Veritas™ Cluster Server Installation Guide

Linux

6.0.2
Veritas Cluster Server 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: 6.0.2

Document version: 6.0.2 Rev 2

Legal Notice

Copyright © 2013 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.
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
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.


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

About Symantec Connect

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

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

Technical Support ............................................................................................................. 4

**Section 1** Installation overview and planning .................................................. 19

**Chapter 1** Introducing Veritas Cluster Server ..................................................... 21

- About Veritas Cluster Server ......................................................................................... 21
- About VCS basics ............................................................................................................. 21
  - About multiple nodes .................................................................................................. 22
  - About shared storage .................................................................................................. 22
  - About LLT and GAB .................................................................................................... 23
  - About network channels for heartbeating .................................................................. 23
  - About preexisting network partitions ....................................................................... 24
  - About VCS seeding ..................................................................................................... 24
- About VCS features ....................................................................................................... 25
  - About VCS notifications ............................................................................................ 25
  - About global clusters .................................................................................................. 25
  - About I/O fencing ........................................................................................................ 25
- About VCS optional components .................................................................................. 26
  - About Veritas Operations Manager .......................................................................... 27
  - About Cluster Manager (Java Console) ..................................................................... 27
  - About VCS Simulator .................................................................................................. 27
- About Symantec Operations Readiness Tools ................................................................. 28
- About configuring VCS clusters for data integrity ............................................................ 28
  - About I/O fencing for VCS in virtual machines that do not support
    SCSI-3 PR .................................................................................................................. 29
  - About I/O fencing components .................................................................................. 29
  - About preferred fencing .............................................................................................. 31

**Chapter 2** System requirements .................................................................................. 33

- Important preinstallation information for VCS ............................................................ 33
- Hardware requirements for VCS ..................................................................................... 34
- Disk space requirements ................................................................................................. 35
- Supported operating systems .......................................................................................... 35
- Supported software for VCS .......................................................................................... 35
Getting your VCS installation and configuration information ready ................................................................. 70

Section 3  
Installation using the script-based installer ........................................................................................................... 77

Chapter 6  
Installing VCS ..................................................................................................................................................... 79
Installing VCS using the installer ........................................................................................................................... 79
Encrypting a password .............................................................................................................................................. 84

Chapter 7  
Preparing to configure VCS clusters for data integrity ......................................................................................... 87
About planning to configure I/O fencing .................................................................................................................. 87
Typical VCS cluster configuration with disk-based I/O fencing ........................................................................... 91
Typical VCS cluster configuration with server-based I/O fencing ...................................................................... 92
Recommended CP server configurations ............................................................................................................. 92
Setting up the CP server ....................................................................................................................................... 95
Planning your CP server setup ................................................................................................................................ 95
Installing the CP server using the installer ........................................................................................................... 96
Configuring the CP server cluster in secure mode .................................................................................................. 97
Setting up shared storage for the CP server database .......................................................................................... 97
Configuring the CP server using the installer program ........................................................................................ 98
Configuring the CP server manually ..................................................................................................................... 108
Configuring CP server using response files ........................................................................................................ 109
Verifying the CP server configuration ................................................................................................................... 113

Chapter 8  
Configuring VCS .................................................................................................................................................... 115
Overview of tasks to configure VCS using the script-based installer ......................................................................... 116
Starting the software configuration ........................................................................................................................ 117
Specifying systems for configuration .................................................................................................................... 117
Configuring the cluster name .................................................................................................................................. 118
Configuring private heartbeat links ........................................................................................................................ 118
Configuring the virtual IP of the cluster ................................................................................................................... 122
Configuring Veritas Cluster Server in secure mode ................................................................................................ 124
Setting up trust relationships for your VCS cluster ................................................................................................. 125
Configuring a secure cluster node by node ............................................................................................................. 126
Configuring the first node ....................................................................................................................................... 127
Chapter 12  Performing an automated I/O fencing configuration using response files ................................................. 181

Configuring I/O fencing using response files ................................. 181
Response file variables to configure disk-based I/O fencing ............... 182
Sample response file for configuring disk-based I/O fencing .......... 185
Response file variables to configure server-based I/O fencing .......... 186
Sample response file for configuring server-based I/O fencing ........ 187
Response file variables to configure non-SCSI-3 server-based I/O fencing ............................................................... 188
Sample response file for configuring non-SCSI-3 server-based I/O fencing ............................................................... 189

Section 5  Manual installation .................................................. 191

Chapter 13  Performing preinstallation tasks .................................... 193

Preparing for a manual installation ............................................. 193
Requirements for installing VCS ................................................ 193

Chapter 14  Manually installing VCS .............................................. 195

About VCS manual installation .................................................. 195
Installing VCS software manually ............................................. 195
  Viewing the list of VCS RPMs .................................................. 196
  Installing VCS RPMs for a manual installation ......................... 197
  Adding a license key for a manual installation ......................... 199
  Copying the installation guide to each node ............................. 201

Chapter 15  Manually configuring VCS ........................................ 203

About configuring VCS manually ............................................. 203
Configuring LLT manually ..................................................... 203
  Setting up /etc/Ilthosts for a manual installation ..................... 204
  Setting up /etc/llttab for a manual installation ...................... 204
  About LLT directives in /etc/llttab file ................................. 205
  Additional considerations for LLT for a manual installation ........ 207
Configuring GAB manually .................................................... 207
Configuring VCS manually .................................................... 207
  Configuring the cluster UUID when creating a cluster manually ................. 209
Configuring VCS in single node mode ..................................... 209
Starting LLT, GAB, and VCS after manual configuration .............. 209
Modifying the VCS configuration .......................................... 211
Chapter 16  Manually configuring the clusters for data integrity ................................................................. 213

Setting up disk-based I/O fencing manually ................................................................. 213
Identifying disks to use as coordinator disks ............................................................... 214
Setting up coordinator disk groups ........................................................................... 214
Creating I/O fencing configuration files ..................................................................... 215
Modifying VCS configuration to use I/O fencing ...................................................... 216
Verifying I/O fencing configuration ............................................................................ 218
Setting up server-based I/O fencing manually ........................................................... 218
Preparing the CP servers manually for use by the VCS cluster .................................. 219
Configuring server-based fencing on the VCS cluster manually ................................... 222
Configuring CoordPoint agent to monitor coordination points ................................... 228
Verifying server-based I/O fencing configuration ..................................................... 230
Setting up non-SCSI-3 fencing in virtual environments manually .............................. 231
Sample /etc/vxfenmode file for non-SCSI-3 fencing .................................................. 233

Section 6  Upgrading VCS ......................................................................................... 237

Chapter 17  Planning to upgrade VCS .......................................................................... 239

About upgrading to VCS 6.0.2 .................................................................................. 239
Supported VCS upgrade paths ................................................................................... 240
Upgrading VCS in secure enterprise environments .................................................... 240
Considerations for upgrading secure VCS 5.x clusters to VCS 6.0.2 ............................. 241
Considerations for upgrading secure CP servers ....................................................... 242
Considerations for upgrading secure CP clients ....................................................... 242
Setting up trust relationship between CP server and CP clients manually ............... 242

Chapter 18  Performing a typical VCS upgrade using the installer ................................. 245

Before upgrading using the script-based installer ...................................................... 245
Upgrading VCS using the script-based installer ....................................................... 246
<table>
<thead>
<tr>
<th>Chapter 19</th>
<th>Performing an automated VCS upgrade using response files</th>
<th>249</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Upgrading VCS using response files</td>
<td>249</td>
</tr>
<tr>
<td></td>
<td>Response file variables to upgrade VCS</td>
<td>250</td>
</tr>
<tr>
<td></td>
<td>Sample response file for upgrading VCS</td>
<td>251</td>
</tr>
<tr>
<td>Section 7</td>
<td>Post-installation tasks</td>
<td>253</td>
</tr>
<tr>
<td>Chapter 20</td>
<td>Performing post-installation tasks</td>
<td>255</td>
</tr>
<tr>
<td></td>
<td>About enabling LDAP authentication for clusters that run in secure mode</td>
<td>255</td>
</tr>
<tr>
<td></td>
<td>Enabling LDAP authentication for clusters that run in secure mode</td>
<td>257</td>
</tr>
<tr>
<td></td>
<td>Accessing the VCS documentation</td>
<td>262</td>
</tr>
<tr>
<td></td>
<td>Removing permissions for communication</td>
<td>262</td>
</tr>
<tr>
<td>Chapter 21</td>
<td>Installing or upgrading VCS components</td>
<td>263</td>
</tr>
<tr>
<td></td>
<td>Installing the Java Console</td>
<td>263</td>
</tr>
<tr>
<td></td>
<td>Software requirements for the Java Console</td>
<td>263</td>
</tr>
<tr>
<td></td>
<td>Installing the Java Console on Linux</td>
<td>264</td>
</tr>
<tr>
<td></td>
<td>Installing the Java Console on a Windows system</td>
<td>265</td>
</tr>
<tr>
<td></td>
<td>Upgrading the Java Console</td>
<td>265</td>
</tr>
<tr>
<td></td>
<td>Installing VCS Simulator</td>
<td>266</td>
</tr>
<tr>
<td></td>
<td>Software requirements for VCS Simulator</td>
<td>266</td>
</tr>
<tr>
<td></td>
<td>Installing VCS Simulator on Windows systems</td>
<td>266</td>
</tr>
<tr>
<td></td>
<td>Reviewing the installation</td>
<td>266</td>
</tr>
<tr>
<td></td>
<td>Upgrading VCS Simulator</td>
<td>267</td>
</tr>
<tr>
<td></td>
<td>Upgrading the VCS agents</td>
<td>268</td>
</tr>
<tr>
<td>Chapter 22</td>
<td>Verifying the VCS installation</td>
<td>269</td>
</tr>
<tr>
<td></td>
<td>About verifying the VCS installation</td>
<td>269</td>
</tr>
<tr>
<td></td>
<td>About the cluster UUID</td>
<td>269</td>
</tr>
<tr>
<td></td>
<td>Verifying the LLT, GAB, and VCS configuration files</td>
<td>270</td>
</tr>
<tr>
<td></td>
<td>Verifying LLT, GAB, and cluster operation</td>
<td>270</td>
</tr>
<tr>
<td></td>
<td>Verifying LLT</td>
<td>271</td>
</tr>
<tr>
<td></td>
<td>Verifying GAB</td>
<td>273</td>
</tr>
<tr>
<td></td>
<td>Verifying the cluster</td>
<td>274</td>
</tr>
<tr>
<td></td>
<td>Verifying the cluster nodes</td>
<td>275</td>
</tr>
<tr>
<td></td>
<td>Performing a postcheck on a node</td>
<td>278</td>
</tr>
</tbody>
</table>
About using the postcheck option ......................................................... 278

Section 8 Adding and removing cluster nodes ................................. 281

Chapter 23 Adding a node to a single-node cluster .......................... 283
Adding a node to a single-node cluster .............................................. 283
Setting up a node to join the single-node cluster .............................. 284
Installing and configuring Ethernet cards for private
network ..................................................................................... 285
Configuring the shared storage .................................................... 286
Bringing up the existing node ...................................................... 286
Installing the VCS software manually when adding a node to a
single node cluster .................................................................... 287
Creating configuration files ....................................................... 287
Starting LLT and GAB ................................................................. 287
Reconfiguring VCS on the existing node ....................................... 288
Verifying configuration on both nodes ......................................... 289

Chapter 24 Adding a node to a multi-node VCS cluster ..................... 291
Adding nodes using the VCS installer ............................................ 291
Manually adding a node to a cluster ............................................ 293
Setting up the hardware ............................................................ 294
Installing the VCS software manually when adding a node ............ 295
Setting up the node to run in secure mode .................................. 296
Configuring LLT and GAB when adding a node to the
cluster ...................................................................................... 299
Configuring I/O fencing on the new node ..................................... 302
Adding the node to the existing cluster ....................................... 305
Starting VCS and verifying the cluster ....................................... 306

Chapter 25 Removing a node from a VCS cluster ............................ 307
Removing a node from a VCS cluster ........................................... 307
Verifying the status of nodes and service groups ......................... 308
Deleting the departing node from VCS configuration .................. 309
Modifying configuration files on each remaining node .............. 312
Removing the node configuration from the CP server .................. 312
Removing security credentials from the leaving node ................. 313
Unloading LLT and GAB and removing VCS on the departing
node ...................................................................................... 314
Section 9 Uninstallation of VCS ......................................................... 317
Chapter 26 Uninstalling VCS using the installer .............................. 319
Preparing to uninstall VCS .............................................................. 319
Uninstalling VCS using the script-based installer ............................ 319
  Removing VCS 6.0.2 RPMs ....................................................... 320
  Running uninstallvcs from the VCS 6.0.2 disc ............................ 321
Removing the CP server configuration using the installer program ....................................................... 321
Chapter 27 Uninstalling VCS using response files ......................... 325
Uninstalling VCS using response files ........................................... 325
Response file variables to uninstall VCS ....................................... 326
Sample response file for uninstalling VCS ................................. 327
Chapter 28 Manually uninstalling VCS .......................................... 329
Removing VCS RPMs manually .................................................... 329
Manually remove the CP server fencing configuration ................ 330
Manually deleting cluster details from a CP server ....................... 331
Section 10 Installation reference .................................................... 335
Appendix A Services and ports ...................................................... 337
  About SFHA services and ports .................................................. 337
Appendix B VCS installation RPMs .............................................. 341
  Veritas Cluster Server installation RPMs ................................. 341
Appendix C Installation command options .................................... 345
  Installation script options ....................................................... 345
  Command options for uninstallvcs program ............................ 349
Appendix D Changes to bundled agents in VCS 6.0.2 ...................... 351
  Deprecated agents ............................................................... 351
  New agents ........................................................................... 352
  New and modified attributes for 6.0.1 agents ............................ 352
  Manually removing deprecated resource types and modifying attributes ....................................................... 366
Creating new VCS accounts if you used native operating system accounts ............................................................. 367

Appendix E Configuration files ............................................................. 369
- About the LLT and GAB configuration files ............................................................. 369
- About the AMF configuration files ............................................................. 372
- About the VCS configuration files ......................................................................... 373
  - Sample main.cf file for VCS clusters ............................................................. 375
  - Sample main.cf file for global clusters ............................................................. 376
- About I/O fencing configuration files ...................................................................... 379
- Sample configuration files for CP server ............................................................. 381
  - Sample main.cf file for CP server hosted on a single node that runs VCS ................. 382
  - Sample main.cf file for CP server hosted on a two-node SFHA cluster ............................................................. 384
  - Sample CP server configuration (/etc/vxcps.conf) file output ............................................................. 387

Appendix F Installing VCS on a single node ............................................................. 389
- About installing VCS on a single node ............................................................. 389
- Creating a single-node cluster using the installer program ............................................................. 390
  - Preparing for a single node installation ............................................................. 390
  - Starting the installer for the single node cluster ............................................................. 390
- Creating a single-node cluster manually ............................................................. 391
- Setting the path variable for a manual single node installation ............................................................. 391
- Installing VCS software manually on a single node ............................................................. 392
- Modifying the startup files ..................................................................................... 392
- Configuring VCS ..................................................................................... 392
- Verifying single-node operation ..................................................................................... 392

Appendix G Configuring LLT over UDP ............................................................. 393
- Using the UDP layer for LLT ..................................................................................... 393
  - When to use LLT over UDP ..................................................................................... 393
- Manually configuring LLT over UDP using IPv4 ............................................................. 393
  - Broadcast address in the /etc/llttab file ............................................................. 394
  - The link command in the /etc/llttab file ............................................................. 395
  - The set-addr command in the /etc/llttab file ............................................................. 395
- Selecting UDP ports ..................................................................................... 396
- Configuring the netmask for LLT ..................................................................................... 396
- Configuring the broadcast address for LLT ..................................................................................... 397
- Sample configuration: direct-attached links ..................................................................................... 397
Sample configuration: links crossing IP routers ................................................. 399
Manually configuring LLT over UDP using IPv6 .............................................. 400
The link command in the /etc/llttab file ...................................................... 401
The set-addr command in the /etc/llttab file .............................................. 401
Selecting UDP ports .................................................................................. 402
Sample configuration: direct-attached links ............................................... 402
Sample configuration: links crossing IP routers ....................................... 404
LLT over UDP sample /etc/llttab ............................................................... 405

Appendix H   Configuring the secure shell or the remote shell for communications .................................................. 407
Setting up inter-system communication ................................................... 407
Setting up ssh on cluster systems ......................................................... 407
Configuring ssh ................................................................................... 408

Appendix I   Troubleshooting VCS installation .............................................. 411
What to do if you see a licensing reminder ............................................. 411
Restarting the installer after a failed connection .................................... 412
Starting and stopping processes for the Veritas products .................... 412
Installer cannot create UUID for the cluster ......................................... 413
LLT startup script displays errors ......................................................... 414
The vxfentshdw utility fails when SCSI TEST UNIT READY command fails ................................................................. 414
Issues during fencing startup on VCS cluster nodes set up for server-based fencing ................................................................. 415

Appendix J   Sample VCS cluster setup diagrams for CP server-based I/O fencing .............................................. 417
Configuration diagrams for setting up server-based I/O fencing ............ 417
Two unique client clusters served by 3 CP servers ............................... 417
Client cluster served by highly available CPS and 2 SCSI-3 disks .................................................................................. 418
Two node campus cluster served by remote CP server and 2 SCSI-3 disks .................................................................. 420
Multiple client clusters served by highly available CP server and 2 SCSI-3 disks ................................................................. 422

Contents
Appendix K  Compatibility issues when installing Veritas Cluster Server with other products ................................. 425

Installing, uninstalling, or upgrading Storage Foundation products
  when other Veritas products are present .................................. 425
Installing, uninstalling, or upgrading Storage Foundation products
  when VOM is already present ............................................. 426
Installing, uninstalling, or upgrading Storage Foundation products
  when ApplicationHA is already present .............................. 426
Installing, uninstalling, or upgrading Storage Foundation products
  when NetBackup is already present ................................. 427

Index ........................................................................................................................................ 429
Installation overview and planning

- Chapter 1. Introducing Veritas Cluster Server
- Chapter 2. System requirements
- Chapter 3. Planning to install VCS
- Chapter 4. Licensing VCS
Introducing Veritas Cluster Server

This chapter includes the following topics:

- About Veritas Cluster Server
- About VCS basics
- About VCS features
- About VCS optional components
- About Symantec Operations Readiness Tools
- About configuring VCS clusters for data integrity

About Veritas Cluster Server

Veritas™ Cluster Server by Symantec is a high-availability solution for applications and services configured in a cluster. Veritas Cluster Server (VCS) monitors systems and application services, and restarts services when hardware or software fails.

