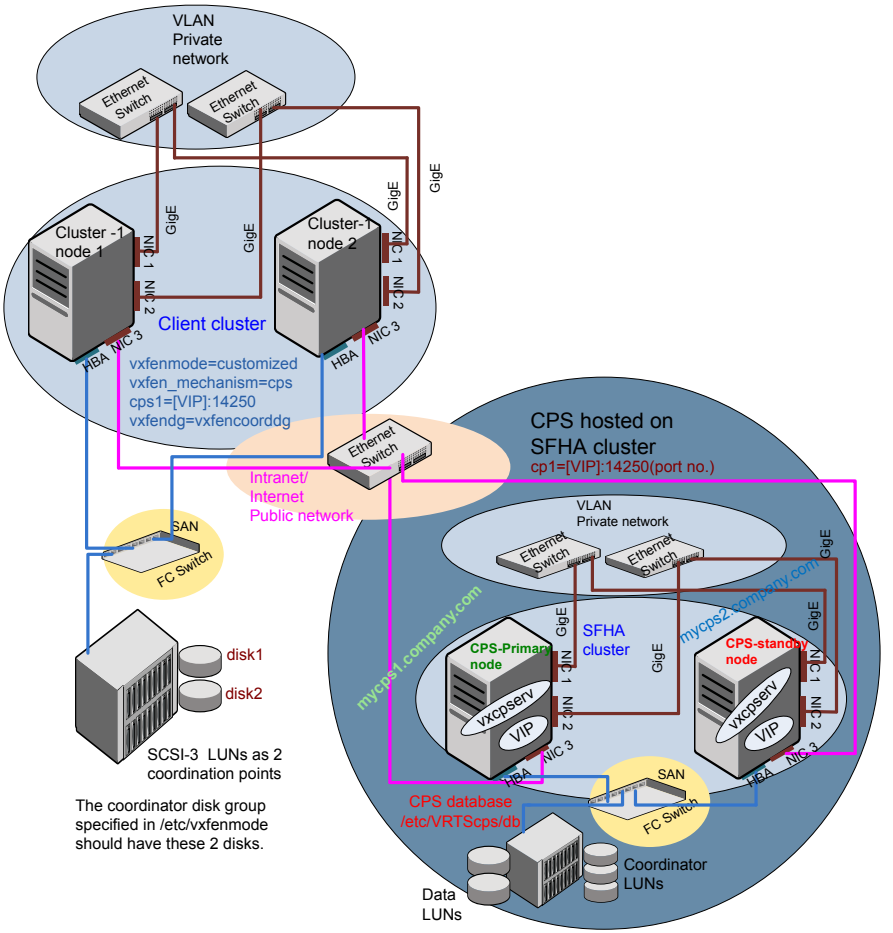

## Client cluster served by highly available CPS and 2 SCSI-3 disks

Figure H-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 H-2** Client cluster served by highly available CP server and 2 SCSI-3 disks



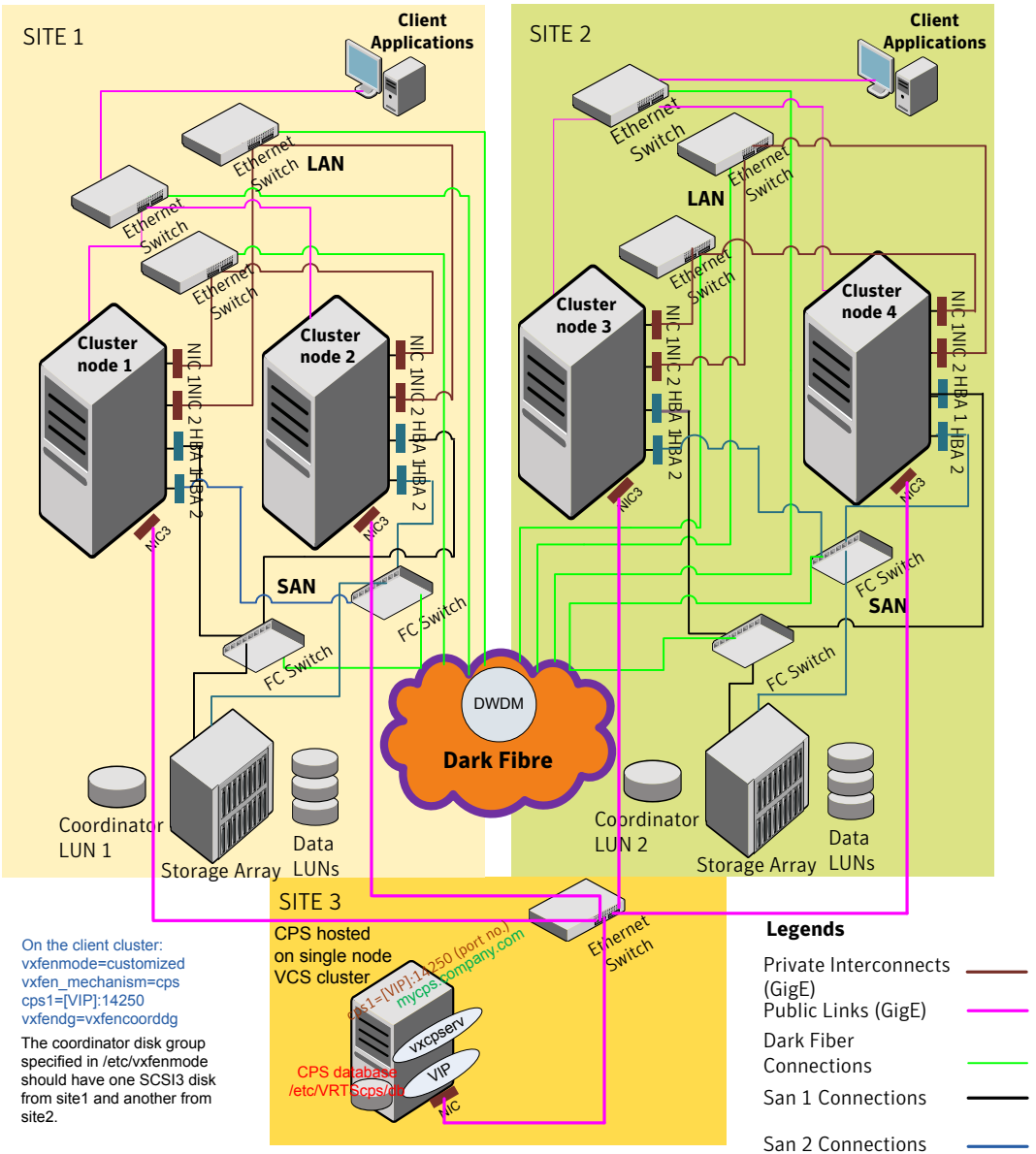
# Two node campus cluster served by remote CP server and 2 SCSI-3 disks