About VCS basics

A single VCS cluster consists of multiple systems that are connected in various combinations to storage devices. When a system is part of a VCS cluster, it is called a node. VCS monitors and controls applications running in the cluster on nodes, and restarts applications in response to a variety of hardware or software faults. Applications can continue to operate with little or no downtime. In some cases, such as NFS, this continuation is transparent to high-level applications and users.
In other cases, a user might have to retry an operation, such as a Web server reloading a page.

**Figure 1-1** illustrates a typical VCS configuration of four nodes that are connected to shared storage.

**Figure 1-1**  Example of a four-node VCS cluster

Client workstations receive service over the public network from applications running on VCS nodes. VCS monitors the nodes and their services. VCS nodes in the cluster communicate over a private network.

**About multiple nodes**

VCS runs in a replicated state on each node in the cluster. A private network enables the nodes to share identical state information about all resources. The private network also recognizes active nodes, nodes that join or leave the cluster, and failed nodes. The private network requires two communication channels to guard against network partitions.

**About shared storage**

A VCS hardware configuration typically consists of multiple nodes that are connected to shared storage through I/O channels. Shared storage provides multiple systems with an access path to the same data. It also enables VCS to restart applications on alternate nodes when a node fails, which ensures high availability.

VCS nodes can only access physically-attached storage.
**Figure 1-2** illustrates the flexibility of VCS shared storage configurations.

**Figure 1-2** Two examples of shared storage configurations

---

**About LLT and GAB**

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

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

GAB (Group Membership and Atomic Broadcast) provides globally ordered message that is required to maintain a synchronized state among the nodes.

---

**About network channels for heartbeating**

For the VCS private network, two network channels must be available to carry heartbeat information. These network connections also transmit other VCS-related information.

Each cluster configuration requires at least two network channels between the systems. The requirement for two channels protects your cluster against network partitioning. For more information on network partitioning, refer to the *Veritas Cluster Server Administrator’s Guide*.

**Figure 1-3** illustrates a two-node VCS cluster where the nodes galaxy and nebula have two private network connections.
About preexisting network partitions

A preexisting network partition refers to failure in the communication channels that occurs while the systems are down and VCS cannot respond. When the systems start, VCS seeding reduces vulnerability to network partitioning, regardless of the cause of the failure.

About VCS seeding

To protect your cluster from a preexisting network partition, VCS uses the concept of seeding. Seeding is a function of GAB that determines whether or not all nodes have joined a cluster. For this determination, GAB requires that you declare the number of nodes in the cluster. Note that only seeded nodes can run VCS.

GAB automatically seeds nodes under the following conditions:

- An unseeded node communicates with a seeded node
- All nodes in the cluster are unseeded but can communicate with each other

When the last system starts and joins the cluster, the cluster seeds and starts VCS on all nodes. You can then bring down and restart nodes in any combination. Seeding remains in effect as long as at least one instance of VCS is running somewhere in the cluster.

Perform a manual seed to run VCS from a cold start when one or more systems of the cluster are unavailable. VCS does not start service groups on a system until it has a seed. However, if you have I/O fencing enabled in your cluster, you can still configure GAB to automatically seed the cluster even when some cluster nodes are unavailable.

See the *Veritas Cluster Server Administrator's Guide*. 
About VCS features

VCS offers the following features that you can configure during VCS configuration:

- **VCS notifications**  
  See “About VCS notifications” on page 25.
- **VCS global clusters**  
  See “About global clusters” on page 25.
- **I/O fencing**  
  See “About I/O fencing” on page 25.

About VCS notifications

You can configure both Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) notifications for VCS. Symantec recommends you to configure at least one of these notifications. You have the following options:

- Configure SNMP trap notification of VCS events using the VCS Notifier component.
- Configure SMTP email notification of VCS events using the VCS Notifier component.

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

About global clusters

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

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

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 VCS, the installer installs the `VRTSvxfen` RPM, which includes the I/O fencing driver. To protect
data on shared disks, you must configure I/O fencing after you install and configure VCS.

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.

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.

Server-based I/O fencing ensures data integrity in clusters.

In virtualized environments that do not support SCSI-3 PR, VCS supports non-SCSI-3 server-based I/O fencing.

See “About I/O fencing for VCS in virtual machines that do not support SCSI-3 PR” on page 29.

---

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

---

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

---

### About VCS optional components

You can add the following optional components to VCS:

- **Veritas Operations Manager**
  
  See “About Veritas Operations Manager” on page 27.

- **Cluster Manager (Java console)**
  
  See “About Cluster Manager (Java Console)” on page 27.

- **VCS Simulator**
  
  See “About VCS Simulator” on page 27.
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.

If you want to manage a single cluster using Cluster Manager (Java Console), a version is available for download from http://go.symantec.com/vcsdm_download. You cannot manage the new features of this release using the Java Console. Veritas Cluster Server Management Console is deprecated.

About Cluster Manager (Java Console)

Cluster Manager (Java Console) offers administration capabilities for your cluster. Use the different views in the Java Console to monitor and manage clusters and Veritas Cluster Server (VCS) objects, including service groups, systems, resources, and resource types. You cannot manage the new features of releases 6.0 and later using the Java Console.

See Veritas Cluster Server Administrator's Guide.

You can download the console from http://go.symantec.com/vcsdm_download.

About VCS Simulator

VCS Simulator enables you to simulate and test cluster configurations. Use VCS Simulator to view and modify service group and resource configurations and test failover behavior. VCS Simulator can be run on a stand-alone system and does not require any additional hardware. You can install VCS Simulator only on a Windows operating system.

VCS Simulator runs an identical version of the VCS High Availability Daemon (HAD) as in a cluster, ensuring that failover decisions are identical to those in an actual cluster.

You can test configurations from different operating systems using VCS Simulator. For example, you can run VCS Simulator to test configurations for VCS clusters
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

About configuring VCS clusters for data integrity

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

About I/O fencing for VCS 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, VCS attempts to provide reasonable safety for the data disks. VCS 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 installvcs program” on page 156.

See “Setting up non-SCSI-3 fencing in virtual environments manually” on page 231.

About I/O fencing components

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

- Data disks—Store shared data
  See “About data disks” on page 30.
Coordination points—Act as a global lock during membership changes
See “About coordination points” on page 30.

About data disks
Data disks are standard disk devices for data storage and are either physical disks or RAID Logical Units (LUNs).
These disks must support SCSI-3 PR and must be part of standard VxVM disk groups. VxVM is responsible for fencing data disks on a disk group basis. Disks that are added to a disk group and new paths that are discovered for a device are automatically fenced.

About coordination points
Coordination points provide a lock mechanism to determine which nodes get to fence off data drives from other nodes. A node must eject a peer from the coordination points before it can fence the peer from the data drives. VCS 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 VCS 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 VCS cluster nodes to perform the following tasks:

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

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

See “Enabling or disabling the preferred fencing policy” on page 158.
System requirements

This chapter includes the following topics:

- Important preinstallation information for VCS
- Hardware requirements for VCS
- Disk space requirements
- Supported operating systems
- Supported software for VCS
- I/O fencing requirements
- Number of nodes supported
- Discovering product versions and various requirement information

**Important preinstallation information for VCS**

Before you install VCS, make sure that you have reviewed the following information:

- The hardware compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware visit the following URL:
  
  [http://www.symantec.com/docs/TECH170013](http://www.symantec.com/docs/TECH170013)

  Before installing or upgrading VCS, review the current compatibility list to confirm the compatibility of your hardware and software.

- For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:
  
  [http://www.symantec.com/docs/TECH164885](http://www.symantec.com/docs/TECH164885)

- You can install VCS on clusters of up to 64 systems.
Every system where you want to install VCS must meet the hardware and the software requirements.

## Hardware requirements for VCS

*Table 2-1* lists the hardware requirements for a VCS cluster.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCS nodes</td>
<td>From 1 to 64 Linux systems that run a supported Linux operating system version.</td>
</tr>
<tr>
<td>DVD drive</td>
<td>One drive in a system that can communicate to all the nodes in the cluster.</td>
</tr>
</tbody>
</table>
| Disks                       | Typical VCS configurations require that the applications are configured to use shared disks/storage to enable migration of applications between systems in the cluster.  
                                | The VCS I/O fencing feature requires that all data and coordinator disks support SCSI-3 Persistent Reservations (PR).  
                                | **Note:** VCS also supports non-SCSI3 server-based fencing configuration in virtual environments that do not support SCSI-3 PR-compliant storage. |
| Disk space                  | **Note:** VCS may require more temporary disk space during installation than the specified disk space.                                         |
| Network Interface Cards (NICs) | In addition to the built-in public NIC, VCS requires at least one more NIC per system. Symantec recommends two additional NICs.  
                                | You can also configure aggregated interfaces.  
                                | Symantec recommends that you turn off the spanning tree on the LLT switches, and set port-fast on. |
| Fibre Channel or SCSI host bus adapters | Typical VCS configuration requires at least one SCSI or Fibre Channel Host Bus Adapter per system for shared data disks. |
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 -precheck option of the script-based installer to determine whether there is sufficient space.

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

```
#/installer -precheck
```

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

```
#/installvcs program -precheck<version>
```

Where <version> is the specific release version.

Supported operating systems

For information on supported operating systems, see the Veritas Cluster Server Release Notes.

Supported software for VCS

VCS supports the following volume managers and file systems:

- ext2, ext3, reiserfs, NFS, and bind on LVM2, raw disks, and VxVM.
- ext4 and xfs on LVM2 and raw disks

VCS supports the following versions of Veritas Storage Foundation:

Veritas Storage Foundation: Veritas Volume Manager (VxVM) with Veritas File System (VxFS)

- Storage Foundation 6.0.1
  - VxVM 6.0.1 with VxFS 6.0.1
- Storage Foundation 6.0
  - VxVM 6.0 with VxFS 6.0

Note: VCS supports the previous and the next versions of Storage Foundation to facilitate product upgrades.
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 36.

- **CP servers**

To configure disk-based fencing or to configure server-based fencing with at least one coordinator disk, make sure a version of Veritas Volume Manager (VxVM) that supports SCSI-3 persistent reservations (SCSI-3 PR) is installed on the VCS cluster.

See the *Veritas Storage Foundation and High Availability Installation Guide*.

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

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

VCS 6.0.2 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 6.0.2, you must upgrade all the application clusters that use this CP server to version 6.0.2. 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 Storage Foundation High Availability Installation Guide.*

See “Hardware requirements for VCS” on page 34.

**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

<table>
<thead>
<tr>
<th>Hardware required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk space</td>
<td>To host the CP server on a VCS cluster or SFHA cluster, each host requires the following file system space:</td>
</tr>
<tr>
<td></td>
<td>■ 550 MB in the /opt directory (additionally, the language pack requires another 15 MB)</td>
</tr>
<tr>
<td></td>
<td>■ 300 MB in /usr</td>
</tr>
<tr>
<td></td>
<td>■ 20 MB in /var</td>
</tr>
<tr>
<td></td>
<td>■ 10 MB in /etc (for the CP server database)</td>
</tr>
<tr>
<td>Storage</td>
<td>When CP server is hosted on an SFHA cluster, there must be shared storage between the nodes of this SFHA cluster.</td>
</tr>
<tr>
<td>RAM</td>
<td>Each CP server requires at least 512 MB.</td>
</tr>
<tr>
<td>Network</td>
<td>Network hardware capable of providing TCP/IP connection between CP servers and VCS clusters (application clusters).</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>CP server hosted on a VCS single-node cluster or on an SFHA cluster</th>
<th>Operating system and version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP server supports any of the following operating systems:</td>
<td></td>
</tr>
<tr>
<td>■ RHEL 5</td>
<td></td>
</tr>
<tr>
<td>■ RHEL 6</td>
<td></td>
</tr>
<tr>
<td>■ SLES 10</td>
<td></td>
</tr>
<tr>
<td>■ SLES 11</td>
<td></td>
</tr>
</tbody>
</table>

Review other details such as supported operating system levels and architecture for the supported operating systems.

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 VCS cluster (application cluster) and the CP server, review the following support matrix:

<table>
<thead>
<tr>
<th>Communication mode</th>
<th>CP server in secure mode</th>
<th>CP server in non-secure mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCS cluster in secure mode</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VCS cluster in non-secure mode</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

For secure communications between the VCS 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 Cluster Server Administrator’s Guide.

Non-SCSI-3 I/O fencing requirements

Supported virtual environment for non-SCSI-3 fencing:
- VMware Server ESX 3.5, 4.0, and 5.0 on AMD Opteron or Intel Xeon EM64T (x86_64)
  Guest operating system: See the Veritas Cluster Server Release Notes for the list of supported Linux operating systems.

Make sure that you also meet the following requirements to configure fencing in the virtual environments that do not support SCSI-3 PR:
- VCS must be configured with Cluster attribute UseFence set to SCSI3
- All coordination points must be CP servers

Number of nodes supported

VCS supports cluster configurations with up to 64 nodes.

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 RPMs 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
Discovering product versions and various requirement information
Planning to install VCS

This chapter includes the following topics:

- VCS installation methods
- Typical VCS cluster setup models

VCS installation methods

Table 3-1 lists the different methods you can choose to install and configure VCS:
### Table 3-1 VCS installation methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Interactive installation using the script-based installer | You can use one of the following script-based installers:  
  - Veritas product installer  
    Use to install and configure multiple Veritas products.  
  - `installvcs` program  
    Use to install and configure just VCS.  
  **Note:** When you use this method, you have two additional options. a) You can simultaneously configure single sign-on with the Symantec High Availability Console. This is required to support vSphere integrated VCS configuration and administration menu. b) You can also simultaneously install application-specific VCS agents.  
    For more information: See “Installing VCS using the installer” on page 79.  
  The script-based installer asks you a series of questions and installs and configures VCS based on the information you provide. |
| Interactive installation using the vCenter menu | In a VMware environment, you can install VCS on multiple systems, using the vCenter menu.  
  For more information, see the *Symantec High Availability Solutions Guide for VMware*. |
| Automated installation using the VCS response files | Use response files to perform unattended installations. You can generate a response file in one of the following ways:  
  - Use the automatically generated response file after a successful installation.  
  - Use the `-makeresponsefile` option to create a response file. |
| Manual installation using the Linux commands and utilities | You can install VCS using the operating system commands like `rpm -i` on Linux systems, and then manually configure VCS as described in the section on Manual installation. |
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 VCS using the installer” on page 79.

- 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.

<table>
<thead>
<tr>
<th>Veritas product name</th>
<th>Product installation script (When running the script from the install media)</th>
<th>Product installation script (When running the script from a system on which the SFHA Solutions product is installed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veritas Cluster Server (VCS)</td>
<td>installvcs</td>
<td>installvcs&lt;version&gt;</td>
</tr>
<tr>
<td>Veritas Storage Foundation and High Availability (SFHA)</td>
<td>installsfha</td>
<td>installsfha&lt;version&gt;</td>
</tr>
</tbody>
</table>

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

For example, for the 6.0.2 version:

# /opt/VRTS/install/installvcs602 -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 345.

About the VCS installation program

You can access the `installvcs` program from the command line or through the Veritas product installer.

The VCS installation program is interactive and manages the following tasks:

■ Licensing VCS

■ Installing VCS RPMs on multiple cluster systems

■ Configuring VCS, by creating several detailed configuration files on each system

■ Starting VCS processes

You can choose to configure different optional features, such as the following:

■ SNMP and SMTP notification

■ VCS configuration in secure mode

■ The wide area Global Cluster feature

■ Cluster Virtual IP address

Review the highlights of the information for which `installvcs` program prompts you as you proceed to configure.

See “About preparing to install VCS” on page 59.
The uninstallvcs program, a companion to installvcs program, uninstalls VCS RPMs. 

See “Preparing to uninstall VCS” on page 319.

**Features of the script-based installer**

The script-based installer supports installing, configuring, upgrading, and uninstalling VCS. In addition, the script-based installer also provides command options to perform the following tasks:

- Check the systems for VCS installation requirements.
  See “Performing automated preinstallation check” on page 69.

- Upgrade VCS if a previous version of VCS currently runs on a cluster.
  See “Upgrading VCS using the script-based installer” on page 246.

- Start or stop VCS processes
  See “Starting and stopping processes for the Veritas products” on page 412.

- Enable or disable a cluster to run in secure mode
  See the *Veritas Cluster Server Administrator’s Guide*.

- Configure I/O fencing for the clusters to prevent data corruption
  See “Setting up disk-based I/O fencing using installvcs program” on page 139.
  See “Setting up server-based I/O fencing using installvcs program” on page 147.
  See “Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installvcs program” on page 156.

- Create a single-node cluster
  See “Creating a single-node cluster using the installer program” on page 390.

- Add a node to an existing cluster
  See “Adding nodes using the VCS installer” on page 291.

- Create a kickstart configuration file to install VCS using the Kickstart utility for RHEL.

- Perform automated installations using the values that are stored in a configuration file.
  See “Installing VCS using response files” on page 163.
  See “Configuring VCS using response files” on page 169.
  See “Upgrading VCS using response files” on page 249.

**Interacting with the installvcs program**

As you run the program, you are prompted to answer yes or no questions. A set of responses that resemble \([y, n, q, ?]\) (y) typically follow these questions. The
response within parentheses is the default, which you can select by pressing the Enter key. Enter the ? character to get help to answer the prompt. Enter q to quit the installation.

Installation of VCS RPMs takes place only after you have confirmed the information. However, you must remove the partially installed VCS files before you run the installvcs program again.

See “Preparing to uninstall VCS” on page 319.

During the installation, the installer prompts you to type information. The installer expects your responses to be within a certain range or in a specific format. The installer provides examples. If you are prompted to enter an item from a list, enter your selection exactly as it is shown in the list.

The installer also prompts you to answer a series of questions that are related to a configuration activity. For such questions, you can enter the b character to return to the first prompt in the series. When the installer displays a set of information items you have entered, you are prompted to confirm it. If you answer n, the program lets you reenter all of the information for the set.

You can install the VCS Java Console on a single system, which is not required to be part of the cluster. Note that the installvcs program does not install the VCS Java Console.

See “Installing the Java Console” on page 263.

About response files

The installer generates a "response file" after performing an installer task such as installation, configuration, uninstallation, or upgrade. These response files contain the details that you provided to the installer questions in the form of values for the response file variables. The response file also contains descriptions and explanations of the variables and their values.

You can also create a response file using the -makeresponsefile option of the installer.

The installer displays the location of the response file at the end of each successful installer task. The installer saves the response file in the default location for the install-related log files: /opt/VRTS/install/logs. If you provided a different log path using the -logpath option, the installer saves the response file in the path that you specified.

The format of the response file name is:

/opt/VRTS/install/logs/installscript-YYYYMMDDHHSSxxx
/installscript-YYYYMMDDHHSSxxx.response, where:
installscript may be, for example: installer, installvcs program, or uninstallvcs program

YYYYMMDDHHSS is the current date when the installscript is run and xxx are three random letters that the script generates for an installation instance

For example:
/opt/VRTS/install/logs/installer-200910101010ldS/installer-200910101010ldS.response

You can customize the response file as required to perform unattended installations using the -responsefile option of the installer. This method of automated installations is useful in the following cases:

- To perform multiple installations to set up a large VCS cluster.
  See “Installing VCS using response files” on page 163.
- To upgrade VCS on multiple systems in a large VCS cluster.
  See “Upgrading VCS using response files” on page 249.
- To uninstall VCS from multiple systems in a large VCS cluster.
  See “Uninstalling VCS using response files” on page 325.

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}=["value1", "value2", "value3"];

Typical VCS cluster setup models

VCS clusters support different failover configurations, storage configurations, and cluster topologies.

See the Veritas Cluster Server Administrator’s Guide for more details.

Some of the typical VCS setup models are as follows:

- Basic VCS cluster with two nodes
  See “Typical configuration of two-node VCS cluster” on page 50.
VCS clusters in secure mode
See “Typical configuration of VCS clusters in secure mode” on page 50.

VCS clusters centrally managed using Veritas Operations Manager (VOM)
See “Typical configuration of VOM-managed VCS clusters” on page 51.

VCS clusters with I/O fencing for data protection
See “Typical VCS cluster configuration with disk-based I/O fencing” on page 91.
See “Typical VCS cluster configuration with server-based I/O fencing” on page 92.

VCS clusters such as global clusters, replicated data clusters, or campus clusters for disaster recovery
See the Veritas Cluster Server Administrator's Guide for disaster recovery cluster configuration models.

Typical configuration of two-node VCS cluster

Figure 3-1 illustrates a simple VCS cluster setup with two nodes.

Typical configuration of VCS clusters in secure mode

Enabling secure mode for VCS guarantees that all inter-system communication is encrypted and that security credentials of users are verified.

Figure 3-2 illustrates typical configuration of VCS clusters in secure mode.
Figure 3-2  Typical configuration of VCS clusters in secure mode

Multiple clusters

Cluster 1

Cluster 2

Each node is a root and authentication broker

Single cluster

node1  node2  node3

Each node is a root and authentication broker

Typical configuration of VOM-managed VCS clusters

Veritas Operations Manager (VOM) provides a centralized management console for Veritas Storage Foundation and High Availability products.

See “About Veritas Operations Manager” on page 27.

Figure 3-3 illustrates a typical setup of VCS clusters that are centrally managed using Veritas Operations Manager.
Figure 3-3  Typical configuration of VOM-managed clusters

VOM Central Server and Symantec Product Authentication Service

Cluster 1  Cluster 2
Licensing VCS

This chapter includes the following topics:

- About Veritas product licensing
- Obtaining VCS license keys
- 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 199.
  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 55.
  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.

---

**Obtaining VCS license keys**

If you decide to not use the keyless licensing, you must obtain and install a license key for VCS.

See “About Veritas product licensing” on page 53.

This product includes a License Key certificate. The certificate specifies the product keys and the number of product licenses purchased. A single key lets you install the product on the number and type of systems for which you purchased the license. A key may enable the operation of more products than are specified on
the certificate. However, you are legally limited to the number of product licenses purchased. The product installation procedure describes how to activate the key. To register and receive a software license key, go to the Symantec Licensing Portal at the following location:

https://licensing.symantec.com

Make sure you have your Software Product License document. You need information in this document to retrieve and manage license keys for your Symantec product. After you receive the license key, you can install the product.

Click the Help link at this site to access the License Portal User Guide and FAQ.

The VRTSvlic RPM enables product licensing. For information about the commands that you can use after the installing VRTSvlic:

See “Installing Veritas product license keys” on page 55.

You can only install the Symantec software products for which you have purchased a license. The enclosed software discs might include other products for which you have not purchased a license.

## Installing Veritas product license keys

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

- Chapter 5. Preparing to install VCS
Preparing to install VCS

This chapter includes the following topics:

- About preparing to install VCS
- Performing preinstallation tasks
- Getting your VCS installation and configuration information ready

About preparing to install VCS

Before you perform the preinstallation tasks, make sure you reviewed the installation requirements, set up the basic hardware, and planned your VCS setup.

See “Important preinstallation information for VCS” on page 33.

Performing preinstallation tasks

Table 5-1 lists the tasks you must perform before proceeding to install VCS.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain license keys if you do not want to use keyless licensing.</td>
<td>See “Obtaining VCS license keys” on page 54.</td>
</tr>
<tr>
<td>Set up the private network.</td>
<td>See “Setting up the private network” on page 60.</td>
</tr>
<tr>
<td>Configure persistent network interfaces</td>
<td>See “Verifying network interfaces for persistent names” on page 62.</td>
</tr>
</tbody>
</table>
Table 5-1  Preinstallation tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable communication between systems.</td>
<td>See “Setting up inter-system communication” on page 407.</td>
</tr>
<tr>
<td>Set up ssh on cluster systems.</td>
<td>See “Setting up ssh on cluster systems” on page 407.</td>
</tr>
<tr>
<td>Set up shared storage for I/O fencing (optional)</td>
<td>See “Setting up shared storage” on page 63.</td>
</tr>
<tr>
<td>Creating root user</td>
<td></td>
</tr>
<tr>
<td>Set the PATH and the MANPATH variables.</td>
<td>See “Setting the PATH variable” on page 66.</td>
</tr>
<tr>
<td></td>
<td>See “Setting the MANPATH variable” on page 66.</td>
</tr>
<tr>
<td>Set the kernel.panic tunable</td>
<td>See “Setting the kernel.panic tunable” on page 67.</td>
</tr>
<tr>
<td>Review basic instructions to optimize LLT media speeds.</td>
<td>See “Optimizing LLT media speed settings on private NICs” on page 67.</td>
</tr>
<tr>
<td>Review guidelines to help you set the LLT interconnects.</td>
<td>See “Guidelines for setting the media speed of the LLT interconnects” on page 68.</td>
</tr>
<tr>
<td>Mount the product disc</td>
<td></td>
</tr>
<tr>
<td>Verify the systems before installation</td>
<td>See “Performing automated preinstallation check” on page 69.</td>
</tr>
</tbody>
</table>

Setting up the private network

VCS requires you to set up a private network between the systems that form a cluster. You can use either NICs or aggregated interfaces to set up private network. You can use network switches instead of hubs. Refer to the Veritas Cluster Server Administrator’s Guide to review VCS performance considerations.

Figure 5-1 shows two private networks for use with VCS.
Symantec recommends configuring two independent networks between the cluster nodes with a network switch for each network. You can also interconnect multiple layer 2 switches for advanced failure protection. Such connections for LLT are called cross-links.

Figure 5-2 shows a private network configuration with crossed links between the network switches.

**To set up the private network**

1. Install the required network interface cards (NICs).
   
   Create aggregated interfaces if you want to use these to set up private network.

2. Connect the VCS private NICs on each system.

3. Use crossover Ethernet cables, switches, or independent hubs for each VCS communication network. Note that the crossover Ethernet cables are supported only on two systems.
   
   Ensure that you meet the following requirements:
The power to the switches or hubs must come from separate sources.

On each system, you must use two independent network cards to provide redundancy.

If a network interface is part of an aggregated interface, you must not configure the network interface under LLT. However, you can configure the aggregated interface under LLT.

When you configure Ethernet switches for LLT private interconnect, disable the spanning tree algorithm on the ports used for the interconnect.

During the process of setting up heartbeat connections, consider a case where a failure removes all communications between the systems.

Note that a chance for data corruption exists under the following conditions:

- The systems still run, and
- The systems can access the shared storage.

Test the network connections. Temporarily assign network addresses and use `telnet` or `ping` to verify communications.

LLT uses its own protocol, and does not use TCP/IP. So, you must ensure that the private network connections are used only for LLT communication and not for TCP/IP traffic. To verify this requirement, unplug and unconfigure any temporary IP addresses that are configured on the network interfaces.

The installer configures the private network in the cluster during configuration.

You can also manually configure LLT.

See “Configuring LLT manually” on page 203.

Verifying network interfaces for persistent names

VCS requires that the network interface cards use persistent interface names. By default, SLES 10, RHEL5 and later Linux flavors use udev to achieve persistent interface names.

**To verify and configure persistent network interfaces**

- Make sure that the network interface names are persistent.

  If the network interface names are not persistent, then manually configure persistent interfaces.

  For RHEL, SLES, and OEL, refer to the OS documentation for information on configuring persistent interfaces.
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 \texttt{-comcleanup} option to remove the ssh or rsh configuration from the systems.

See “Installation script options” on page 345.

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 “Setting up inter-system communication” on page 407.

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.

\textbf{Note}: VCS also supports non-SCSI3 server-based fencing configuration in virtual environments that do not support SCSI-3 PR-compliant storage.

See also the \textit{Veritas Cluster Server Administrator's Guide} for a description of I/O fencing.

\textbf{Setting up shared storage: SCSI}

Perform the following steps to set up shared storage.

\textbf{To set up shared storage}

1. Connect the disk to the first cluster system.
2. Power on the disk.
3. Connect a terminator to the other port of the disk.
4 Boot the system. The disk is detected while the system boots.
5 Press CTRL+A to bring up the SCSI BIOS settings for that disk.
   Set the following:
   - Set Host adapter SCSI ID = 7, or to an appropriate value for your configuration.
   - Set Host Adapter BIOS in Advanced Configuration Options to Disabled.
6 Format the shared disk and create required partitions on it.
   Perform the following:
   - Identify your shared disk name. If you have two internal SCSI hard disks, your shared disk is /dev/sdc.
     Identify whether the shared disk is sdc, sdb, and so on.
   - Type the following command:
     
```sh
     # fdisk /dev/sharediskname
     
     For example, if your shared disk is sdc, type:
     
     # fdisk /dev/sdc
     
     - Create disk groups and volumes using Volume Manager utilities.
     - To apply a file system on the volumes, type:
     
     # mkfs -t fs-type /dev/vx/dsk/disk-group/volume
     
     For example, enter the following command:
     
     # mkfs -t vxfs /dev/vx/dsk/dg/vol01
     
     Where the name of the disk group is dg, the name of the volume is vol01, and the file system type is vxfs.
7 Power off the disk.
8 Remove the terminator from the disk and connect the disk to the other cluster system.
9 Power on the disk.
10 Boot the second system. The system can now detect the disk.
11 Press Ctrl+A to bring up the SCSI BIOS settings for the disk.
   Set the following:
Set Host adapter SCSI ID = 6, or to an appropriate value for your configuration. Note that the SCSI ID should be different from the one configured on the first cluster system.

Set Host Adapter BIOS in Advanced Configuration Options to Disabled.

Verify that you can view the shared disk using the `fdisk` command.

**Setting up shared storage: Fibre Channel**

Perform the following steps to set up Fibre Channel.

**To set up shared storage for Fibre Channel**

1. Connect the Fibre Channel disk to a cluster system.
2. Boot the system and change the settings of the Fibre Channel. Perform the following tasks for all QLogic adapters in the system:
   - Press Alt+Q to bring up the QLogic adapter settings menu.
   - Choose **Configuration Settings**.
   - Click Enter.
   - Choose **Advanced Adapter Settings**.
   - Click Enter.
   - Set the Enable Target Reset option to **Yes** (the default value).
   - Save the configuration.
   - Reboot the system.
3. Verify that the system detects the Fibre Channel disks properly.
4. Create volumes. Format the shared disk and create required partitions on it and perform the following:
   - Identify your shared disk name. If you have two internal SCSI hard disks, your shared disk is `/dev/sdc`. Identify whether the shared disk is sdc, sdb, and so on.
   - Type the following command:
     ```
     # fdisk /dev/shreddiskname
     ```
     For example, if your shared disk is sdc, type:
     ```
     # fdisk /dev/sdc
     ```
   - Create disk groups and volumes using Volume Manager utilities.
To apply a file system on the volumes, type:

```
# mkfs -t fs-type /dev/vx/dsk/disk-group/volume
```

For example, enter the following command:

```
# mkfs -t vxfs /dev/vx/dsk/dg/vol01
```

Where the name of the disk group is dg, the name of the volume is vol01, and the file system type is vxfs.

5. Repeat step 2 and step 3 for all nodes in the clusters that require connections with Fibre Channel.

6. Power off this cluster system.

7. Connect the same disks to the next cluster system.

8. Turn on the power for the second system.

9. Verify that the second system can see the disk names correctly—the disk names should be the same.

See “Verifying that the nodes have access to the same disk” on page 144.

### Setting the PATH variable

Installation commands as well as other commands reside in the /opt/VRTS/bin directory. Add this directory to your PATH environment variable.

If you have any custom scripts located in /opt/VRTSvcs/bin directory, make sure to add the /opt/VRTSvcs/bin directory to your PATH environment variable.

**To set the PATH variable**

- Do one of the following:
  - For the Bourne Shell (sh), Bourne-again Shell (bash), or Korn shell (ksh), type:

    ```
    # PATH=/opt/VRTS/bin:$PATH; export PATH
    ```

  - For the C Shell (csh) or enhanced C Shell (tcsh), type:

    ```
    $ setenv PATH :/opt/VRTS/bin:$PATH
    ```

### Setting the MANPATH variable

Set the MANPATH variable to view the manual pages.
To set the MANPATH variable

◆ Do one of the following:
  ■ For the Bourne Shell (sh), Bourne-again Shell (bash), or Korn shell (ksh), type:
    
    # MANPATH=/opt/VRTS/man:$MANPATH; export MANPATH
  ■ For the C Shell (csh) or enhanced C Shell (tcsh), type:
    % setenv MANPATH /usr/share/man:/opt/VRTS/man

If you use the `man` command to access manual pages, set LC_ALL to "C" in your shell for correct page display.

# export LC_ALL=C

See incident 82099 on the Red Hat support web site for more information.

Setting the kernel.panic tunable

By default, the kernel.panic tunable is set to zero. Therefore the kernel does not reboot automatically if a node panics. To ensure that the node reboots automatically after it panics, this tunable must be set to a non zero value.

To set the kernel.panic tunable

1 Set the kernel.panic tunable to a desired value in the /etc/sysctl.conf file.
   For example, kernel.panic = 10, will assign a value 10 seconds to the kernel.panic tunable. This step makes the change persistent across reboots.

2 Run the command:
   
   sysctl -w kernel.panic=10

   In case of a panic, the node will reboot after 10 seconds.

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.

Mounting the product disc

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

To mount the product disc

1. Log in as superuser on a system where you want to install VCS.
   The system from which you install VCS need not be part of the cluster. The systems must be in the same subnet.

2. Insert the product disc with the VCS software into a drive that is connected to the system.
   The disc is automatically mounted.

3. If the disc does not automatically mount, then enter:
   ```
   # mkdir /mnt/cdrom
   # mount -o ro /dev/cdrom /mnt/cdrom
   ```
4 Navigate to the location of the RPMs.

```bash
# cd /mnt/cdrom/dist_arch/rpms
```

Where `dist` is `rhel5`, `rhel6`, `sles10`, or `sles11`, and `arch` is `x86_64` for RHEL and SLES.

Performing automated preinstallation check

Before you begin the installation of VCS software, you can check the readiness of the systems where you plan to install VCS. The command to start the preinstallation check is:

```bash
installvcs -precheck system1 system2 ...
```

You can also run the `installer -precheck` command.


You can use the Veritas Operation Services to assess your setup for VCS installation.

To check the systems

1 Navigate to the folder that contains the installvcs program.

2 Start the preinstallation check:

```bash
# ./installvcs -precheck sys1 sys2 ...
```

The program proceeds in a noninteractive mode to examine the systems for licenses, RPMs, disk space, and system-to-system communications.

3 Review the output as the program displays the results of the check and saves the results of the check in a log file.

Reformatting VCS configuration files on a stopped cluster

When you manually edit VCS configuration files (for example, the main.cf or types.cf file) you can potentially create formatting issues that may cause the installer to interpret the cluster configuration information incorrectly.

If you have manually edited any of the configuration files, you need to perform one of the following before you run the installation program:

- On a running cluster, perform an `haconf -dump` command. This command saves the configuration files and ensures that they do not have formatting errors before you run the installer.
On cluster that is not running, perform the `hacf -cftocmd` and then the `hacf -cmdtocf` commands to format the configuration files.

**Note:** Remember to make back up copies of the configuration files before you edit them.

You also need to use this procedure if you have manually changed the configuration files before you perform the following actions using the installer:
- Upgrade VCS
- Uninstall VCS

For more information about the main.cf and types.cf files, refer to the *Veritas Cluster Server Administrator's Guide*.

**To display the configuration files in the correct format on a running cluster**
- Run the following commands to display the configuration files in the correct format:

  ```
  # haconf -dump
  ```

**To display the configuration files in the correct format on a stopped cluster**
- Run the following commands to display the configuration files in the correct format:

  ```
  # hacf -cftocmd config
  # hacf -cmdtocf config
  ```

---

### Getting your VCS installation and configuration information ready

The VCS installer prompts you for some information during the installation and configuration process. Review the following information and make sure you have made the necessary decisions and you have the required information ready before you perform the installation and configuration.

*Table 5-2* lists the information you need to install the VCS RPMs.
Table 5-2 Information to install the VCS RPMs

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System names</td>
<td>The system names where you plan to install VCS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: sys1, sys2</td>
<td></td>
</tr>
<tr>
<td>The required license keys</td>
<td>If you decide to use keyless licensing, you do not need to obtain license keys. However, you require to set up management server within 60 days to manage the cluster.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See “About Veritas product licensing” on page 53.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Depending on the type of installation, keys can include:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ A valid site license key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ A valid demo license key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ A valid license key for VCS global clusters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See “Obtaining VCS license keys” on page 54.</td>
<td></td>
</tr>
</tbody>
</table>

Decide which RPMs to install

<table>
<thead>
<tr>
<th>Information</th>
<th>Minimum RPMs—provides basic VCS functionality.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Recommended RPMs—provides full functionality of VCS without advanced features.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All RPMs—provides advanced feature functionality of VCS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default option is to install the recommended RPMs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See “Viewing the list of VCS RPMs” on page 196.</td>
<td></td>
</tr>
</tbody>
</table>

Table 5-3 lists the information you need to configure VCS cluster name and ID.

Table 5-3 Information you need to configure VCS cluster name and ID

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A name for the cluster</td>
<td>The cluster name must begin with a letter of the alphabet. The cluster name can contain only the characters &quot;a&quot; through &quot;z&quot;, &quot;A&quot; through &quot;Z&quot;, the numbers &quot;0&quot; through &quot;9&quot;, the hyphen &quot;-&quot;, and the underscore &quot;_&quot;.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: my_cluster</td>
<td></td>
</tr>
<tr>
<td>A unique ID number for the cluster</td>
<td>A number in the range of 0-65535. If multiple distinct and separate clusters share the same network, then each cluster must have a unique cluster ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: 12133</td>
<td></td>
</tr>
</tbody>
</table>

Table 5-4 lists the information you need to configure VCS private heartbeat links.
**Table 5-4** Information you need to configure VCS private heartbeat links

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decide how you want to configure LLT</td>
<td>You can configure LLT over Ethernet or LLT over UDP. Symantec recommends that you configure heartbeat links that use LLT over Ethernet, unless hardware requirements force you to use LLT over UDP. If you want to configure LLT over UDP, make sure you meet the prerequisites. See “Using the UDP layer for LLT” on page 393.</td>
</tr>
</tbody>
</table>

**Decide which configuration mode you want to choose**

Installer provides you with three options:

- Configure heartbeat links using LLT over Ethernet
- Configure heartbeat links using LLT over UDP
- Automatically detect configuration for LLT over Ethernet

You must manually enter details for options 1 and 2, whereas the installer detects the details for option 3.

**For option 1: LLT over Ethernet**

- The device names of the NICs that the private networks use among systems
  - A network interface card or an aggregated interface. Do not use the network interface card that is used for the public network, which is typically eth0.
  - Example: eth1, eth2
- Choose whether to use the same NICs on all systems. If you want to use different NICs, enter the details for each system.

**For option 2: LLT over UDP**

For each system, you must have the following details:

- The device names of the NICs that the private networks use among systems
- IP address for each NIC
- UDP port details for each NIC

**Table 5-5** lists the information you need to configure virtual IP address of the cluster (optional).

**Table 5-5** Information you need to configure virtual IP address

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the public NIC for each node in the cluster</td>
<td>The device name for the NIC that provides public network access. A network interface card or an aggregated interface. Example: eth0</td>
</tr>
</tbody>
</table>
### Table 5-5

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
</table>
| A virtual IP address of the NIC                  | You can enter either an IPv4 or an IPv6 address. This virtual IP address becomes a resource for use by the ClusterService group. The "Cluster Virtual IP address" can fail over to another cluster system.  
Example IPv4 address: 192.168.1.16  
| The netmask for the virtual IPv4 address         | The subnet that you use with the virtual IPv4 address.  
Example: 255.255.240.0                                                                                                                                         |            |
| The prefix for the virtual IPv6 address          | The prefix length for the virtual IPv6 address.  
Example: 64                                                                                                                                                    |            |

**Table 5-6** lists the information you need to add VCS users.

### Table 5-6

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
</table>
| User names          | VCS usernames are restricted to 1024 characters.  
Example: smith                                                                                       |            |
| User passwords      | VCS passwords are restricted to 255 characters.  
Enter the password at the prompt.  
**Note**: VCS leverages native authentication in secure mode. Therefore, user passwords are not needed in secure mode. |            |
| To decide user privileges | Users have three levels of privileges: Administrator, Operator, or Guest.  
Example: Administrator                                                                                 |            |

**Table 5-7** lists the information you need to configure SMTP email notification (optional).
### Table 5-7  Information you need to configure SMTP email notification (optional)

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the public NIC for each node in the cluster</td>
<td>The device name for the NIC that provides public network access. A network interface card or an aggregated interface. Examples: \texttt{eth0}</td>
<td></td>
</tr>
<tr>
<td>The domain-based address of the SMTP server</td>
<td>The SMTP server sends notification emails about the events within the cluster. Example: \texttt{smtp.symantecexample.com}</td>
<td></td>
</tr>
<tr>
<td>The email address of each SMTP recipient to be notified</td>
<td>Example: \texttt{<a href="mailto:john@symantecexample.com">john@symantecexample.com</a>}</td>
<td></td>
</tr>
</tbody>
</table>
| To decide the minimum severity of events for SMTP email notification | Events have four levels of severity, and the severity levels are cumulative:  
- Information  
  VCS sends notifications for important events that exhibit normal behavior.  
- Warning  
  VCS sends notifications for events that exhibit any deviation from normal behavior. Notifications include both Warning and Information type of events.  
- Error  
  VCS sends notifications for faulty behavior. Notifications include both Error, Warning, and Information type of events.  
- SevereError  
  VCS sends notifications for a critical error that can lead to data loss or corruption. Notifications include both Severe Error, Error, Warning, and Information type of events. Example: \texttt{Error} |  |

### Table 5-8  Information you need to configure SNMP trap notification (optional)

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the public NIC for each node in the cluster</td>
<td>The device name for the NIC that provides public network access. A network interface card or an aggregated interface. Examples: \texttt{eth0}</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-8  Information you need to configure SNMP trap notification (optional) (continued)

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The port number for the SNMP trap daemon</td>
<td>The default port number is 162.</td>
<td></td>
</tr>
<tr>
<td>The system name for each SNMP console</td>
<td>Example: sys5</td>
<td></td>
</tr>
</tbody>
</table>
| To decide the minimum severity of events for SNMP trap notification | Events have four levels of severity, and the severity levels are cumulative:  
  ■ Information  
  VCS sends notifications for important events that exhibit normal behavior.  
  ■ Warning  
  VCS sends notifications for events that exhibit any deviation from normal behavior. Notifications include both Warning and Information type of events.  
  ■ Error  
  VCS sends notifications for faulty behavior. Notifications include both Error, Warning, and Information type of events.  
  ■ SevereError  
  VCS sends notifications for a critical error that can lead to data loss or corruption. Notifications include both Severe Error, Error, Warning, and Information type of events.  
Example: Error                                           |            |

Table 5-9 lists the information you need to configure global clusters (optional).

Table 5-9  Information you need to configure global clusters (optional)

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
</table>
| The name of the public NIC   | You can use the same NIC that you used to configure the virtual IP of the cluster. Otherwise, specify appropriate values for the NIC.  
A network interface card or an aggregated interface.  
Examples: eth0                |            |
### Table 5-9  Information you need to configure global clusters (optional) (continued)

<table>
<thead>
<tr>
<th>Information</th>
<th>Description and sample value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The virtual IP address of the NIC</td>
<td>You can enter either an IPv4 or an IPv6 address. You can use the same virtual IP address that you configured earlier for the cluster. Otherwise, specify appropriate values for the virtual IP address. Example IPv4 address: <strong>192.168.1.16</strong> Example IPv6 address: <strong>2001:454e:205a:110:203:baff:feee:10</strong></td>
<td></td>
</tr>
<tr>
<td>The netmask for the virtual IPv4 address</td>
<td>You can use the same netmask that you used to configure the virtual IP of the cluster. Otherwise, specify appropriate values for the netmask. Example: <strong>255.255.240.0</strong></td>
<td></td>
</tr>
<tr>
<td>The prefix for the virtual IPv6 address</td>
<td>The prefix length for the virtual IPv6 address. Example: <strong>64</strong></td>
<td></td>
</tr>
</tbody>
</table>

Review the information you need to configure I/O fencing.
Installation using the script-based installer

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

This chapter includes the following topics:

- Installing VCS using the installer

Installing VCS using the installer

Perform the following steps to install VCS.

**Note:** The system from where you install VCS must run the same Linux distribution as the target systems.

To install VCS

1. Confirm that you are logged in as the superuser and you mounted the product disc.

2. If you want to install VCS using the Veritas product installer, perform the following steps:
   - Start the installer.
     
     ```
     # ./installer
     ```
   The installer starts with a copyright message and specifies the directory where the logs are created.
   - From the opening Selection Menu, choose 1 for "Install a Product."
   - From the displayed list of products to install, choose: Veritas Cluster Server.

If you want to install VCS using installvcs program, perform the following steps:
Navigate to the folder that contains the installvcs program.

```
# cd installation_media/dist_arch/cluster_server
```

where `dist` is `rhel5`, `rhel6`, `sles10`, or `sles11` and `arch` is `x86_64`.

Start the Install VCS program

```
# ./installvcs
```

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

If you want to install VCS in a VMware environment, with single sign-on between the system and the Symantec High Availability Console enabled, perform the following steps:

- Create a file, say `SSO_inputs_file`, in the `tmp` directory with the following contents:

  ```
  $Obj::pool{Cfg}{sso_console_ip} = '1.2.3.4';
  $Obj::pool{Cfg}{sso_local_username} = 'root';
  $Obj::pool{Cfg}{sso_local_password} = 'encryptedpassword';
  ```

  **Note:** You must enter only encrypted passwords in the SSO input files. For more information: See “Encrypting a password” on page 84.

- Navigate to the directory that contains the installvcs program.

  ```
  # cd install_media/dist_arch/cluster_server
  ```

  where `dist` is `rhel5`, `rhel6`, `sles10`, or `sles11` and `arch` is `x86_64`.

- Start the installvcs program:

  ```
  # ./installvcs -require /tmp/SSO_inputs_file
  ```

If you want to simultaneously install VCS and application-specific VCS agents on a system in a VMware environment, execute the following steps:

- Create a temporary directory, say `temp_install`:

  ```
  # mkdir /temp_install
  ```

- From the `rpms` directory of the installation media, copy the product binaries to the temporary directory:
# cp -rp rpms/* /temp_install

- From the addons directory of the installation media, copy the agent binaries to the temporary directory:
  
  # cp -rp addons/agents/* /temp_install

- Navigate to the folder that contains the installvcs program:
  
  # cd install_media/dist_arch/cluster_server

  where dist is rhel5, rhel6, sles10, or sles11 and arch is x86_64.

- Start the installvcs program with the pkgpath option:
  
  # ./installvcs -pkgpath /temp_install/

3 Enter y to agree to the End User License Agreement (EULA).

Do you agree with the terms of the End User License Agreement as specified in the cluster_server/EULA/<lang>/EULA_VCS_Lx_6.0.2.pdf file present on media? [y,n,q,?] y

4 Choose the VCS RPMs that you want to install.

    **Note:** In a VMware virtual environment, you must specify either option 2 or 3.

Based on what RPMs you want to install, enter one of the following:

1 Installs only the minimal required VCS RPMs that provides basic functionality of the product.

2 Installs the recommended VCS RPMs that provides complete functionality of the product. This option does not install the optional VCS RPMs.
   
   Note that this option is the default.

3 Installs all the VCS RPMs.
   
   You must choose this option to configure any optional VCS feature.

4 Displays the VCS RPMs for each option.
Select the RPMs to be installed on all systems? [1-4,q,?]
(2) 3

5 Enter the names of the systems where you want to install VCS.

Enter the 64 bit operating system system names separated by spaces: [q,?] sys1 sys2

For a single-node VCS installation, enter one name for the system.
See “Creating a single-node cluster using the installer program” on page 390.

The installer does the following for the systems:

- Checks that the local system that runs the installer can communicate with remote systems.
  - If the installer finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases.
  - If the default communication method ssh fails, the installer attempts to use rsh.

- Makes sure the systems use one of the supported operating systems.

- Makes sure that the systems have the required operating system patches.
  - If the installer reports that any of the patches are not available, install the patches on the system before proceeding with the VCS installation.

- Checks for product licenses.

- Checks whether a previous version of VCS is installed.
  - If a previous version of VCS is installed, the installer provides an option to upgrade to VCS 6.0.2.

- Checks for the required file system space and makes sure that any processes that are running do not conflict with the installation.
  - If requirements for installation are not met, the installer stops and indicates the actions that you must perform to proceed with the process.

- Checks whether any of the RPMs already exists on a system.
  - If the current version of any RPM exists, the installer removes the RPM from the installation list for the system. If a previous version of any RPM exists, the installer replaces the RPM with the current version.

6 Review the list of RPMs that the installer would install on each node.

The installer installs the VCS RPMs on the systems sys1 and sys2.

7 Select the license type.
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)

Based on what license type you want to use, enter one of the following:

1  You must have a valid license key. Enter the license key at the prompt:

Enter a VCS license key: [b,q,?]

If you plan to configure global clusters, enter the corresponding license keys when the installer prompts for additional licenses.

Do you wish to enter additional licenses? [y,n,q,b] (n) y

2  The keyless license option enables you to install VCS without entering a key. However, to ensure compliance, keyless licensing requires that you manage the systems with a management server.

For more information, go to the following website:

http://go.symantec.com/sfhakeyless

Note that this option is the default.

The installer registers the license and completes the installation process.

8  To install the Global Cluster Option, enter y at the prompt.

9  To configure VCS, enter y at the prompt. You can also configure VCS later.

Would you like to configure VCS on sys1 sys2 [y,n,q] (n) n

See “Overview of tasks to configure VCS using the script-based installer” on page 116.

10 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

The installer provides an option to collect data about the installation process each time you complete an installation, upgrade, configuration, or uninstall of the product. The installer transfers the contents of the install log files to an internal Symantec site. The information is used only to gather metrics about how you use the installer. No personal customer data is collected, and no information will be shared by any other parties. Information gathered
may include the product and the version installed or upgraded, how many systems were installed, and the time spent in any section of the install process.

11 The installer checks for online updates and provides an installation summary.

12 After the installation, note the location of the installation log files, the summary file, and the response file for future reference.

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

- **summary file**: Lists the RPMs that are installed on each system.
- **log file**: Details the entire installation.
- **response file**: Contains the installation information that can be used to perform unattended or automated installations on other systems.
  
  See “Installing VCS using response files” on page 163.

### Encrypting a password

You must encrypt passwords before adding them to the SSO input files or the response files. Veritas Cluster Server (VCS) provides the `vcsencrypt` utility to encrypt passwords. You can find this utility in the product disc.

For example, to install VCS on a machine running the RHEL 5 operating system, you can find the utility in the following location:

`redhat_media/rhel5_x86_64/scripts/vcsencrypt`
To encrypt a password:

1. Navigate to the directory that contains the encryption utility for the required operating system:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Enterprise Linux 5</td>
<td>redhat_media/rhel5_x86_64</td>
</tr>
<tr>
<td>Oracle Enterprise Linux 6</td>
<td>redhat_media/rhel6_x86_64</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5</td>
<td>redhat_media/rhel5_x86_64</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6</td>
<td>redhat_media/rhel6_x86_64</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 10</td>
<td>suse_media/sles10_x86_64</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 11</td>
<td>suse_media/sles11_x86_64</td>
</tr>
</tbody>
</table>

For example, to encrypt a password when installing VCS on a machine running the RHEL 5 operating system:

```
# cd redhat_media/rhel5_x86_64/scripts/
```

2. Run the encrypt utility by using the following command:

```
# ./vcsencrypt -agent
```

3. Enter the password.

The encrypt program displays the encrypted password. Copy the encrypted password to the SSO input files or the response files.
Installing VCS

Installing VCS using the installer
Preparing to configure VCS 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 VCS 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 VCS 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 90.

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

**Preparatory tasks**
- Use the following utilities:
  - `vxdiskadm` or `vxdisksetup` utilities
  - `vxenadm` and `vxentshtdw` utilities

**Configuration tasks**
- Use one of the following methods:
  - Run the `installvcs` command, choose option 2, and follow the prompts
  - Edit the values in the response file you created and use them with `installvcs` command
  - Manually configure disk-based I/O fencing

**Figure 7-2** illustrates a high-level flowchart to configure non-SCSI-3 server-based I/O fencing for the VCS cluster in virtual environments that do not support SCSI-3 PR.
After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:
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 VCS cluster configuration with disk-based I/O fencing**

*Figure 7-3* displays a typical VCS configuration with two nodes and shared storage. The configuration uses three coordinator disks for I/O fencing.
Typical VCS cluster configuration with server-based I/O fencing

Figure 7-4 displays a configuration using a VCS cluster (with two nodes), a single CP server, and two coordinator disks. The nodes within the VCS cluster are connected to and communicate with each other using LLT links.

Recommended CP server configurations

Following are the recommended CP server configurations:

- Multiple application clusters use three CP servers as their coordination points
  See Figure 7-5 on page 93.

- Multiple application clusters use a single CP server and single or multiple pairs of coordinator disks (two) as their coordination points
  See Figure 7-6 on page 94.

- 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 7-7 on page 94.
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 7-5 displays a configuration using three CP servers that are connected to multiple application clusters.

Figure 7-5 Three CP servers connecting to multiple application clusters

Figure 7-6 displays a configuration using a single CP server that is connected to multiple application clusters with each application cluster also using two coordinator disks.
Figure 7-6  Single CP server with two coordinator disks for each application cluster

CP server hosted on a single-node VCS cluster
(can also be hosted on an SFHA cluster)

TCP/IP
Public network

TCP/IP

Fibre channel
coordinator disks

TCP/IP
Public network

application clusters
(clusters which run VCS, SFHA, SFCFS, SVS, or SF Oracle RAC to provide high availability for applications)

---

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

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

CP server hosted on an SFHA cluster

TCP/IP
Public network

TCP/IP

TCP/IP

application clusters
(clusters which run VCS, SFHA, SFCFS, SVS, or SF Oracle RAC to provide high availability for applications)

See “Configuration diagrams for setting up server-based I/O fencing” on page 417.
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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan your CP server setup</td>
<td>See “Planning your CP server setup” on page 95.</td>
</tr>
<tr>
<td>Install the CP server</td>
<td>See “Installing the CP server using the installer” on page 96.</td>
</tr>
<tr>
<td>Configure the CP server cluster in secure mode</td>
<td>See “Configuring the CP server cluster in secure mode” on page 97.</td>
</tr>
<tr>
<td>Set up shared storage for the CP server database</td>
<td>See “Setting up shared storage for the CP server database” on page 97.</td>
</tr>
<tr>
<td>Configure the CP server</td>
<td>See “Configuring the CP server using the installer program” on page 98.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the CP server manually” on page 108.</td>
</tr>
<tr>
<td>Verify the CP server configuration</td>
<td>See “Verifying the CP server configuration” on page 113.</td>
</tr>
</tbody>
</table>

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 VCS 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 (VCS clusters). It also secures the HAD communication on the CP server cluster.

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

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.

During installation, make sure to select all RPMs for installation. The VRTScps RPM is installed only if you select to install all RPMs.

Proceed to configure the CP server.

See “Configuring the CP server using the installer program” on page 98.

See “Configuring the CP server manually” on page 108.
<table>
<thead>
<tr>
<th>CP server setup uses multiple systems</th>
<th>Install and configure SFHA to create an SFHA cluster. This makes the CP server highly available.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meet the following requirements for CP server:</td>
<td></td>
</tr>
<tr>
<td>■ During installation, make sure to select all RPMs for installation. The VRTScps RPM is installed only if you select to install all RPMs.</td>
<td></td>
</tr>
<tr>
<td>■ During configuration, configure disk-based fencing (scsi3 mode).</td>
<td></td>
</tr>
<tr>
<td>See the Veritas Storage Foundation and High Availability Installation Guide for instructions on installing and configuring SFHA.</td>
<td></td>
</tr>
<tr>
<td>Proceed to set up shared storage for the CP server database.</td>
<td></td>
</tr>
</tbody>
</table>

### 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 VCS 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.

  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.

### 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 99.

For CP servers on an SFHA cluster: See “To configure the CP server on an SFHA cluster” on page 103.
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.

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 linux92216 for NIC resource - 1: eth0
Enter a valid network interface on linux92216 for NIC resource - 2: eth1

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 eth0 on system linux92216? [y,n,q] y
Enter a valid IP address to configure NetworkHosts for NIC eth0 on system linux92216: 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.

   ```bash
   # ./installsfha<version> -configcps
   