Figure H-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 H-3** Two node campus cluster served by remote CP server and 2 SCSI-3



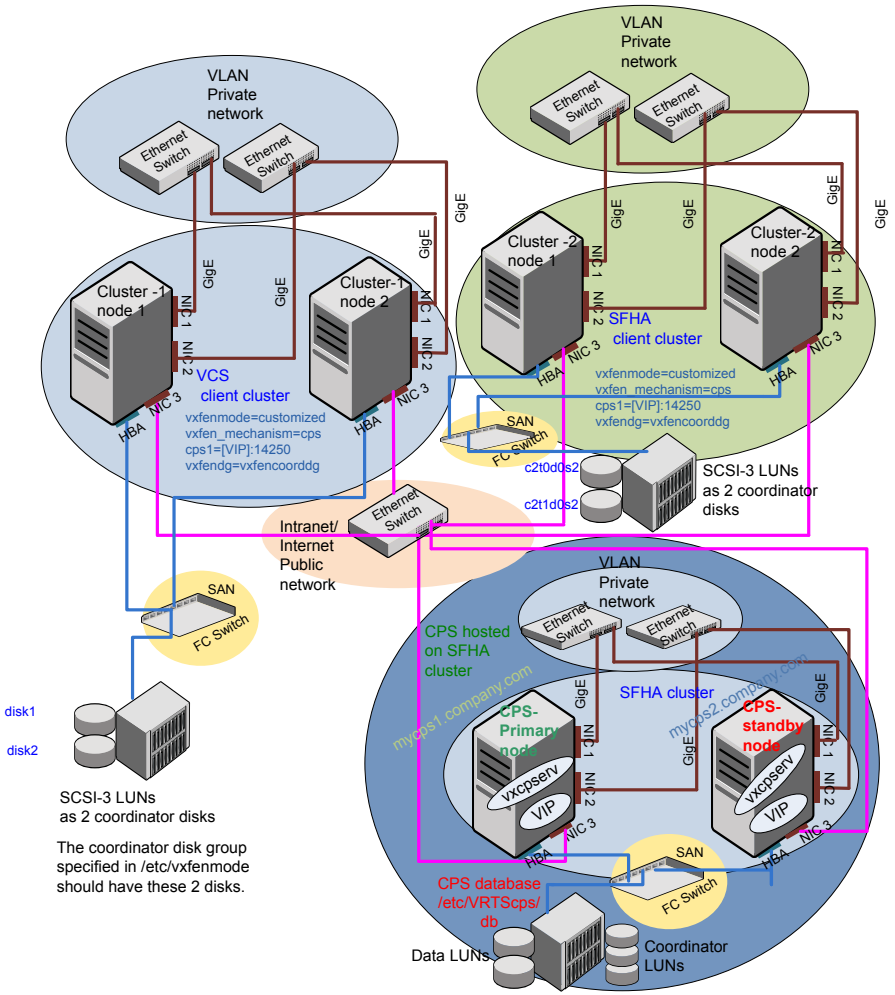
# Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

Figure H-4 displays a configuration where multiple client clusters are being served by one highly available CP server and 2 local SCSI-3 LUNS (disks).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

The two SCSI-3 disks are are part of the disk group vxfencoorddg. The third coordination point is a CP server, hosted on an SFHA cluster, with its own shared database and coordinator disks.

**Figure H-4** Multiple client clusters served by highly available CP server and 2 SCSI-3 disks



Appendix I

# Reconciling major/minor numbers for NFS shared disks

This appendix includes the following topics:


- Reconciling major/minor numbers for NFS shared disks


## Reconciling major/minor numbers for NFS shared disks

Your configuration may include disks on the shared bus that support NFS. You can configure the NFS file systems that you export on disk partitions or on Veritas Volume Manager volumes.

An example disk partition name is `/dev/dsk/c1t1d0s2`.

An example volume name is `/dev/vx/dsk/shareddg/vol3`. Each name represents the block device on which the file system is to be mounted.

In a VCS cluster, block devices providing NFS service must have the same major and minor numbers on each cluster node. Major numbers identify required device drivers (such as a Solaris partition or a VxVM volume). Minor numbers identify the specific devices themselves. NFS also uses major and minor numbers to identify the exported file system.

Major and minor numbers must be verified to ensure that the NFS identity for the file system is the same when exported from each node.

# Checking major and minor numbers for disk partitions

The following sections describe checking and changing, if necessary, the major and minor numbers for disk partitions used by cluster nodes.

**To check major and minor numbers on disk partitions**

- Use the following command on all nodes exporting an NFS file system. This command displays the major and minor numbers for the block device.

  ```
  # ls -lL block_device
  ```

  The variable *block_device* refers to a partition where a file system is mounted for export by NFS. Use this command on each NFS file system. For example, type:

  ```
  # ls -lL /dev/dsk/c1t1d0s2
  ```

  Output on Node A resembles:

  ```
  crw-r-----  1 root  sys  32,1 Dec 3 11:50 /dev/dsk/c1t1d0s2
  ```

  Output on Node B resembles:

  ```
  crw-r-----  1 root  sys  32,1 Dec 3 11:55 /dev/dsk/c1t1d0s2
  ```

  Note that the major numbers (32) and the minor numbers (1) match, satisfactorily meeting the requirement for NFS file systems.

**To reconcile the major numbers that do not match on disk partitions**

1. Reconcile the major and minor numbers, if required. For example, if the output in the previous section resembles the following, perform the instructions beginning step 2:

   Output on Node A:

   ```
   crw-r-----  1 root  sys  32,1 Dec 3 11:50 /dev/dsk/c1t1d0s2
   ```

   Output on Node B:

   ```
   crw-r-----  1 root  sys  36,1 Dec 3 11:55 /dev/dsk/c1t1d0s2
   ```

2. Place the VCS command directory in your path.

   ```
   # export PATH=$PATH:/usr/sbin:/sbin:/opt/VRTS/bin
   ```

3 Attempt to change the major number on System B (now 36) to match that of System A (32). Use the command:

```
# haremajor -sd major_number
```

For example, on Node B, enter:

```
# haremajor -sd 32
```

4 If the command succeeds, go to step 8.

5 If the command fails, you may see a message resembling:

```
Error: Preexisting major number 32
These are available numbers on this system: 128...
Check /etc/name_to_major on all systems for
available numbers.
```

6 Notice that the number 36 (the major number on Node A) is not available on Node B. Run the `haremajor` command on Node B and change it to 128,

```
# haremajor -sd 128
```

7 Run the same command on Node A. If the command fails on Node A, the output lists the available numbers. Rerun the command on both nodes, setting the major number to one available to both.

8 Reboot each system on which the command succeeds.

9 Proceed to reconcile the major numbers for your next partition.

**To reconcile the minor numbers that do not match on disk partitions**

1 In the example, the minor numbers are `1` and `3` and are reconciled by setting to 30 on each node.

2 Type the following command on both nodes using the name of the block device:

```
# ls -1 /dev/dsk/c1t1d0s2
```

Output from this command resembles the following on Node A:

```
lrwxrwxrwx  1 root  root  83 Dec 3 11:50
 /dev/dsk/c1t1d0s2         -> ../../
 devices/sbus@1f,0/QLGC,isp@0,10000/sd@1,0:d,raw
```

The `device name` (in bold) includes the slash following the word `devices`, and continues to, but does not include, the colon.

3 Type the following command on both nodes to determine the instance numbers that the SCSI driver uses:

```
# grep sd /etc/path_to_inst | sort -n -k 2,2
```

Output from this command resembles the following on Node A:

```
"/sbus@1f,0/QLGC,isp@0,10000/sd@0,0" 0 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@1,0" 1 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@2,0" 2 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@3,0" 3 "sd"
.
.
"/sbus@1f,0/SUNW,fas@e,8800000/sd@d,0" 27 "sd"
"/sbus@1f,0/SUNW,fas@e,8800000/sd@e,0" 28 "sd"
"/sbus@1f,0/SUNW,fas@e,8800000/sd@f,0" 29 "sd"
```

In the output, the instance numbers are in the second field.

The instance number that is associated with the device name that matches the name for Node A displayed in step 2, is "1."

4 Compare instance numbers for the device in the output on each node.

After you review the instance numbers, perform one of the following tasks:

- If the instance number from one node is unused on the other— it does not appear in the output of step 3—edit `/etc/path_to_inst`.
  You edit this file to make the second node's instance number similar to the number of the first node.
- If the instance numbers in use on both nodes, edit `/etc/path_to_inst` on both nodes. Change the instance number that is associated with the device name to an unused number. The number needs to be greater than the highest number that other devices use. For example, the output of step 3 shows the instance numbers that all devices use (from 0 to 29). You edit the file `/etc/path_to_inst` on each node and reset the instance numbers to 30.

5 Type the following command to reboot each node on which `/etc/path_to_inst` was modified:

```
# reboot -- -rv
```

# Checking the major and minor number for VxVM volumes

The following sections describe checking and changing, if necessary, the major and minor numbers for the VxVM volumes that cluster systems use.

**To check major and minor numbers on VxVM volumes**

1. Place the VCS command directory in your path. For example:

   ```
   # export PATH=$PATH:/usr/sbin:/sbin:/opt/VRTS/bin
   ```

2. To list the devices, use the `ls -lL` *block_device* command on each node:

   ```
   # ls -lL /dev/vx/dsk/shareddg/vol3
   ```

   On Node A, the output may resemble:

   ```
   brw-------   1 root  root  32,43000 Mar 22 16:4 1
   /dev/vx/dsk/shareddg/vol3
   ```

   On Node B, the output may resemble:

   ```
   brw-------   1 root  root  36,43000 Mar 22 16:4 1
   /dev/vx/dsk/shareddg/vol3
   ```

3. Import the associated shared disk group on each node.

4 Use the following command on each node exporting an NFS file system. The command displays the major numbers for `vxio` and `vxspec` that Veritas Volume Manager uses . Note that other major numbers are also displayed, but only `vxio` and `vxspec` are of concern for reconciliation:

```
# grep vx /etc/name_to_major
```

Output on Node A:

```
vxdmp 30
vxio 32
vxspec 33
vxfen 87
vxglm 91
```

Output on Node B:

```
vxdmp 30
vxio 36
vxspec 37
vxfen 87
vxglm 91
```

5 To change Node B's major numbers for `vxio` and `vxspec` to match those of Node A, use the command:

```
haremajor -vx major_number_vxio major_number_vxspec
```

For example, enter:

```
# haremajor -vx 32 33
```

If the command succeeds, proceed to step 8. If this command fails, you receive a report similar to the following:

```
Error: Preexisting major number 32
These are available numbers on this system: 128...
Check /etc/name_to_major on all systems for
available numbers.
```