   Where <version> is the specific release version.
   ```

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 linux92216 for NIC resource - 1: eth0
   Enter a valid network interface on linux92216 for NIC resource - 2: eth1

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 eth0 on system linux92216? [y,n,q] y
Enter a valid IP address to configure NetworkHosts for NIC eth0 on system linux92216: 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 existing credentials.

Do you want to reuse these credentials? [y,n,q] (y)
26 After the configuration process has completed, a success message appears.

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

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

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

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

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

### Configuring the CP server 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 381.
   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:

<table>
<thead>
<tr>
<th>Group</th>
<th>Attribute</th>
<th>System</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPSSG</td>
<td>State</td>
<td>cpsl.symantecexample.com</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>

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.
On a SFHA cluster:

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

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

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

Response file variables to configure CP server

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[opt]{configcps}</td>
<td>Scalar</td>
<td>This variable performs CP server configuration task</td>
</tr>
<tr>
<td>CFG{cps_singlenode_config}</td>
<td>Scalar</td>
<td>This variable describes if the CP server will be configured on a singlenode VCS cluster</td>
</tr>
<tr>
<td>CFG{cps_sfha_config}</td>
<td>Scalar</td>
<td>This variable describes if the CP server will be configured on a SFHA cluster</td>
</tr>
<tr>
<td>CFG{cps_unconfig}</td>
<td>Scalar</td>
<td>This variable describes if the CP server will be unconfigured</td>
</tr>
<tr>
<td>CFG{cpsname}</td>
<td>Scalar</td>
<td>This variable describes the name of the CP server</td>
</tr>
<tr>
<td>CFG{cps_db_dir}</td>
<td>Scalar</td>
<td>This variable describes the absolute path of CP server database</td>
</tr>
<tr>
<td>CFG{cps_security}</td>
<td>Scalar</td>
<td>This variable describes if security is configured for the CP server</td>
</tr>
<tr>
<td>CFG{cps_reuse_cred}</td>
<td>Scalar</td>
<td>This variable describes if reusing the existing credentials for the CP server</td>
</tr>
<tr>
<td>CFG{cps_vips}</td>
<td>List</td>
<td>This variable describes the virtual IP addresses for the CP server</td>
</tr>
</tbody>
</table>
Table 7-2 describes response file variables to configure CP server (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{cps_ports}</td>
<td>List</td>
<td>This variable describes the port number for the virtual IP addresses for the CP server</td>
</tr>
<tr>
<td>CFG{cps_nic_list}{cpsvip&lt;n&gt;}</td>
<td>List</td>
<td>This variable describes the NICs of the systems for the virtual IP address</td>
</tr>
<tr>
<td>CFG{cps_netmasks}</td>
<td>List</td>
<td>This variable describes the netmasks for the virtual IP addresses</td>
</tr>
<tr>
<td>CFG{cps_prefix_length}</td>
<td>List</td>
<td>This variable describes the prefix length for the virtual IP addresses</td>
</tr>
<tr>
<td>CFG{cps_network_hosts}{cpsnic&lt;n&gt;}</td>
<td>List</td>
<td>This variable describes the network hosts for the NIC resource</td>
</tr>
<tr>
<td>CFG{cps_vip2nicres_map}{&lt;vip&gt;}</td>
<td>Scalar</td>
<td>This variable describes the NIC resource to associate with the virtual IP address</td>
</tr>
<tr>
<td>CFG{cps_diskgroup}</td>
<td>Scalar</td>
<td>This variable describes the disk group for the CP server database</td>
</tr>
<tr>
<td>CFG{cps_volume}</td>
<td>Scalar</td>
<td>This variable describes the volume for the CP server database</td>
</tr>
<tr>
<td>CFG{cps_newdg_disks}</td>
<td>List</td>
<td>This variable describes the disks to be used to create a new disk group for the CP server database</td>
</tr>
<tr>
<td>CFG{cps_newvol_volsize}</td>
<td>Scalar</td>
<td>This variable describes the volume size to create a new volume for the CP server database</td>
</tr>
<tr>
<td>CFG{cps_delete_database}</td>
<td>Scalar</td>
<td>This variable describes if deleting the database of the CP server during the unconfiguration</td>
</tr>
<tr>
<td>CFG{cps_delete_config_log}</td>
<td>Scalar</td>
<td>This variable describes if deleting the config files and log files of the CP server during the unconfiguration</td>
</tr>
</tbody>
</table>

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

Review the response file variables and their definitions.
See Table 7-2 on page 110.

# # 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(en0) ];
$CFG{cps_ports}=[ qw(14250) ];
$CFG{cps_security}=0;
$CFG{cps_single_node_config}=1;
$CFG{cps_vip2nicres_map}{"10.200.58.233"}=1;
$CFG{cps_vips}=[ qw(10.200.58.233) ];
$CFG{cpsname}="cps1";
$CFG{opt}{configcps}=1;
$CFG{opt}{configure}=1;
$CFG{prod}="VCS601";
$CFG{systems}=[ qw(cps1) ];
$CFG{vcs_clusterid}=18523;
$CFG{vcs_clustername}="vcs92216";

1;

Sample response file for configuring the CP server on SFHA cluster

Review the response file variables and their definitions.

See Table 7-2 on page 110.

# # 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) ];
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.
Preparing to configure VCS clusters for data integrity

Setting up the CP server
This chapter includes the following topics:

- Overview of tasks to configure VCS 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 Cluster Server in secure mode
- Setting up trust relationships for your VCS cluster
- Configuring a secure cluster node by node
- Adding VCS users
- Configuring SMTP email notification
- Configuring SNMP trap notification
- Configuring global clusters
- Completing the VCS configuration
- Verifying and updating licenses on the system
Overview of tasks to configure VCS using the script-based installer

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

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start the software configuration</td>
<td>See “Starting the software configuration” on page 117.</td>
</tr>
<tr>
<td>Specify the systems where you want to configure VCS</td>
<td>See “Specifying systems for configuration” on page 117.</td>
</tr>
<tr>
<td>Configure the basic cluster</td>
<td>See “Configuring the cluster name” on page 118.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring private heartbeat links” on page 118.</td>
</tr>
<tr>
<td>Configure virtual IP address of the cluster (optional)</td>
<td>See “Configuring the virtual IP of the cluster” on page 122.</td>
</tr>
<tr>
<td>Configure the cluster in secure mode (optional)</td>
<td></td>
</tr>
<tr>
<td>Add VCS users (required if you did not configure the cluster in secure mode)</td>
<td>See “Adding VCS users” on page 130.</td>
</tr>
<tr>
<td>Configure SMTP email notification (optional)</td>
<td>See “Configuring SMTP email notification” on page 131.</td>
</tr>
<tr>
<td>Configure SNMP email notification (optional)</td>
<td>See “Configuring SNMP trap notification” on page 132.</td>
</tr>
<tr>
<td>Configure global clusters (optional)</td>
<td>See “Configuring global clusters” on page 134.</td>
</tr>
<tr>
<td><strong>Note:</strong> You must have enabled Global Cluster Option when you installed VCS.</td>
<td></td>
</tr>
<tr>
<td>Complete the software configuration</td>
<td>See “Completing the VCS configuration” on page 135.</td>
</tr>
</tbody>
</table>
Starting the software configuration

You can configure VCS using the Veritas product installer or the installvcs program command.

**Note:** If you want to reconfigure VCS, 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 VCS 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:

   Veritas Cluster Server

**To configure VCS using the installvcs program**

1. Confirm that you are logged in as the superuser.

2. Start the `installvcs` program, with the configure option.

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

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

   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 VCS. 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 VCS.

   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 rsh 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
   - Verifies that VCS is installed
   - Exits if VCS 6.0.2 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)

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 393.

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.
     Make sure that you activated the NICs for the installer to be able to detect and automatically configure the heartbeat links.
     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.

You must not enter the network interface card that is used for the public network (typically eth0.)

Enter the NIC for the first private heartbeat link on sys1: [b,q,?] eth1
eth1 has an IP address configured on it. It could be a public NIC on sys1.
Are you sure you want to use eth1 for the first private heartbeat link? [y,n,q,b,?] (n) y

Would you like to configure a second private heartbeat link? [y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat link on sys1: [b,q,?] eth2
eth2 has an IP address configured on it. It could be a public NIC on sys1.
Are you sure you want to use eth2 for the second private heartbeat link? [y,n,q,b,?] (n) y

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

Do you want to configure an additional low priority heartbeat link? [y,n,q,b,?] (n)
3 If you chose option 2, enter the NIC details for the private heartbeat links. This step uses examples such as private_NIC1 or private_NIC2 to refer to the available names of the NICs.

Enter the NIC for the first private heartbeat 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: eth0
Enter the NIC for Virtual IP of the Cluster to use on sys1:
[b,q,?] (eth0)

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 eth0 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: eth0
    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: eth0
  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 “Setting up trust relationships for your VCS cluster” on page 125.

See “Configuring a secure cluster node by node” on page 126.

### Configuring Veritas Cluster Server in secure mode

Configuring VCS in secure mode ensures that all the communication between the systems is encrypted and users are verified against security credentials. VCS 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 VCS 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.

Setting up trust relationships for your VCS cluster

If you need to use an external authentication broker for authenticating VCS users, you must set up a trust relationship between VCS and the broker. For example, if Veritas Operations Manager (VOM) is your external authentication broker, the trust relationship ensures that VCS accepts the credentials that VOM issues.

Perform the following steps to set up a trust relationship between your VCS cluster and a broker.

To set up a trust relationship

1. Ensure that you are logged in as superuser on one of the nodes in the cluster.

2. Enter the following command:

   # /opt/VRTS/install/installvcs<version> -securitytrust

   Where <version> is the specific release version.

   The installer specifies the location of the log files. It then lists the cluster information such as cluster name, cluster ID, node names, and service groups.
3 When the installer prompts you for the broker information, specify the IP address, port number, and the data directory for which you want to establish trust relationship with the broker.

Input the broker name of IP address: **15.193.97.204**

Input the broker port: **(14545)**

Specify a port number on which broker is running or press Enter to accept the default port.

Input the data directory to setup trust with: **(/var/VRTSvcs/vcsauth/data/HAD)**

Specify a valid data directory or press Enter to accept the default directory.

4 The installer performs one of the following actions:

- If you specified a valid directory, the installer prompts for a confirmation.

  Are you sure that you want to setup trust for the VCS cluster with the broker 15.193.97.204 and port 14545? [y,n,q] **y**

  The installer sets up trust relationship with the broker for all nodes in the cluster and displays a confirmation.

  Setup trust with broker 15.193.97.204 on cluster node1 .........Done

  Setup trust with broker 15.193.97.204 on cluster node2 .........Done

  The installer specifies the location of the log files, summary file, and response file and exits.

- If you entered incorrect details for broker IP address, port number, or directory name, the installer displays an error. It specifies the location of the log files, summary file, and response file and exits.

---

**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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure security on one node</td>
<td>See “Configuring the first node” on page 127.</td>
</tr>
<tr>
<td>Configure security on the remaining nodes</td>
<td>See “Configuring the remaining nodes” on page 128.</td>
</tr>
<tr>
<td>Complete the manual configuration steps</td>
<td>See “Completing the secure cluster configuration” on page 128.</td>
</tr>
</tbody>
</table>

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/installvcs<version> -securityonenode
   ```
   
   Where `<version>` is the specific release version.

   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/installvcs<version> -securityoncnode
```

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

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

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

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 132.

3. Provide information to configure SMTP notification.

   Provide the following information:

   - Enter the NIC information.

     Active NIC devices discovered on sys1: eth0
     Enter the NIC for the VCS Notifier to use on sys1: [b,q,?] (eth0)
     Is eth0 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: eth0
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 VCS based on the configuration details you provided.

   See “Configuring global clusters” on page 134.

3  Provide information to configure SNMP trap notification.

   Provide the following information:

   ■ Enter the NIC information.

       Active NIC devices discovered on sys1: eth0
       Enter the NIC for the VCS Notifier to use on sys1: [b,q,?] (eth0)
       Is eth0 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: eth0
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. If not, the installer proceeds to configure VCS based on the configuration details you provided. You can also run the gcoconfig utility in each cluster later to update the VCS configuration file for global cluster.

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

See the *Veritas Cluster Server Administrator’s Guide* for instructions to set up VCS 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: eth0
   IP: 10.198.89.22
   Netmask: 255.255.240.0

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

   For IPv6: Global Cluster Option configuration verification:

   NIC: eth0
   Prefix: 64

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

Completing the VCS configuration

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

To complete the VCS configuration

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

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

2. Review the output as the installer stops various processes and performs the configuration. The installer then restarts VCS 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 VCS successfully, note the location of summary, log, and response files that installer creates.

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

   summary file  Describes the cluster and its configured resources.
   log file       Details the entire configuration.
   response file  Contains the configuration information that can be used to perform secure or unattended installations on other systems.

   See “Configuring VCS using response files” on page 169.

Verifying the NIC configuration

The installer verifies on all the nodes if all NICs have PERSISTENT_NAME set correctly.

If the persistent interface names are not configured correctly for the network devices, the installer displays the following messages:

   PERSISTENT_NAME is not set for all the NICs.
   You need to set them manually before the next reboot.

Set the PERSISTENT_NAME for all the NICs.

See “Performing preinstallation tasks” on page 59.
Warning: If the installer finds the network interface name to be different from the name in the configuration file, then the installer exits.

Verifying and updating licenses on the system

After you install VCS, 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 137.
See “Updating product licenses” on page 138.

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.

   License Key = xxx-xxx-xxx-xxx-xxx
   Product Name = Veritas Cluster Server
   Serial Number = xxxxx
   License Type = PERMANENT
   OEM ID = xxxxx

   Features :=
   Platform = Linux
   Version = 6.0
   Tier = 0
   Reserved = 0
   Mode = VCS
Updating product licenses

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

See “Replacing a VCS demo license with a permanent license” on page 138.

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 VCS demo license with a permanent license

When a VCS 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 VCS 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 VCS.

    # vxlicrep

5  Start VCS on each node:

    # hastart
Configuring VCS clusters for data integrity

This chapter includes the following topics:

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

Setting up disk-based I/O fencing using installvcs program

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

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:
   
   ```
   # fdisk -l
   ```

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 sdr
  ```

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

### Configuring disk-based I/O fencing using installvcs program

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

**To set up disk-based I/O fencing using the installvcs program**

1. Start the `installvcs` program with `-fencing` option.

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

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

   The `installvcs` program 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 VCS 6.0.2 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 143.

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 VCS 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 228.
Checking shared disks for I/O fencing

Make sure that the shared storage you set up while preparing to configure VCS 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 Cluster Server Administrator's Guide*.

Checking that disks support SCSI-3 involves the following tasks:

- Verifying the Array Support Library (ASL)
  See “Verifying Array Support Library (ASL)” on page 143.
- Verifying that nodes have access to the same disk
  See “Verifying that the nodes have access to the same disk” on page 144.
- Testing the shared disks for SCSI-3
  See “Testing the disks using vxfentsthdw utility” on page 145.