6 If you receive this report, use the `haremajor` command on Node A to change the major number (`32/33`) to match that of Node B (`36/37`). For example, enter:

```
# haremajor -vx 36 37
```

If the command fails again, you receive a report similar to the following:

```
Error: Preexisting major number 36
These are available numbers on this node: 126...
Check /etc/name_to_major on all systems for
available numbers.
```

7 If you receive the second report, choose the larger of the two available numbers (in this example, `128`). Use this number in the `haremajor` command to reconcile the major numbers. Type the following command on both nodes:

```
# haremajor -vx 128 129
```

8 Reboot each node on which `haremajor` was successful.

9 If the minor numbers match, proceed to reconcile the major and minor numbers of your next NFS block device.

10 If the block device on which the minor number does not match is a volume, consult the `vxdg`(1M) manual page. The manual page provides instructions on reconciling the Veritas Volume Manager minor numbers, and gives specific reference to the `reminor` option.

Node where the vxio driver number have been changed require rebooting.

Appendix J

# Configuring LLT over UDP

This appendix includes the following topics:


- Using the UDP layer for LLT
- Manually configuring LLT over UDP using IPv4
- Using the UDP layer of IPv6 for LLT
- Manually configuring LLT over UDP using IPv6


## Using the UDP layer for LLT

SFCFSHA provides the option of using LLT over the UDP (User Datagram Protocol) layer for clusters using wide-area networks and routers. UDP makes LLT packets routable and thus able to span longer distances more economically.

### When to use LLT over UDP

Use LLT over UDP in the following situations:

- LLT must be used over WANs
- When hardware, such as blade servers, do not support LLT over Ethernet

LLT over UDP is slower than LLT over Ethernet. Use LLT over UDP only when the hardware configuration makes it necessary.

## Manually configuring LLT over UDP using IPv4

The following checklist is to configure LLT over UDP:

- Make sure that the LLT private links are on separate subnets. Set the broadcast address in /etc/lltab explicitly depending on the subnet for each link.

See "Broadcast address in the /etc/llttab file" on page 532.

- 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 534.
- Set the broadcast address correctly for direct-attached (non-routed) links.
  See "Sample configuration: direct-attached links" on page 536.
- 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 538.

## Broadcast address in the /etc/llttab file

The broadcast address is set explicitly for each link in the following example.

- Display the content of the /etc/llttab file on the first node sys1:

```
sys1 # cat /etc/llttab

set-node sys1
set-cluster 1
link link1 /dev/udp - udp  50000  -  192.168.9.1 192.168.9.255
link link2 /dev/udp - udp  50001  -  192.168.10.1 192.168.10.255
```

  Verify the subnet mask using the ifconfig command to ensure that the two links are on separate subnets.

- Display the content of the /etc/llttab file on the second node sys2:

```
sys2 # cat /etc/llttab

set-node sys2
set-cluster 1
link link1 /dev/udp - udp  50000  -  192.168.9.2 192.168.9.255
link link2 /dev/udp - udp  50001  -  192.168.10.2 192.168.10.255
```

  Verify the subnet mask using the ifconfig command to ensure that the two links are on separate subnets.

# The link command in the /etc/lltab file

Review the link command information in this section for the /etc/lltab file. See the following information for sample configurations:

- See "Sample configuration: direct-attached links" on page 536.
- See "Sample configuration: links crossing IP routers" on page 538.

Table J-1 describes the fields of the link command that are shown in the /etc/lltab file examples. Note that some of the fields differ from the command for standard LLT links.

**Table J-1** Field description for link command in /etc/lltab

| Field | Description |
|---|---|
| *tag-name* | A unique string that is used as a tag by LLT; for example link1, link2,.... |
| *device* | The device path of the UDP protocol; for example /dev/udp. |
| *node-range* | Nodes using the link. "-" indicates all cluster nodes are to be configured for this link. |
| *link-type* | Type of link; must be "udp" for LLT over UDP. |
| *udp-port* | Unique UDP port in the range of 49152-65535 for the link.<br>See "Selecting UDP ports" on page 534. |
| *MTU* | "-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the `lltstat -l` command to display the current value. |
| *IP address* | IP address of the link on the local node. |
| *bcast-address* | ■ For clusters with enabled broadcasts, specify the value of the subnet broadcast address.<br>■ "-" is the default for clusters spanning routers. |

# The set-addr command in the /etc/lltab file

The `set-addr` command in the /etc/lltab file is required when the broadcast feature of LLT is disabled, such as when LLT must cross IP routers.

See "Sample configuration: links crossing IP routers" on page 538.

Table J-2 describes the fields of the set-addr command.

**Table J-2** Field description for set-addr command in /etc/lltab

| Field | Description |
|---|---|
| *node-id* | The ID of the cluster node; for example, 0. |
| *link tag-name* | The string that LLT uses to identify the link; for example link1, link2,.... |
| *address* | IP address assigned to the link for the peer node. |

## Selecting UDP ports

When you select a UDP port, select an available 16-bit integer from the range that follows:

- Use available ports in the private range 49152 to 65535
- Do not use the following ports:
  - Ports from the range of well-known ports, 0 to 1023
  - Ports from the range of registered ports, 1024 to 49151

To check which ports are defined as defaults for a node, examine the file /etc/services. You should also use the `netstat` command to list the UDP ports currently in use. For example:

```
# netstat -a | more
UDP
   Local Address         Remote Address     State
-------------------- -------------------- -------
      *.sunrpc                            Idle
      *.*                                 Unbound
      *.32771                             Idle
      *.32776                             Idle
      *.32777                             Idle
      *.name                              Idle
      *.biff                              Idle
      *.talk                              Idle
      *.32779                             Idle
.
.
.
      *.55098                             Idle
      *.syslog                            Idle
```

```
*.58702                              Idle
*.*                                  Unbound
```

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the /etc/services file, its associated name is displayed rather than the port number in the output.

## Configuring the netmask for LLT

For nodes on different subnets, set the netmask so that the nodes can access the subnets in use. Run the following command and answer the prompt to set the netmask:

```
# ifconfig interface_name netmask netmask
```

For example:

- For the first network interface on the node sys1:

  ```
  IP address=192.168.9.1, Broadcast address=192.168.9.255,
  Netmask=255.255.255.0
  ```

  For the first network interface on the node sys2:

  ```
  IP address=192.168.9.2, Broadcast address=192.168.9.255,
  Netmask=255.255.255.0
  ```

- For the second network interface on the node sys1:

  ```
  IP address=192.168.10.1, Broadcast address=192.168.10.255,
  Netmask=255.255.255.0
  ```

  For the second network interface on the node sys2:

  ```
  IP address=192.168.10.2, Broadcast address=192.168.10.255,
  Netmask=255.255.255.0
  ```

## Configuring the broadcast address for LLT

For nodes on different subnets, set the broadcast address in /etc/lltab depending on the subnet that the links are on.

An example of a typical /etc/lltab file when nodes are on different subnets. Note the explicitly set broadcast address for each link.

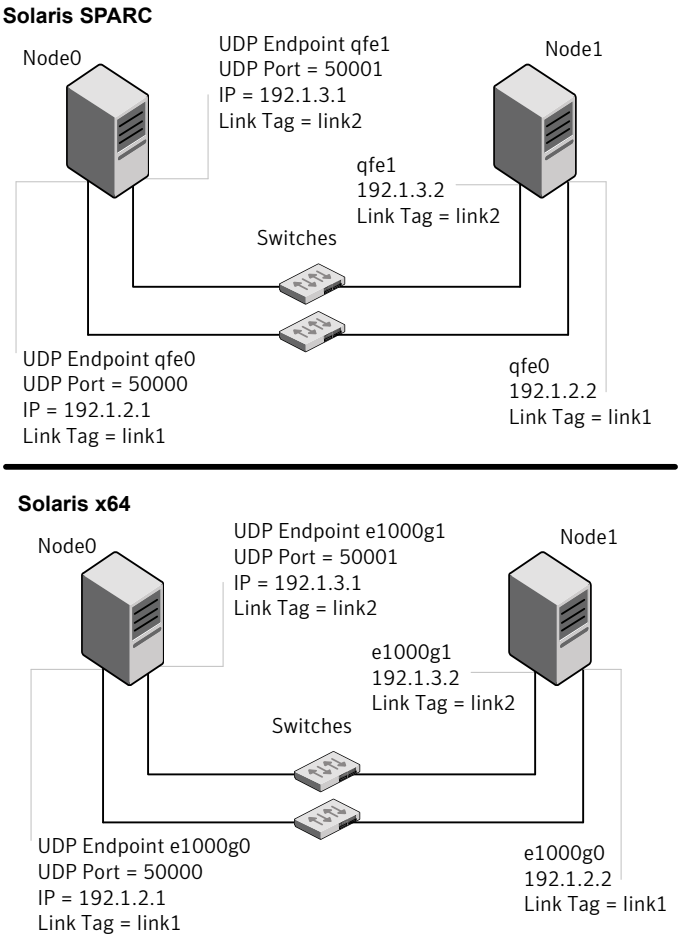
```
# cat /etc/llttab
set-node nodexyz
set-cluster 100

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/lltab file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT broadcasts requests peer nodes to discover their addresses. So the addresses of peer nodes do not need to be specified in the /etc/lltab file using the `set-addr` command. For direct attached links, you do need to set the broadcast address of

the links in the /etc/llttab file. Verify that the IP addresses and broadcast addresses are set correctly by using the `ifconfig -a` command.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.1 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.1 192.1.3.255
```

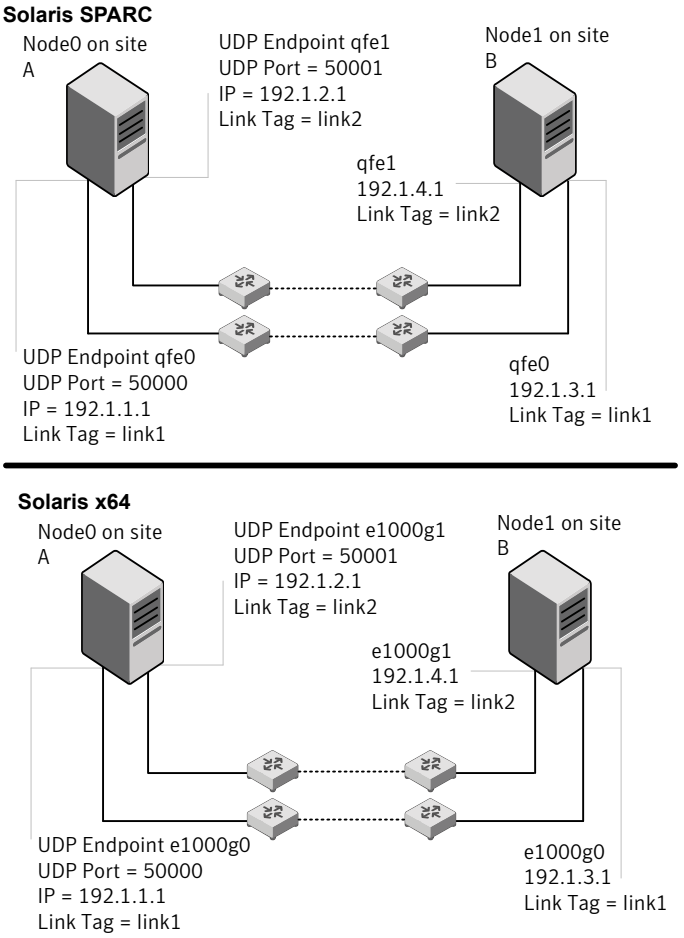
The file for Node 1 resembles:

```
set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.2 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.2 192.1.3.255
```