**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
   ```

<table>
<thead>
<tr>
<th>LIBNAME</th>
<th>VID</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>libvxhitachi.so</td>
<td>HITACHI</td>
<td>DF350, DF400, DF400P,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DF500, DF500F</td>
</tr>
<tr>
<td>libvxxp1281024.so</td>
<td>HP</td>
<td>All</td>
</tr>
<tr>
<td>libvxxp12k.so</td>
<td>HP</td>
<td>All</td>
</tr>
<tr>
<td>libvxddns2a.so</td>
<td>DDN</td>
<td>S2A 9550, S2A 9900,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2A 9700</td>
</tr>
<tr>
<td>libvxpurple.so</td>
<td>SUN</td>
<td>T300</td>
</tr>
<tr>
<td>libvxxiotechE5k.so</td>
<td>XIOTECH</td>
<td>ISE1400</td>
</tr>
<tr>
<td>libvxcopan.so</td>
<td>COPANSYS</td>
<td>8814, 8818</td>
</tr>
<tr>
<td>libvxibmds8k.so</td>
<td>IBM</td>
<td>2107</td>
</tr>
</tbody>
</table>

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 VCS.

2. Ensure that both nodes are connected to the same disk during the testing. Use the vxfenadm command to verify the disk serial number.

   ```bash
   # vxfenadm -i diskpath
   ```

   Refer to the vxfenadm (1M) manual page.

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

   From node A, enter:

   ```bash
   # vxfenadm -i /dev/sdx
   ```

   SCSI ID=>Host: 2 Channel: 0 Id: 0 Lun: E

   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/sdy path.

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

   ```bash
   # vxfenadm -i /dev/sdz
   ```

   SCSI ID=>Host: 2 Channel: 0 Id: 0 Lun: E

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

Testing the disks using vxfentsthdw utility

This procedure uses the /dev/sdx 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/sdx 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 Cluster Server Administrator's Guide*.

**To test the disks using vxfentsthdw utility**

1. Make sure system-to-system communication functions properly.
   See “*Setting up inter-system communication*” on page 407.

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 sys1 in the format:
for dmp: /dev/vx/rdmp/sdx
for raw: /dev/sdx
Make sure it's the same disk as seen by nodes sys1 and sys2
/dev/sdr

Enter the disk name to be checked for SCSI-3 PGR on node sys2 in the format:
for dmp: /dev/vx/rdmp/sdx
for raw: /dev/sdx
Make sure it's the same disk as seen by nodes sys1 and sys2
/dev/sdr

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/sdx 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 installvcs program

You can configure server-based I/O fencing for the VCS cluster using the installvcs program.

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 “Recommended CP server configurations” on page 92.

This section covers the following example procedures:

| Mix of CP servers and coordinator disks | See “To configure server-based fencing for the VCS cluster (one CP server and two coordinator disks)” on page 148. |
| Single CP server | See “To configure server-based fencing for the VCS cluster (single CP server)” on page 153. |

To configure server-based fencing for the VCS 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 VCS cluster. The VCS cluster is also referred to as the application cluster or the client cluster.
   - The coordination disks are verified for SCSI3-PR compliance. See “Checking shared disks for I/O fencing” on page 143.

2. Start the installvcs program with the -fencing option.
   
   ```
   # /opt/VRTS/install/installvcs<version> -fencing
   ```
   Where <version> is the specific release version. The installvcs program starts with a copyright message and verifies the cluster information.
   
   Note the location of log files which you can access in the event of any problem with the configuration process.

3. Confirm that you want to proceed with the I/O fencing configuration at the prompt.
   
   The program checks that the local node running the script can communicate with remote nodes and checks whether VCS 6.0.2 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 VCS (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) sdx
  2) sdy
  3) sdz

  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] (vxfenceoorddg)
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. sdx
   2. sdy
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 VCS (application cluster) node.

10 If the CP server is configured for security, the installer sets up secure communication between the CP server and the VCS (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 379.

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 VCS (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)
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

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 VCS cluster (single CP server)

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

2

3 Start the installvcs program with -fencing option.

    # /opt/VRTS/install/installvcs<version> -fencing

Where <version> is the specific release version. The installvcs program 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.

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 VCS 6.0.2 is configured properly.

5 Review the I/O fencing configuration options that the program presents. Type 1 to configure server-based I/O fencing.

    Select the fencing mechanism to be configured in this Application Cluster [1-4,b,q] 1
6 Make sure that the storage supports SCSI3-PR, and answer y at the following prompt.

Does your storage environment support SCSI3 PR? [y,n,q] (y)

7 Enter the total number of coordination points as 1.

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

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

8 Provide the following CP server details at the installer prompt:

- Enter the total number of virtual IP addresses or the total number of fully qualified host names for each of the CP servers.

  Enter the total number of Virtual IP addresses or fully qualified host name for the Coordination Point Server #1: [b,q,?] (1) 2

- Enter the virtual IP address or the fully qualified host name for the CP server. The installer assumes these values to be identical as viewed from all the application cluster nodes.

  Enter the Virtual IP address or fully qualified host name #1 for the Coordination Point Server #1: [b] 10.209.80.197

  The installer prompts for this information for the number of virtual IP addresses you want to configure for each CP server.

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

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

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

For example:

Total number of coordination points being used: 1
Coordination Point Server ([VIP or FQHN]:Port):
  1. 10.109.80.197 ([10.109.80.197]:14250)
10 If the CP server is configured for security, the installer sets up secure communication between the CP server and the VCS (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 379.

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 VCS (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 installvcs program

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 installvcs program in a non-SCSI-3 PR-compliant setup

1 Start the installvcs program with -fencing option.

```bash
# /opt/VRTS/install/installvcs<version> -fencing
```

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

The installvcs program 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 VCS 6.0.2 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 VCS 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 VCS 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 VCS cluster with the CP server.
     ■ Adds CP server user to the CP server.
     ■ Adds VCS cluster to the CP server user.
   ■ Updates the following configuration files on each node of the VCS cluster
     ■ `/etc/vxfenmode file`
     ■ `/etc/vxenviron file`
     ■ `/etc/sysconfig/vxfen file`
     ■ `/etc/llttab file`
     ■ `/etc/vxfentab file`
10 Review the output as the installer stops VCS on each node, starts I/O fencing on each node, updates the VCS configuration file main.cf, and restarts VCS with non-SCSI-3 server-based fencing.

Confirm to configure the CP agent on the VCS 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 31.

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
Automated installation using response files

- Chapter 10. Performing an automated VCS installation
- Chapter 11. Performing an automated VCS configuration
- Chapter 12. Performing an automated I/O fencing configuration using response files
Performing an automated VCS installation

This chapter includes the following topics:

- Installing VCS using response files
- Response file variables to install VCS
- Sample response file for installing VCS

Installing VCS using response files

Typically, you can use the response file that the installer generates after you perform VCS installation on one cluster to install VCS on other clusters. You can also create a response file using the `makeresponsefile` option of the installer.

To install VCS using response files

1. Make sure the systems where you want to install VCS meet the installation requirements.
   
   See “Important preinstallation information for VCS” on page 33.

2. Make sure the preinstallation tasks are completed.
   
   See “Performing preinstallation tasks” on page 59.

3. Copy the response file to one of the cluster systems where you want to install VCS.

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
# ./installvcs -responsefile /tmp/response_file
```

Where /tmp/response_file is the response file's full path name.

## Response file variables to install VCS

Table 10-1 lists the response file variables that you can define to install VCS.

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[opt][install]</td>
<td>Scalar</td>
<td>Installs VCS RPMs. (Required)</td>
</tr>
<tr>
<td>CFG[acquiteula]</td>
<td>Scalar</td>
<td>Specifies whether you agree with EULA.pdf on the media. (Required)</td>
</tr>
<tr>
<td>CFG[systems]</td>
<td>List</td>
<td>List of systems on which the product is to be installed. Required</td>
</tr>
<tr>
<td>CFG[prod]</td>
<td>Scalar</td>
<td>Defines the product to be installed. The value is VCS60 for VCS. (Required)</td>
</tr>
</tbody>
</table>
Table 10-1  Response file variables specific to installing VCS (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[opt]{installallpkgs} or CFG[opt]{installrecpkgs} or CFG[opt]{installminpkgs}</td>
<td>Scalar</td>
<td>Instructs the installer to install VCS RPMs based on the variable that has the value set to 1:  ■ installallpkgs: Installs all RPMs  ■ installrecpkgs: Installs recommended RPMs  ■ installminpkgs: Installs minimum RPMs  <strong>Note:</strong> The installer requires only one of these variable values to be set to 1. (Required)</td>
</tr>
<tr>
<td>CFG[opt]{rsh}</td>
<td>Scalar</td>
<td>Defines that <em>rsh</em> must be used instead of <em>ssh</em> as the communication method between systems. (Optional)</td>
</tr>
<tr>
<td>CFG[opt]{gco}</td>
<td>Scalar</td>
<td>Defines that the installer must enable the global cluster option. You must set this variable value to 1 if you want to configure global clusters. (Optional)</td>
</tr>
<tr>
<td>CFG[opt]{keyfile}</td>
<td>Scalar</td>
<td>Defines the location of an <em>ssh</em> keyfile that is used to communicate with all remote systems. (Optional)</td>
</tr>
<tr>
<td>CFG[opt]{patchpath}</td>
<td>Scalar</td>
<td>Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems. (Optional)</td>
</tr>
</tbody>
</table>
### Table 10-1  Response file variables specific to installing VCS (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{opt</td>
<td>pkgpath}</td>
<td>Scalar</td>
</tr>
<tr>
<td>CFG{opt</td>
<td>tmppath}</td>
<td>Scalar</td>
</tr>
<tr>
<td>CFG{opt</td>
<td>logpath}</td>
<td>Scalar</td>
</tr>
<tr>
<td>CFG{opt</td>
<td>vxkeyless}</td>
<td>Scalar</td>
</tr>
<tr>
<td>CFG{keys</td>
<td>system}</td>
<td>Scalar</td>
</tr>
<tr>
<td>CFG{sso_console_ip}</td>
<td>Scalar</td>
<td>Specifies the IP address of the associated Symantec High Availability Console. (Required)</td>
</tr>
</tbody>
</table>
Table 10-1  Response file variables specific to installing VCS (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{sso_local_username}</td>
<td>Scalar</td>
<td>Specifies the user name (administrative user account) by using which you can install Symantec Application HA or Veritas Cluster Server on the required virtual machine. (Required)</td>
</tr>
<tr>
<td>CFG{sso_local_password}</td>
<td>Scalar</td>
<td>Specifies the password (for the administrative user account) by using which you can install Application HA or Veritas Cluster Server on the required virtual machine. (Required)</td>
</tr>
<tr>
<td>$CFG{uuid}</td>
<td>Scalar</td>
<td>Defines a UUID for Veritas Cluster Server (optional)</td>
</tr>
<tr>
<td>$CFG{systemscfg}</td>
<td>List</td>
<td>Defines system names of all system nodes in a cluster. (optional)</td>
</tr>
</tbody>
</table>

Sample response file for installing VCS

Review the response file variables and their definitions.

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

$CFG{accepteula}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installrecpkgs}=1;
$CFG{prod}="VCS60";
```

Performing an automated VCS installation
Performing an automated VCS installation
Sample response file for installing VCS

$CFG{systems}=[ qw(sys1 sys2) ];
$CFG{systemscfg}=[ qw(redhat89233 redhat89244) ];
$CFG{uuid} = "16889f4e-1dd2-11b2-a559-afce02598e1b";
Performing an automated VCS configuration

This chapter includes the following topics:

- Configuring VCS using response files
- Response file variables to configure Veritas Cluster Server
- Sample response file for configuring VCS

Configuring VCS using response files

Typically, you can use the response file that the installer generates after you perform VCS configuration on one cluster to configure VCS on other clusters. You can also create a response file using the -makeresponsefile option of the installer.

To configure VCS using response files

1. Make sure the VCS RPMs are installed on the systems where you want to configure VCS.
2. Copy the response file to one of the cluster systems where you want to configure VCS.

See “Sample response file for configuring VCS” on page 179.
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 Cluster Server" on page 170.

4 Start the configuration from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/installvcs<version>
    -responsefile /tmp/response_file
```

Where `<version>` is the specific release version, and `/tmp/response_file` is the response file's full path name.

Response file variables to configure Veritas Cluster Server

Table 11-1 lists the response file variables that you can define to configure VCS.

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$CFG[config_cfs]</td>
<td>Scalar</td>
<td>Performs the Cluster File System configuration for VCS. (Required)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set the value to 1 to configure Cluster File System for VCS.</td>
</tr>
<tr>
<td>CFG[opt]{configure}</td>
<td>Scalar</td>
<td>Performs the configuration if the RPMs are already installed. (Required)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set the value to 1 to configure VCS.</td>
</tr>
<tr>
<td>CFG[accepteula]</td>
<td>Scalar</td>
<td>Specifies whether you agree with EULA.pdf on the media. (Required)</td>
</tr>
<tr>
<td>CFG[systems]</td>
<td>List</td>
<td>List of systems on which the product is to be configured. (Required)</td>
</tr>
</tbody>
</table>
Table 11-1  Response file variables specific to configuring Veritas Cluster Server (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{prod}</td>
<td>Scalar</td>
<td>Defines the product to be configured. The value is VCS60 for VCS. (Required)</td>
</tr>
<tr>
<td>CFG{opt}{keyfile}</td>
<td>Scalar</td>
<td>Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)</td>
</tr>
<tr>
<td>CFG{opt}{rsh}</td>
<td>Scalar</td>
<td>Defines that rsh must be used instead of ssh as the communication method between systems. (Optional)</td>
</tr>
<tr>
<td>CFG{opt}{logpath}</td>
<td>Scalar</td>
<td>Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. <strong>Note</strong>: The installer copies the response files and summary files also to the specified logpath location. (Optional)</td>
</tr>
<tr>
<td>CFG{uploadlogs}</td>
<td>Scalar</td>
<td>Defines a Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site. (Optional)</td>
</tr>
</tbody>
</table>

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 11-2 lists the response file variables that specify the required information to configure a basic VCS cluster.

### Table 11-2 Response file variables specific to configuring a basic VCS cluster

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_clusterid}</td>
<td>Scalar</td>
<td>An integer between 0 and 65535 that uniquely identifies the cluster. (Required)</td>
</tr>
<tr>
<td>CFG{vcs_clustername}</td>
<td>Scalar</td>
<td>Defines the name of the cluster. (Required)</td>
</tr>
<tr>
<td>CFG{vcs_allowcomms}</td>
<td>Scalar</td>
<td>Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)</td>
</tr>
<tr>
<td>CFG{fencingenabled}</td>
<td>Scalar</td>
<td>In a VCS configuration, defines if fencing is enabled. Valid values are 0 or 1. (Required)</td>
</tr>
</tbody>
</table>

Table 11-3 lists the response file variables that specify the required information to configure LLT over Ethernet.

### Table 11-3 Response file variables specific to configuring private LLT over Ethernet

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_lttlink#}</td>
<td>Scalar</td>
<td>Defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (lltlink1 and lltlink2). You can configure up to four LLT links. You must enclose the system name within double quotes. (Required)</td>
</tr>
</tbody>
</table>
Table 11-3  Response file variables specific to configuring private LLT over Ethernet (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_lltlinklowpri}</td>
<td>Scalar</td>
<td>Defines a low priority heartbeat link. Typically, lltlinklowpri is used on a public network link to provide an additional layer of communication. If you use different media speed for the private NICs, you can configure the NICs with lesser speed as low-priority links to enhance LLT performance. For example, lltlinklowpri1, lltlinklowpri2, and so on. You must enclose the system name within double quotes. (Optional)</td>
</tr>
</tbody>
</table>

Table 11-4 lists the response file variables that specify the required information to configure LLT over UDP.

Table 11-4  Response file variables specific to configuring LLT over UDP

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{lltoverudp}=1</td>
<td>Scalar</td>
<td>Indicates whether to configure heartbeat link using LLT over UDP. (Required)</td>
</tr>
<tr>
<td>CFG{vcs_udplink&lt;n&gt;_address}</td>
<td>Scalar</td>
<td>Stores the IP address (IPv4 or IPv6) that the heartbeat link uses on node1. You can have four heartbeat links and &lt;n&gt; for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required)</td>
</tr>
</tbody>
</table>

173Performing an automated VCS configuration
Table 11-4  
Response file variables specific to configuring LLT over UDP  
(continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
</table>
| CFG {vcs_udplinklowpri<n>_address} <system1> | Scalar          | Stores the IP address (IPv4 or IPv6) that the low priority heartbeat link uses on node1.  
You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links.  
(Required)                                      |
| CFG{vcs_udplink<n>_port} <system1> | Scalar          | Stores the UDP port (16-bit integer value) that the heartbeat link uses on node1.  
You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links.  
(Required)                                      |
| CFG{vcs_udplinklowpri<n>_port} <system1> | Scalar          | Stores the UDP port (16-bit integer value) that the low priority heartbeat link uses on node1.  
You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links.  
(Required)                                      |
| CFG{vcs_udplink<n>_netmask} <system1> | Scalar          | Stores the netmask (prefix for IPv6) that the heartbeat link uses on node1.  
You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links.  
(Required)                                      |
Table 11-4  Response file variables specific to configuring LLT over UDP (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_udplinklowpri&lt;n&gt;_netmask} {&lt;system1&gt;}</td>
<td>Scalar</td>
<td>Stores the netmask (prefix for IPv6) that the low priority heartbeat link uses on node1. You can have four low priority heartbeat links and &lt;n&gt; for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required)</td>
</tr>
</tbody>
</table>

Table 11-5 lists the response file variables that specify the required information to configure virtual IP for VCS cluster.

Table 11-5  Response file variables specific to configuring virtual IP for VCS cluster

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_csgnic} {system}</td>
<td>Scalar</td>
<td>Defines the NIC device to use on a system. You can enter ‘all’ as a system value if the same NIC is used on all systems. (Optional)</td>
</tr>
<tr>
<td>CFG{vcs_csgvip}</td>
<td>Scalar</td>
<td>Defines the virtual IP address for the cluster. (Optional)</td>
</tr>
<tr>
<td>CFG{vcs_csgnetmask}</td>
<td>Scalar</td>
<td>Defines the Netmask of the virtual IP address for the cluster. (Optional)</td>
</tr>
</tbody>
</table>

Table 11-6 lists the response file variables that specify the required information to configure the VCS cluster in secure mode.
Table 11-6  Response file variables specific to configuring VCS cluster in secure mode

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[vcs_eat_security]</td>
<td>Scalar</td>
<td>Specifies if the cluster is in secure enabled mode or not.</td>
</tr>
<tr>
<td>CFG[opt][securityonenode]</td>
<td>Scalar</td>
<td>Specifies that the securityonenode option is being used.</td>
</tr>
<tr>
<td>CFG[securityonenode_menu]</td>
<td>Scalar</td>
<td>Specifies the menu option to choose to configure the secure cluster one at a time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 1—Configure the first node</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 2—Configure the other node</td>
</tr>
<tr>
<td>CFG[security_conf_dir]</td>
<td>Scalar</td>
<td>Specifies the directory where the configuration files are placed.</td>
</tr>
<tr>
<td>CFG[opt][security]</td>
<td>Scalar</td>
<td>Specifies that the security option is being used.</td>
</tr>
<tr>
<td>CFG[opt][fips]</td>
<td>Scalar</td>
<td>Specifies that the FIPS option is being used.</td>
</tr>
<tr>
<td>CFG[vcs_eat_security_fips]</td>
<td>Scalar</td>
<td>Specifies that the enabled security is FIPS compliant.</td>
</tr>
</tbody>
</table>

Table 11-7 lists the response file variables that specify the required information to configure VCS users.

Table 11-7  Response file variables specific to configuring VCS users

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[vcs_userenpw]</td>
<td>List</td>
<td>List of encoded passwords for VCS users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value in the list can be &quot;Administrators Operators Guests&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The order of the values for the vcs_userenpw list must match the order of the values in the vcs_username list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
</tbody>
</table>
Table 11-7  Response file variables specific to configuring VCS users (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_username}</td>
<td>List</td>
<td>List of names of VCS users (Optional)</td>
</tr>
<tr>
<td>CFG{vcs_userpriv}</td>
<td>List</td>
<td>List of privileges for VCS users</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The order of the values for the vcs_userpriv list must match the order of the values in the vcs_username list. (Optional)</td>
</tr>
</tbody>
</table>

Table 11-8 lists the response file variables that specify the required information to configure VCS notifications using SMTP.