## Sample configuration: links crossing IP routers

Figure 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/lltab` 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/lltab` 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/lltab` 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
```

# Using the UDP layer of IPv6 for LLT

Veritas Storage Foundation Cluster File System High Availability 6.0.1 provides the option of using LLT over the UDP (User Datagram Protocol) layer for clusters using wide-area networks and routers. UDP makes LLT packets routable and thus able to span longer distances more economically.

## When to use LLT over UDP

Use LLT over UDP in the following situations:

- LLT must be used over WANs
- When hardware, such as blade servers, do not support LLT over Ethernet

# Manually configuring LLT over UDP using IPv6

The following checklist is to configure LLT over UDP:

- For UDP6, the multicast address is set to "-".
- Make sure that each NIC has an IPv6 address that is configured before configuring LLT.
- Make sure the IPv6 addresses in the /etc/lltab files are consistent with the IPv6 addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port.
  See "Selecting UDP ports" on page 542.
- For the links that cross an IP router, disable multicast features and specify the IPv6 address of each link manually in the /etc/lltab file.
  See "Sample configuration: links crossing IP routers" on page 545.

## The link command in the /etc/lltab file

Review the link command information in this section for the /etc/lltab file. See the following information for sample configurations:

- See "Sample configuration: direct-attached links" on page 544.
- See "Sample configuration: links crossing IP routers" on page 545.

Note that some of the fields in Table J-3 differ from the command for standard LLT links.

Table J-3 describes the fields of the link command that are shown in the /etc/lltab file examples.

**Table J-3** Field description for link command in /etc/lltab

| Field | Description |
|---|---|
| *tag-name* | A unique string that is used as a tag by LLT; for example link1, link2,.... |
| *device* | The device path of the UDP protocol; for example /dev/udp6. |

**Table J-3** Field description for link command in /etc/lltab *(continued)*

| Field | Description |
|---|---|
| *node-range* | Nodes using the link. "-" indicates all cluster nodes are to be configured for this link. |
| *link-type* | Type of link; must be "udp6" for LLT over UDP. |
| *udp-port* | Unique UDP port in the range of 49152-65535 for the link.<br>See "Selecting UDP ports" on page 542. |
| *MTU* | "-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the `lltstat -l` command to display the current value. |
| *IPv6 address* | IPv6 address of the link on the local node. |
| *mcast-address* | "-" is the default for clusters spanning routers. |

## The set-addr command in the /etc/lltab file

The `set-addr` command in the /etc/lltab file is required when the multicast feature of LLT is disabled, such as when LLT must cross IP routers.

See "Sample configuration: links crossing IP routers" on page 545.

Table J-4 describes the fields of the set-addr command.

**Table J-4** Field description for set-addr command in /etc/lltab

| Field | Description |
|---|---|
| *node-id* | The ID of the cluster node; for example, 0. |
| *link tag-name* | The string that LLT uses to identify the link; for example link1, link2,.... |
| *address* | IPv6 address assigned to the link for the peer node. |

## Selecting UDP ports

When you select a UDP port, select an available 16-bit integer from the range that follows:

- Use available ports in the private range 49152 to 65535
- Do not use the following ports:
  - Ports from the range of well-known ports, 0 to 1023

- Ports from the range of registered ports, 1024 to 49151

To check which ports are defined as defaults for a node, examine the file /etc/services. You should also use the `netstat` command to list the UDP ports currently in use. For example:

```
# netstat -a |  more

UDP: IPv4
   Local Address        Remote Address      State
-------------------- -------------------- ----------
      *.sunrpc                            Idle
      *.*                                 Unbound
      *.32772                             Idle
      *.*                                 Unbound
      *.32773                             Idle
      *.lockd                             Idle
      *.32777                             Idle
      *.32778                             Idle
      *.32779                             Idle
      *.32780                             Idle
      *.servicetag                        Idle
      *.syslog                            Idle
      *.16161                             Idle
      *.32789                             Idle
      *.177                               Idle
      *.32792                             Idle
      *.32798                             Idle
      *.snmpd                             Idle
      *.32802                             Idle
      *.*                                 Unbound
      *.*                                 Unbound
      *.*                                 Unbound

UDP: IPv6
   Local Address             Remote Address           State      If
------------------------ ------------------------ ---------- -----
      *.servicetag                                 Idle
      *.177                                        Idle
```

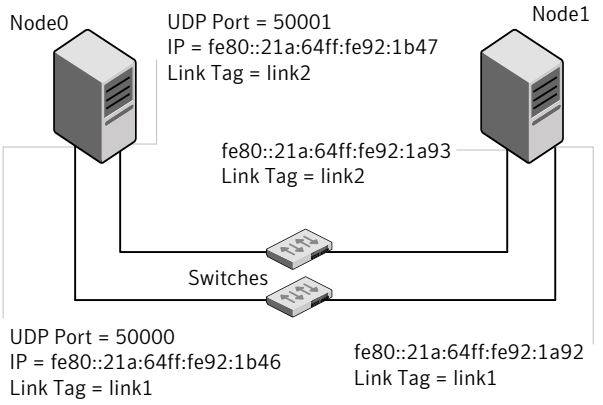
Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the /etc/services file, its associated name is displayed rather than the port number in the output.

# Sample configuration: direct-attached links

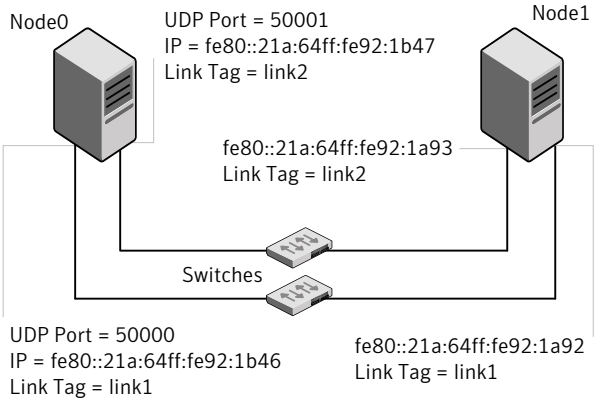
Figure J-3 depicts a typical configuration of direct-attached links employing LLT over UDP.

**Figure J-3** A typical configuration of direct-attached links that use LLT over UDP

**Solaris SPARC**




**Solaris x64**




The configuration that the /etc/lltab file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT uses IPv6 multicast requests for peer node address discovery. So the addresses of peer nodes do not need to be specified in the /etc/lltab file using the `set-addr`

command. Use the `ifconfig -a` command to verify that the IPv6 address is set correctly.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address mcast-address
link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -
```

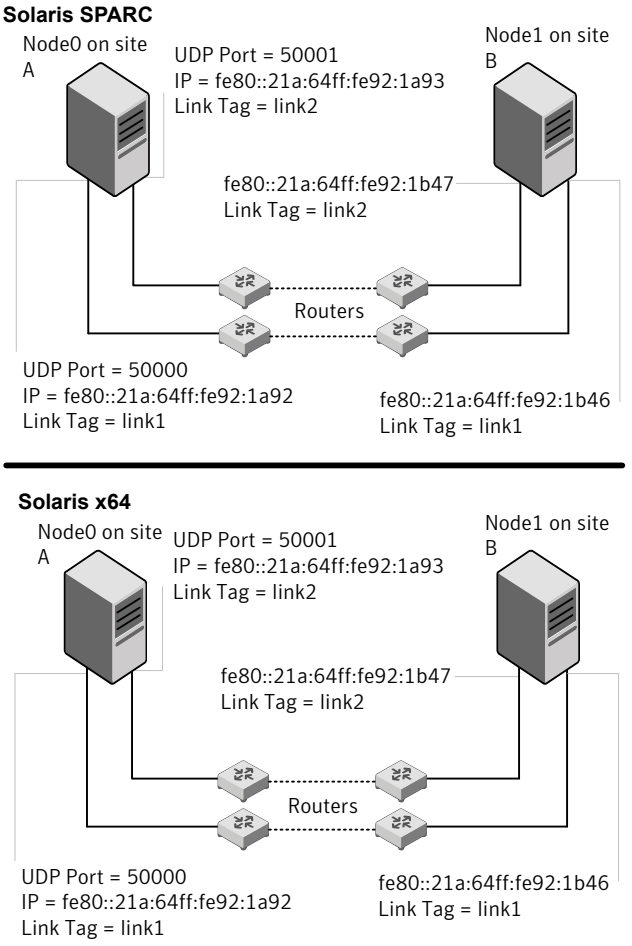
The file for Node 1 resembles:

```
set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address mcast-address
link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -
```

## Sample configuration: links crossing IP routers

Figure J-4 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-4** A typical configuration of links crossing an IP router




The configuration that the following `/etc/lltab` file represents for Node 1 has links crossing IP routers. Notice that IPv6 addresses are shown for each link on each peer node. In this configuration multicasts are disabled.

```
set-node Node1
set-cluster 1

link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -

#set address of each link for all peer nodes in the cluster
```

```
#format: set-addr node-id link tag-name address
set-addr 0 link1 fe80::21a:64ff:fe92:1b46
set-addr 0 link2 fe80::21a:64ff:fe92:1b47
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb     0
set-arp         0
```

The `/etc/llttab` file on Node 0 resembles:

```
set-node Node0
set-cluster 1

link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -
link link2 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 1 link1 fe80::21a:64ff:fe92:1a92
set-addr 1 link2 fe80::21a:64ff:fe92:1a93
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb     0
set-arp         0
```

Appendix K

# Compatability issues when installing Storage Foundation Cluster File System High Availability with other products

This appendix includes the following topics:


- Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present
- Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present
- Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present


## Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.

# Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host packages as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

# Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx, VRTSicsco, and VRTSat.

# Index


## A

adding
  users 112
agents
  about 484
  CFSfsckd 501
  CFSMount 497, 501
  CVMCluster 488
  CVMVolDg 494
  CVMVxconfigd 491
  disabling 378
  of VCS 485
applications, stopping 259
attributes
  about agent attributes 484
  CFSMount agent 498, 502
  CVMCluster agent 489
  CVMVolDg agent 489, 495
  CVMVxconfigd agent 492
  UseFence 224

## B

backup boot disk group 331–332
  rejoining 331
block device
  partitions
    example file name 524
  volumes
    example file name 524
bootdg 215

## C

cables
  cross-over Ethernet 396
CFS
  mount and unmount failures 508
  synchronization 40
  troubleshooting 508
CFSfsckd agent 501
  attributes 502
CFSMount agent 497, 501
  attributes 498
  entry points 498
  sample configuration 500–501
  type definition 500
CFSTypes.cf 500
cluster
  removing a node from 419
  verifying operation 355
cluster functionality
  enabling 217
  shared disks 218
command failures 510
commands
  format 61
  gabconfig 353
  hacf 266
  hastatus 355
  hasys 355
  lltconfig 449
  lltstat 351
  vxdisksetup (initializing disks) 124
  vxlicinst 119
  vxlicrep 118
configuration daemon (vxconfigd)
  starting 213
configuration file
  main.cf 347
configuring
  rsh 57
  shared disks 218
  ssh 57
configuring SFCFSHA
  script-based installer 99
configuring VCS
  adding users 112
  event notification 113–114
  global clusters 116
  starting 100
controllers
  SCSI 58

coordinator disks
DMP devices 28
for I/O fencing 28
setting up 222
creating
Flash archive 207
post-deployment scripts 208
CVM
CVMTypes.cf file 490
CVMCluster agent 488
attributes 489
entry points 489
sample configuration 490
type definition 490
CVMTypes.cf
definition, CVMCluster agent 490
definition, CVMVolDg agent 496
definition, CVMVxconfigd agent 493
CVMVolDg agent 494
attributes 495
entry points 494
sample configuration 497
type definition 496
CVMVxconfigd agent 491
attributes 492
CVMTypes.cf 493
entry points 491
sample configuration 494
type definition 493

## D

data disks
for I/O fencing 28
default disk group 215
defaultdg 215
devices
suppress devices 215
disabling the agents 378
disk groups
bootdg 215
default 215
nodg 215
root 215
rootdg 212, 215
disks
adding and initializing 124
coordinator 222
testing with vxfentsthdw 125
verifying node access 126

## E

Ethernet controllers 396

## F

FC-AL controllers 61
Fibre Channel fabric 49
files
main.cf 347
flarcreate 207
Flash archive 207
post-deployment scripts 208
freezing service groups 259

## G

GAB
port membership information 353
verifying 353
gabconfig command 353
-a (verifying GAB) 353
gabtab file
verifying after installation 449
global clusters
configuration 116

## H

hastatus -summary command 355
hasys -display command 355
high availability issues 511
low memory 511
network partition 510
hubs
independent 396

## I

I/O daemon (vxiod)
starting 213
I/O fencing
checking disks 125
setting up 221
shared storage 125
I/O fencing requirements
non-SCSI-3 37
Installing
SFCFSHA with the Web-based installer 146
installing
JumpStart 203
post 117

intelligent resource monitoring
disabling manually 485
enabling manually 485

## J

jeopardy 510–511
JumpStart
installing 203

## L

language packages
removal 384
license keys
adding with vxlicinst 119
replacing demo key 119
licenses
information about 118
links
private network 449
Live Upgrade
preparing 312
upgrade paths 308
upgrading Solaris on alternate boot disk 316
LLT
interconnects 48
verifying 351
lltconfig command 449
llthosts file
verifying after installation 449
lltstat command 351
lltab file
verifying after installation 449
localized environment settings for using VVR
settings for uisng VVR in a localized environment 256
log files 512

## M

main.cf file 347
main.cf files 454
major and minor numbers
checking 525, 528
shared devices 524
manual pages
potential problems 510
troubleshooting 510
media speed 48
optimizing 47
membership information 353
mount command
potential problems 509
mounting
software disc 63

## N

network partition 510
NFS services
shared storage 524
nodes
adding application nodes
configuring GAB 403
configuring LLT 403
configuring VXFEN 403
starting Volume Manager 403
preparing application nodes
configuring CVM 409
removing a node from a cluster
tasks 418
removing nodes
GAB configuration 421
LLT configuration 421
modifying VCS configuration 422
nodg 215
non-SCSI-3 fencing
manual configuration 239
setting up 239
non-SCSI-3 I/O fencing
requirements 37
non-SCSI3 fencing
setting up 137
using installsfcfsha 137
NTP
network time protocol daemon 40

## O

optimizing
media speed 47

## P

PATH variable
VCS commands 350
persistent reservations
SCSI-3 58
planning to upgrade VVR 253
port a
membership 353

port h
membership 353
port membership information 353
post-deployment scripts 208
preinstallation 253
preparing
Live Upgrade 312
preparing to upgrade VVR 259
Prevent Multipathing/Suppress Devices from VxVM's view 215
problems
accessing manual pages 510
executing file system commands 510
mounting and unmounting file systems 509

## Q

Quick I/O
performance on CFS 510

## R

rejoining
backup boot disk group 331
removing
the Replicated Data Set 379
removing a node from a cluster
editing VCS configuration files 420
procedure 419
tasks 418
Replicated Data Set
removing the 379
rolling upgrade 272, 275
versions 272
root disk group 212, 215
rootdg 215
rsh 100
configuration 57

## S

SAN
see Storage Area Network 49
script-based installer
SFCFSHA configuration overview 99
SCSI driver
determining instance numbers 526
SCSI-3
persistent reservations 58
SCSI-3 persistent reservations
verifying 221
service groups
freezing 259
settings for uisng VVR in a localized environment
localized environment settings for using VVR 256
SFCFSHA
configuring 99
coordinator disks 222
SFCFSHA installation
verifying
cluster operations 350
GAB operations 350
LLT operations 350
shared disks, configuring 218
shared storage
Fibre Channel
setting up 61
NFS services 524
SMTP email notification 113
SNMP trap notification 114
split brain 510
ssh 100
configuration 57
starting configuration
installvcs program 100
Veritas product installer 100
starting vxconfigd configuration daemon 213
starting vxiod daemon 213
stopping
applications 259
storage
setting up shared fibre 61
Storage Area Network 49
suppress devices 215
system state attribute value 355

## T

troubleshooting
accessing manual pages 510
executing file system commands 510
mounting and unmounting file systems 509
tunables file
about setting parameters 437
parameter definitions 442
preparing 441
setting for configuration 438
setting for installation 438
setting for upgrade 438
setting parameters 441
setting with no other operations 439

tunables file *(continued)*
setting with un-integrated response file 440

## U

unsuccessful upgrade 332
upgrade paths
Live Upgrade 308
upgrading
rolling 272
upgrading VVR
from 4.1 254
planning 253
preparing 259
using Live Upgrade 308

## V

VCS
command directory path variable 350
verifying installation
kernel component 345
Veritas Operations Manager 26
Volume Manager
Fibre Channel 61
vradmin
delpri 380
stoprep 380
VVR
global cluster overview 364
VVR 4.1
planning an upgrade from 254
vxconfigd configuration daemon
starting 213
vxdctl mode command 213
vxdisksetup command 124
vxinstall program 214–216
vxinstall program, running 214
vxiod I/O daemon
starting 213
vxlicinst command 119
vxlicrep command 118

## W

Web-based installer 146