Table 11-8  Response file variables specific to configuring VCS notifications using SMTP

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_smtpserver}</td>
<td>Scalar</td>
<td>Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for Web notification. (Optional)</td>
</tr>
<tr>
<td>CFG{vcs_smtprecp}</td>
<td>List</td>
<td>List of full email addresses (example: <a href="mailto:user@symantecexample.com">user@symantecexample.com</a>) of SMTP recipients. (Optional)</td>
</tr>
<tr>
<td>CFG{vcs_smtpredev}</td>
<td>List</td>
<td>Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SMTP recipients are to receive. Note that the ordering of severity levels must match that of the addresses of SMTP recipients. (Optional)</td>
</tr>
</tbody>
</table>
Table 11-9 lists the response file variables that specify the required information to configure VCS notifications using SNMP.

**Table 11-9  Response file variables specific to configuring VCS notifications using SNMP**

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[vcs_snmpport]</td>
<td>Scalar</td>
<td>Defines the SNMP trap daemon port (default=162). (Optional)</td>
</tr>
<tr>
<td>CFG[vcs_snmpcons]</td>
<td>List</td>
<td>List of SNMP console system names (Optional)</td>
</tr>
<tr>
<td>CFG[vcs_snmpcsev]</td>
<td>List</td>
<td>Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names. (Optional)</td>
</tr>
</tbody>
</table>

Table 11-10 lists the response file variables that specify the required information to configure VCS global clusters.

**Table 11-10  Response file variables specific to configuring VCS global clusters**

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[vcs_gconic] {system}</td>
<td>Scalar</td>
<td>Defines the NIC for the Virtual IP that the Global Cluster Option uses. You can enter ‘all’ as a system value if the same NIC is used on all systems. (Optional)</td>
</tr>
<tr>
<td>CFG[vcs_gcovip]</td>
<td>Scalar</td>
<td>Defines the virtual IP address to that the Global Cluster Option uses. (Optional)</td>
</tr>
</tbody>
</table>
Table 11-10  Response file variables specific to configuring VCS global clusters (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_gconetmask}</td>
<td>Scalar</td>
<td>Defines the Netmask of the virtual IP address that the Global Cluster Option uses. (Optional)</td>
</tr>
</tbody>
</table>

Sample response file for configuring VCS

Review the response file variables and their definitions.

See “Response file variables to configure Veritas Cluster Server” on page 170.

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

$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{prod}="VCS601";
$CFG{systems}=[ qw(sys1 sys2) ];
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=13221;
$CFG{vcs_clustername}="clus1";
$CFG{vcs_csgnetmask}="255.255.255.0";
$CFG{vcs_csgnic}{all}="eth0";
$CFG{vcs_csgvip}="10.10.12.1";
$CFG{vcs_gconetmask}="255.255.255.0";
$CFG{vcs_gcovip}="10.10.12.1";
$CFG{vcs_l1ltlink1}{sys1}="eth1";
$CFG{vcs_l1ltlink1}{sys2}="eth1";
$CFG{vcs_l1ltlink2}{sys1}="eth2";
$CFG{vcs_l1ltlink2}{sys2}="eth2";

$CFG{vcs_smtprecp}=[ qw(earnie@symantecexample.com) ];
$CFG{vcs_smtpsev}=[ qw(SevereError) ];
$CFG{vcssmtpserver}="smtp.symantecexample.com";
$CFG{vcs_snmpcons}=[ qw(neptune) ];
$CFG{vcs_snmpcsev}=[ qw(SevereError) ];
```
Performing an automated VCS configuration

Sample response file for configuring VCS

$CFG{vcs_snmpport}=162;
1;
Performing an automated I/O fencing configuration using response files

This chapter includes the following topics:

- Configuring I/O fencing using response files
- Response file variables to configure disk-based I/O fencing
- Sample response file for configuring disk-based I/O fencing
- Response file variables to configure server-based I/O fencing
- Sample response file for configuring server-based I/O fencing
- Response file variables to configure non-SCSI-3 server-based I/O fencing
- Sample response file for configuring non-SCSI-3 server-based I/O fencing

Configuring I/O fencing using response files

Typically, you can use the response file that the installer generates after you perform I/O fencing configuration to configure I/O fencing for VCS.

To configure I/O fencing using response files

1. Make sure that VCS 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.
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 185.

See “Sample response file for configuring server-based I/O fencing” on page 187.

4 Edit the values of the response file variables as necessary.

See “Response file variables to configure disk-based I/O fencing” on page 182.

See “Response file variables to configure server-based I/O fencing” on page 186.

5 Start the configuration from the system to which you copied the response file. For example:

```bash
# /opt/VRTS/install/installvcs<version>
-respfile /tmp/response_file
```

Where `<version>` is the specific release version, and `/tmp/response_file` is the response file’s full path name.

### Response file variables to configure disk-based I/O fencing

Table 12-1 lists the response file variables that specify the required information to configure disk-based I/O fencing for VCS.

**Table 12-1**

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[opt][fencing]</td>
<td>Scalar</td>
<td>Performs the I/O fencing configuration. (Required)</td>
</tr>
</tbody>
</table>
### Table 12-1  
Response file variables specific to configuring disk-based I/O fencing (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{fencing_option}</td>
<td>Scalar</td>
<td>Specifies the I/O fencing configuration mode.</td>
</tr>
</tbody>
</table>
|                           |                | ■ 1—Coordination Point Server-based I/O fencing  
■ 2—Coordinator disk-based I/O fencing  
■ 3—Disabled mode  
■ 4—Fencing migration when the cluster is online (Required) |
| CFG {fencing_scsi3_disk_policy} | Scalar | Specifies the I/O fencing mechanism. This variable is not required if you had configured fencing in disabled mode. For disk-based fencing, you must configure the fencing_scsi3_disk_policy variable and either the fencing_dgname variable or the fencing_newdg_disks variable. (Optional) |
| CFG{fencing_dgname}       | Scalar         | Specifies the disk group for I/O fencing. (Optional)                                                                                                                                                       |

**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 12-1  Response file variables specific to configuring disk-based I/O fencing

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
</table>
| CFG[fencing_newdg_disks]      | List           | Specifies the disks to use to create a new disk group for I/O fencing. (Optional)                                                                ;
|                               |                | **Note:** You must define the 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_cagent_monitor_freq] | Scalar       | Specifies the frequency at which the Coordination Point Agent monitors for any changes to the Coordinator Disk Group constitution.  
**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. |
### Table 12-1  
Response file variables specific to configuring disk-based I/O fencing (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG {fencing_config_cpagent}</td>
<td>Scalar</td>
<td>Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter &quot;0&quot; if you do not want to configure the Coordination Point agent using the installer. Enter &quot;1&quot; if you want to use the installer to configure the Coordination Point agent.</td>
</tr>
</tbody>
</table>
| CFG {fencing_cpagentgrp} | Scalar | Name of the service group which will have the Coordination Point agent resource as part of it. 
**Note:** This field is obsolete if the fencing_config_cpagent field is given a value of '0'. |

---

### Sample response file for configuring disk-based I/O fencing

Review the disk-based I/O fencing response file variables and their definitions. See “Response file variables to configure disk-based I/O fencing” on page 182.

```bash
#
# 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}="VCS601";

$CFG{systems}=\{ qw(pilot25) \};
$CFG{vcs_clusterid}=32283;
$CFG{vcs_clustername}="whf";
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 12-2 lists the fields in the response file that are relevant for server-based customized I/O fencing.

<table>
<thead>
<tr>
<th>Response file field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG {fencing_config_cpagent}</td>
<td>Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not.</td>
</tr>
<tr>
<td></td>
<td>Enter &quot;0&quot; if you do not want to configure the Coordination Point agent using the installer.</td>
</tr>
<tr>
<td></td>
<td>Enter &quot;1&quot; if you want to use the installer to configure the Coordination Point agent.</td>
</tr>
<tr>
<td>CFG {fencing_cpagentgrp}</td>
<td>Name of the service group which will have the Coordination Point agent resource as part of it.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is obsolete if the fencing_config_cpagent field is given a value of '0'.</td>
</tr>
<tr>
<td>CFG {fencing_cps}</td>
<td>Virtual IP address or Virtual hostname of the CP servers.</td>
</tr>
</tbody>
</table>
Table 12-2  Coordination point server (CP server) based fencing response file definitions (continued)

<table>
<thead>
<tr>
<th>Response file field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG {fencing_reusedg}</td>
<td>This response file field indicates whether to reuse an existing DG name for the fencing configuration in customized fencing (CP server and coordinator disks). Enter either a &quot;1&quot; or &quot;0&quot;. Entering a &quot;1&quot; indicates reuse, and entering a &quot;0&quot; indicates do not reuse. When reusing an existing DG name for the mixed mode fencing configuration, you need to manually add a line of text, such as &quot;$CFG{fencing_reusedg}=0&quot; or &quot;$CFG{fencing_reusedg}=1&quot; before proceeding with a silent installation.</td>
</tr>
<tr>
<td>CFG {fencing_dgname}</td>
<td>The name of the disk group to be used in the customized fencing, where at least one disk is being used.</td>
</tr>
<tr>
<td>CFG {fencing_disks}</td>
<td>The disks being used as coordination points if any.</td>
</tr>
<tr>
<td>CFG {fencing_ncp}</td>
<td>Total number of coordination points being used, including both CP servers and disks.</td>
</tr>
<tr>
<td>CFG {fencing_ndisks}</td>
<td>The number of disks being used.</td>
</tr>
<tr>
<td>CFG {fencing_cps_vips}</td>
<td>The virtual IP addresses or the fully qualified host names of the CP server.</td>
</tr>
<tr>
<td>CFG {fencing_ports}</td>
<td>The port that the virtual IP address or the fully qualified host name of the CP server listens on.</td>
</tr>
<tr>
<td>CFG {fencing_scsi3_disk_policy}</td>
<td>The disk policy that the customized fencing uses. The value for this field is either &quot;raw&quot; or &quot;dmp&quot;</td>
</tr>
</tbody>
</table>

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) ];
```
Response file variables to configure non-SCSI-3 server-based I/O fencing

Table 12-3 lists the fields in the response file that are relevant for non-SCSI-3 server-based customized I/O fencing.

See “About I/O fencing for VCS in virtual machines that do not support SCSI-3 PR” on page 29.

Table 12-3: Non-SCSI-3 server-based I/O fencing response file definitions

<table>
<thead>
<tr>
<th>Response file field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{non_scsi3_fencing}</td>
<td>Defines whether to configure non-SCSI-3 server-based I/O fencing. Valid values are 1 or 0. Enter 1 to configure non-SCSI-3 server-based I/O fencing.</td>
</tr>
<tr>
<td>CFG{fencing_config_cpagent}</td>
<td>Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter '0' if you do not want to configure the Coordination Point agent using the installer. Enter '1' if you want to use the installer to configure the Coordination Point agent.</td>
</tr>
</tbody>
</table>
Table 12-3  Non-SCSI-3 server-based I/O fencing response file definitions (continued)

<table>
<thead>
<tr>
<th>Response file field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG {fencing_cpagentgrp}</td>
<td>Name of the service group which will have the Coordination Point agent resource as part of it.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is obsolete if the fencing_config_cpagent field is given a value of '0'.</td>
</tr>
<tr>
<td>CFG {fencing_cps}</td>
<td>Virtual IP address or Virtual hostname of the CP servers.</td>
</tr>
<tr>
<td>CFG {fencing_cps_vips}</td>
<td>The virtual IP addresses or the fully qualified host names of the CP server.</td>
</tr>
<tr>
<td>CFG {fencing_ncp}</td>
<td>Total number of coordination points (CP servers only) being used.</td>
</tr>
<tr>
<td>CFG {fencing_ports}</td>
<td>The port of the CP server that is denoted by cps.</td>
</tr>
</tbody>
</table>

Sample response file for configuring non-SCSI-3 server-based I/O fencing

The following is a sample response file used for non-SCSI-3 server-based I/O fencing:

```
$CFG{fencing_config_cpagent}=0;
$CFG{fencing_cps}={ qw(10.198.89.251 10.198.89.252 10.198.89.253) };
$CFG{fencing_cps_vips}{"10.198.89.251"}={ qw(10.198.89.251) };
$CFG{fencing_cps_vips}{"10.198.89.252"}={ qw(10.198.89.252) };
$CFG{fencing_cps_vips}{"10.198.89.253"}={ qw(10.198.89.253) };
$CFG{fencing_ncp}=3;
$CFG{fencing_ndisks}=0;
$CFG{fencing_ports}"10.198.89.251"=14250;
$CFG{fencing_ports}"10.198.89.252"=14250;
$CFG{fencing_ports}"10.198.89.253"=14250;
$CFG{non_scsi3_fencing}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="VCS60";
$CFG{systems}={ qw(sys1 sys2) };
$CFG{vcs_clusterid}=1256;
```
Performing an automated I/O fencing configuration using response files

Sample response file for configuring non-SCSI-3 server-based I/O fencing

```bash
$CFG{vcs_clustername}="clus1";
$CFG{fencing_option}=1;
```
Manual installation

- Chapter 13. Performing preinstallation tasks
- Chapter 14. Manually installing VCS
- Chapter 15. Manually configuring VCS
- Chapter 16. Manually configuring the clusters for data integrity
Performing preinstallation tasks

This chapter includes the following topics:

■ Preparing for a manual installation
■ Requirements for installing VCS

Preparing for a manual installation

Before you start installation, log in as the superuser. Mount the disc, copy the files to a temporary location locally for your convenience. Each operating system occupies an entire disc. Each disc has an identical directory structure.

To prepare for installation

1. Log in as the superuser.
2. Mount the appropriate disc.
3. Copy the files to a temporary location on the system.

```bash
# cp -r rpms/* /tmp/install
```

Requirements for installing VCS

Review requirements before you install.

See “Important preinstallation information for VCS” on page 33.
Performing preinstallation tasks

Requirements for installing VCS
Manually installing VCS

This chapter includes the following topics:

- About VCS manual installation
- Installing VCS software manually

About VCS manual installation

You can manually install and configure VCS instead of using the installvcs program.

A manual installation takes a lot of time, patience, and care. Symantec recommends that you use the installvcs program instead of the manual installation when possible.

Installing VCS software manually

Table 14-1 lists the tasks that you must perform when you manually install and configure VCS 6.0.2.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install VCS software manually on each node in the cluster.</td>
<td>See “Adding a license key for a manual installation” on page 199.</td>
</tr>
<tr>
<td>Add a license key.</td>
<td></td>
</tr>
<tr>
<td>Copy the installation guide to each node.</td>
<td>See “Copying the installation guide to each node” on page 201.</td>
</tr>
</tbody>
</table>
Table 14-1 Manual installation tasks for VCS 6.0.2 (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LLT and GAB.</td>
<td>■ See “Configuring LLT manually” on page 203.</td>
</tr>
<tr>
<td></td>
<td>■ See “Configuring GAB manually” on page 207.</td>
</tr>
<tr>
<td>Configure VCS.</td>
<td>See “Configuring VCS manually” on page 207.</td>
</tr>
<tr>
<td>Start LLT, GAB, and VCS services.</td>
<td>See “Starting LLT, GAB, and VCS after manual configuration” on page 209.</td>
</tr>
<tr>
<td>Modify the VCS configuration.</td>
<td>See “Modifying the VCS configuration” on page 211.</td>
</tr>
<tr>
<td>Replace demo license with a permanent license.</td>
<td>See “Replacing a VCS demo license with a permanent license for manual installations” on page 201.</td>
</tr>
</tbody>
</table>

Viewing the list of VCS RPMs

During the VCS installation, the installer prompts you with an option to choose the VCS RPMs to install. You can view the list of RPMs that each of these options would install using the installer command-line option.

Manual installation or upgrade of the product requires you to install the RPMs in a specified order. For example, you must install some RPMs before other RPMs because of various product dependencies. The following installer command options list the RPMs in the order in which you must install these RPMs.

Table 14-2 describes the VCS RPM installation options and the corresponding command to view the list of RPMs.

Table 14-2 Installer command options to view VCS RPMs

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Command option to view the list of RPMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Installs only the minimal required VCS RPMs that provide basic functionality of the product.</td>
<td>installvcs -minpkgs</td>
</tr>
<tr>
<td>2</td>
<td>Installs the recommended VCS RPMs that provide complete functionality of the product. This option does not install the optional VCS RPMs.</td>
<td>installvcs -recpkgs</td>
</tr>
<tr>
<td>3</td>
<td>Installs all the VCS RPMs. You must choose this option to configure any optional VCS feature.</td>
<td>installvcs -allpkgs</td>
</tr>
</tbody>
</table>
To view the list of VCS RPMs

1. Navigate to the directory where you can start the installvcs program.
   
   ```
   # cd cluster_server
   ```

2. Run the following command to view the list of RPMs. Based on what RPMs you want to install, enter the appropriate command option:
   
   ```
   # ./installvcs -minpkgs
   ```
   
   Or
   
   ```
   # ./installvcs -recpkgs
   ```
   
   Or
   
   ```
   # ./installvcs -allpkgs
   ```

Installing VCS RPMs for a manual installation

All RPMs are installed into the `/opt` directory and a few files are installed into the `/etc` and `/var` directories.

You can create lists of the RPMs to install.

See “Viewing the list of VCS RPMs” on page 196.

If you copied the packages to `/tmp/install`, navigate to the directory and perform the following on each system:

To install VCS RPMs on a node

- Install the RPMs in the order shown. Do not install any RPMs already installed on the system. Pay special attention to operating system distribution and architecture.

  - RHEL5:
    
    ```
    # VRTSperl-5.14.2.6-RHEL5.2.x86_64.rpm
    # VRTSvlic-3.02.61.004-0.x86_64.rpm
    # VRTSapt-6.0.100.000-GA.noarch.rpm
    # VRTS11t-6.0.100.000-GA_RHEL5.x86_64.rpm
    # VRTSgab-6.0.100.000-GA_RHEL5.x86_64.rpm
    # VRTSvxfen-6.0.100.000-GA_RHEL5.x86_64.rpm
    # VRTSamf-6.0.100.000-GA_RHEL5.x86_64.rpm
    # VRTScps-6.0.100.000-GA_RHEL5.i686.rpm
    ```
Manually installing VCS
Installing VCS software manually

# RHEL6:
# VRTSvcsag-6.0.200.000-GA_RHEL5.i686.rpm
# VRTSvcsdr-6.0.100.000-GA_RHEL5.x86_64.rpm
# VRTSvcsea-6.0.100.000-GA_RHEL5.i686.rpm
# VRTSvcsvmw-6.0.200.000-GA_RHEL5.i686.rpm
# VRTSsfmh-5.0.196.0_Linux.rpm
# VRTSvbs-6.0.100.000-GA_RHEL5.i686.rpm
# VRTSsfcpi602-6.0.200.000-GA_GENERIC.noarch.rpm

# SLES10:
# VRTSperl-5.14.2.6-SLES10.i586.rpm
# VRTSvlic-3.02.61.004-0.x86_64.rpm
# VRTSspt-6.0.100.000-GA.noarch.rpm
# VRTSllt-6.0.100.000-GA_SLES10.x86_64.rpm
# VRTSgab-6.0.100.000-GA_SLES10.x86_64.rpm
# VRTSvxfen-6.0.100.000-GA_SLES10.x86_64.rpm
# VRTSsamf-6.0.100.000-GA_SLES10.x86_64.rpm
# VRTSvcs-6.0.100.000-GA_SLES10.i586.rpm
# VRTSscps-6.0.100.000-GA_SLES10.i586.rpm
# VRTSvcsag-6.0.200.000-GA_SLES10.i586.rpm
# VRTSvcsdr-6.0.100.000-GA_SLES10.x86_64.rpm
# VRTSvcsea-6.0.100.000-GA_SLES10.i586.rpm
# VRTSvcsvmw-6.0.200.000-GA_SLES10.i586.rpm
Adding a license key for a manual installation

You can either add the VCS license keys or use keyless licensing for VCS.

See “Setting or changing the product level for keyless licensing” on page 199.

After you have installed all RPMs on each cluster node, use the `vxlicinst` command to add the VCS license key on each system:

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

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 /optVRTSvlic/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.

**Checking licensing information on the system for a manual installation**

Use the `vxlicrep` utility to display information about all Veritas licenses on a system. For example, enter:

```
# vxlicrep
```

From the output, you can determine the following:

- The license key
- The type of license
- The product for which it applies
- Its expiration date, if one exists

Demo keys have expiration dates, while permanent keys and site keys do not.

**Replacing a VCS demo license with a permanent license for manual installations**

When a VCS demo key license expires, you can replace it with a permanent license using the `vxlicinst` program.

See “Checking licensing information on the system” on page 137.

**Copying the installation guide to each node**

After you install VCS, Symantec recommends that you copy the PDF version of this guide from the installation disc to the `/optVRTS/docs` directory on each node to make it available for reference. The PDF is located at `cluster_server/docs/vcs_install_version_platform.pdf`, where `version` is the release version and `platform` is the name of the operating system.
Manually installing VCS

Installing VCS software manually
Manually configuring VCS

This chapter includes the following topics:

- About configuring VCS manually
- Configuring LLT manually
- Configuring GAB manually
- Configuring VCS manually
- Configuring VCS in single node mode
- Starting LLT, GAB, and VCS after manual configuration
- Modifying the VCS configuration

About configuring VCS manually

This section describes the procedures to manually configure VCS.

Note: For manually configuring VCS in single node mode, you can skip steps about configuring LLT manually and configuring GAB manually.

Configuring LLT manually

VCS uses the Low Latency Transport (LLT) protocol for all cluster communications as a high-performance, low-latency replacement for the IP stack. LLT has two major functions.

It handles the following tasks:

- Traffic distribution
Heartbeat traffic

To configure LLT over Ethernet, perform the following steps on each node in the cluster:

- Set up the file `/etc/llthosts`.
  See “Setting up `/etc/llthosts` for a manual installation” on page 204.

- Set up the file `/etc/llttab`.
  See “Setting up `/etc/llttab` for a manual installation” on page 204.

- Edit the following file on each node in the cluster to change the values of the `LLT_START` and the `LLT_STOP` environment variables to 1:
  `/etc/sysconfig/llt`

You can also configure LLT over UDP.
See “Using the UDP layer for LLT” on page 393.

### Setting up `/etc/llthosts` for a manual installation

The file `llthosts(4)` is a database. It contains one entry per system that links the LLT system ID (in the first column) with the LLT host name. You must ensure that contents of this file are identical on all the nodes in the cluster. A mismatch of the contents of the file can cause indeterminate behavior in the cluster.

Use `vi` or another editor, to create the file `/etc/llthosts` that contains the entries that resemble:

```
0 sys1
1 sys2
```

### Setting up `/etc/llttab` for a manual installation

The `/etc/llttab` file must specify the system’s ID number (or its node name), its cluster ID, and the network links that correspond to the system. In addition, the file can contain other directives. Refer also to the sample `llttab` file in `/opt/VRTSllt`.

See “About LLT directives in `/etc/llttab` file” on page 205.

Use `vi` or another editor to create the file `/etc/llttab` that contains the entries that resemble:

```
set-node node name
set-cluster cluster_id
link eth1 eth-MAC_address - ether - -
link eth2 eth-MAC_address - ether - -
```
The first line must identify the system where the file exists. In the example, the value for `set-node` can be: `sys1` or `0`. The next line, beginning with the `set-cluster` command, identifies the cluster number, which must be a unique number when more than one cluster is configured on the same physical network connection.

The next two lines, beginning with the `link` command, identify the two private network cards that the LLT protocol uses. The order of directives must be the same as in the sample `llttab` file in `/opt/VRTSllt`.

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. For example:

Use `vi` or another editor to create the file `/etc/llttab` that contains the entries that resemble:

```bash
set-node node name
set-cluster cluster_id
link eth1 eth-MAC_address - ether - -
link eth2 eth-MAC_address - ether - -
link-lowpri eth3 eth-MAC_address - ether - -
```

### About LLT directives in `/etc/llttab` file

*Table 15-1* lists the LLT directives in `/etc/llttab` file for LLT over Ethernet.

<table>
<thead>
<tr>
<th>Directive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set-node</code></td>
<td>Assigns the system ID or symbolic name. The system ID number must be unique for each system in the cluster, and must be in the range 0-63. The symbolic name corresponds to the system ID, which is in <code>/etc/llthosts</code> file. Note that LLT fails to operate if any systems share the same ID.</td>
</tr>
</tbody>
</table>
Table 15-1  LLT directives (continued)

<table>
<thead>
<tr>
<th>Directive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>link</td>
<td>Attaches LLT to a network interface. At least one link is required, and up to eight are supported. LLT distributes network traffic evenly across all available network connections unless you mark the link as low-priority using the link-lowpri directive or you configured LLT to use destination-based load balancing. The first argument to link is a user-defined tag shown in the lltstat(1M) output to identify the link. It may also be used in llttab to set optional static MAC addresses. The second argument to link specifies the network interface to use. For bonds or vlan interfaces, use the interface name. For standard network interfaces, Symantec recommends the usage of eth-mac to specify the corresponding network interface. The remaining four arguments to link are defaults; these arguments should be modified only in advanced configurations. There should be one link directive for each network interface. LLT uses an unregistered Ethernet SAP of 0xCAFE. If the SAP is unacceptable, refer to the llttab(4) manual page for information on how to customize SAP. Note that IP addresses do not need to be assigned to the network device; LLT does not use IP addresses.</td>
</tr>
<tr>
<td>set-cluster</td>
<td>Assigns a unique cluster number. Use this directive when more than one cluster is configured on the same physical network connection. LLT uses a default cluster number of zero.</td>
</tr>
<tr>
<td>link-lowpri</td>
<td>Use this directive in place of link for public network interfaces. This directive prevents VCS communication on the public network until the network is the last link, and reduces the rate of heartbeat broadcasts. If you use private NICs with different speed, use &quot;link-lowpri&quot; directive in place of &quot;link&quot; for all links with lower speed. Use the &quot;link&quot; directive only for the private NIC with higher speed to enhance LLT performance. LLT uses low-priority network links for VCS communication only when other links fail.</td>
</tr>
</tbody>
</table>

For more information about the LLT directives, refer to the llttab(4) manual page.
Additional considerations for LLT for a manual installation

You must attach each network interface that is configured for LLT to a separate and distinct physical network.

Configuring GAB manually

VCS uses the Group Membership Services/Atomic Broadcast (GAB) protocol for cluster membership and reliable cluster communications. GAB has two major functions.

It handles the following tasks:
- Cluster membership
- Cluster communications

To configure GAB

1. Set up an /etc/gabtab configuration file on each node in the cluster using vi or another editor. The following example shows an /etc/gabtab file:

```
/sbin/gabconfig -c -nN
```

   Where the `-c` option configures the driver for use. The `-nN` option specifies that the cluster is not formed until at least N systems are ready to form the cluster. Symantec recommends that you set N to be the total number of systems in the cluster.

   **Warning:** Symantec does not recommend the use of the `-c -x` option or `-x` option for `/sbin/gabconfig`. Using `-c -x` or `-x` can lead to a split-brain condition.

2. Edit the following file on each node in the cluster to change the values of the GAB_START and the GAB_STOP environment variables to 1:

```
/etc/sysconfig/gab
```

Configuring VCS manually

VCS configuration requires the types.cf and main.cf files on each system in the cluster. Both of the files are in the `/etc/VRTSvcs/conf/config` directory.
main.cf file  The main.cf configuration file requires the following minimum essential elements:

- An "include" statement that specifies the file, types.cf, which defines the VCS bundled agent resource type definitions.
- The name of the cluster.
- The name of the systems that make up the cluster.

types.cf file  Note that the "include" statement in main.cf refers to the types.cf file. This text file describes the VCS bundled agent resource type definitions. During new installations, the types.cf file is automatically copied in to the /etc/VRTSvcs/conf/config directory.

When you manually install VCS, the file /etc/VRTSvcs/conf/config/main.cf contains only the line:

```
include "types.cf"
```

For a full description of the main.cf file, and how to edit and verify it, refer to the Veritas Cluster Server Administrator's Guide.

To configure VCS manually

1  Log on as superuser, and move to the directory that contains the configuration file:

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

2  Use vi or another text editor to edit the main.cf file, defining your cluster name and system names. Refer to the following example.

An example main.cf for a two-node cluster:

```
include "types.cf"
cluster VCSCluster2 ( )
system sys1 ( )
system sys2 ( )
```

An example main.cf for a single-node cluster:

```
include "types.cf"
cluster VCSCluster1 ( )
system sn1 ( )
```
3 Save and close the main.cf file.

4 Edit the following file on each node in the cluster to change the values of the VCS_START and the VCS_STOP environment variables to 1:

/etc/sysconfig/vcs

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.

Configuring VCS in single node mode

In addition to the steps mentioned in the manual configuration section, complete the following steps to configure VCS in single node mode.

See “Configuring VCS manually” on page 207.

To configure VCS in single node mode

- Edit the following file to change the value of the ONENODE environment variable to yes.

```
/etc/sysconfig/vcs
```

Starting LLT, GAB, and VCS after manual configuration

After you have configured LLT, GAB, and VCS, use the following procedures to start LLT, GAB, and VCS.
To start LLT

1. On each node, run the following command to start LLT:

   # /etc/init.d/llt start

   If LLT is configured correctly on each node, the console output resembles:

   Loading LLT Driver...
   Starting LLT...
   Starting LLT done.

2. On each node, run the following command to verify that LLT is running:

   # /sbin/lltconfig

   LLT is running

To start GAB

1. On each node, run the following command to start GAB:

   # /etc/init.d/gab start

   If GAB is configured correctly on each node, the console output resembles:

   GAB: Starting
   GAB: Starting Done

2. On each node, run the following command to verify that GAB is running:

   # /sbin/gabconfig -a

   GAB Port Memberships
   ---------------------------
   Port a gen a36e0003 membership 01

To start VCS

- On each node, type:

   # /etc/init.d/vcs start

   If VCS is configured correctly on each node, the console output resembles:

   VCS NOTICE V-16-1-10619 'HAD' starting on: sys1
   VCS NOTICE V-16-1-10620 Waiting for local cluster configuration status
   VCS NOTICE V-16-1-10625 Local cluster configuration valid
   VCS NOTICE V-16-1-11034 Registering for cluster membership
Modifying the VCS configuration

After the successful installation of VCS, you can modify the configuration of VCS using several methods. You can dynamically modify the configuration from the command line, Veritas Operations Manager, or the Cluster Manager (Java Console). For information on management tools, refer to the Veritas Cluster Server Administrator’s Guide.

You can also edit the main.cf file directly. For information on the structure of the main.cf file, refer to the Veritas Cluster Server Administrator’s Guide.

Configuring the ClusterService group

When you have installed VCS, and verified that LLT, GAB, and VCS work, you can create a service group to include the optional features. These features include the VCS notification components and the Global Cluster option. If you manually added VCS to your cluster systems, you must manually create the ClusterService group. You can refer to the configuration examples of a system with a ClusterService group. See the Veritas Cluster Server Administrator’s Guide for more information.

See “Sample main.cf file for VCS clusters” on page 375.
Manually configuring VCS

Modifying the VCS configuration
Manually configuring the 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 16-1 lists the tasks that are involved in setting up I/O fencing.

Table 16-1 Tasks to set up I/O fencing manually

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initializing disks as VxVM disks</td>
<td>See “Initializing disks as VxVM disks” on page 139.</td>
</tr>
<tr>
<td>Identifying disks to use as coordinator disks</td>
<td>See “Identifying disks to use as coordinator disks” on page 214.</td>
</tr>
<tr>
<td>Checking shared disks for I/O fencing</td>
<td>See “Checking shared disks for I/O fencing” on page 143.</td>
</tr>
<tr>
<td>Setting up coordinator disk groups</td>
<td>See “Setting up coordinator disk groups” on page 214.</td>
</tr>
<tr>
<td>Creating I/O fencing configuration files</td>
<td>See “Creating I/O fencing configuration files” on page 215.</td>
</tr>
</tbody>
</table>
### Tasks to set up I/O fencing manually (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifying VCS configuration to use I/O fencing</td>
<td>See “Modifying VCS configuration to use I/O fencing” on page 216.</td>
</tr>
<tr>
<td>Configuring CoordPoint agent to monitor coordination points</td>
<td>See “Configuring CoordPoint agent to monitor coordination points” on page 228.</td>
</tr>
<tr>
<td>Verifying I/O fencing configuration</td>
<td>See “Verifying I/O fencing configuration” on page 218.</td>
</tr>
</tbody>
</table>

### Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See “Initializing disks as VxVM disks” on page 139.

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 143.

### 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 sdx, sdy, and sdz.
To create the vxfencoorddg disk group

1. On any node, create the disk group by specifying the device names:
   
   ```
   # vxdg init vxfencoorddg sdx sdy sdz
   ```

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 node, 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:
Modifying VCS configuration to use I/O fencing

After you add coordination points and configure I/O fencing, add the UseFence = SCSI3 cluster attribute to the VCS configuration file /etc/VRTSvcs/conf/config/main.cf.

If you reset this attribute to UseFence = None, VCS does not make use of I/O fencing abilities while failing over service groups. However, I/O fencing needs to be disabled separately.

To modify VCS configuration to enable I/O fencing

1. Save the existing configuration:
   ```
   # haconf -dump -makero
   ```

2. Stop VCS on all nodes:
   ```
   # hastop -all
   ```

3. To ensure High Availability has stopped cleanly, run `gabconfig -a`.
   In the output of the commands, check that Port h is not present.

4. If the I/O fencing driver vxfen is already running, stop the I/O fencing driver.
   ```
   # /etc/init.d/vxfen stop
   ```
5 Make a backup copy of the main.cf file:

```bash
# 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.

```plaintext
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:

```bash
# 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:

```bash
# 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.

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

- Start VCS.

  ```bash
  # /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 16-2 Tasks to set up server-based I/O fencing manually

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparing the CP servers for use by the VCS cluster</td>
<td>See “Preparing the CP servers manually for use by the VCS cluster” on page 219.</td>
</tr>
</tbody>
</table>
Table 16-2  Tasks to set up server-based I/O fencing manually (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifying I/O fencing configuration files to configure server-based I/O fencing</td>
<td>See “Configuring server-based fencing on the VCS cluster manually” on page 222.</td>
</tr>
<tr>
<td>Modifying VCS configuration to use I/O fencing</td>
<td>See “Modifying VCS configuration to use I/O fencing” on page 216.</td>
</tr>
<tr>
<td>Configuring Coordination Point agent to monitor coordination points</td>
<td>See “Configuring CoordPoint agent to monitor coordination points” on page 228.</td>
</tr>
<tr>
<td>Verifying the server-based I/O fencing configuration</td>
<td>See “Verifying server-based I/O fencing configuration” on page 230.</td>
</tr>
</tbody>
</table>

Preparing the CP servers manually for use by the VCS cluster

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

Table 16-3 displays the sample values used in this procedure.

Table 16-3  Sample values in procedure

<table>
<thead>
<tr>
<th>CP server configuration component</th>
<th>Sample name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP server</td>
<td>cps1</td>
</tr>
<tr>
<td>Node #1 - VCS cluster</td>
<td>sys1</td>
</tr>
<tr>
<td>Node #2 - VCS cluster</td>
<td>sys2</td>
</tr>
<tr>
<td>Cluster name</td>
<td>clus1</td>
</tr>
<tr>
<td>Cluster UUID</td>
<td>{f0735332-1dd1-11b2}</td>
</tr>
</tbody>
</table>
To manually configure CP servers for use by the VCS cluster

1. Determine the cluster name and uuid on the VCS cluster.
   For example, issue the following commands on one of the VCS 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 VCS cluster and nodes are present in the CP server.
   For example:

   # cpsadm -s cps1.symantecexample.com -a list_nodes

<table>
<thead>
<tr>
<th>ClusName</th>
<th>UUID</th>
<th>Hostname(Node ID)</th>
<th>Registered</th>
</tr>
</thead>
<tbody>
<tr>
<td>clus1</td>
<td>{f0735332-1dd1-11b2-bb31-00306eea460a}</td>
<td>sys1(0)</td>
<td>0</td>
</tr>
<tr>
<td>clus1</td>
<td>{f0735332-1dd1-11b2-bb31-00306eea460a}</td>
<td>sys2(1)</td>
<td>0</td>
</tr>
</tbody>
</table>

   If the output does not show the cluster and nodes, then add them as described in the next step.

   For detailed information about the cpsadm command, see the Veritas Cluster Server Administrator's Guide.
3 Add the VCS 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_cluster
  -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):

```shell
# cpsadm -s cps1.symantecexample.com -a add_user -e\n  CPSADM@VCS_SERVICES@cluster_uuid\n  -f cps_operator -g vx
```

User CPSADM@VCS_SERVICES@cluster_uuid successfully added

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

For example, issue the following command on the CP server
(cps1.symantecexample.com) for VCS cluster clus1 with two nodes sys1 and
sys2:

```shell
# cpsadm -s cps1.symantecexample.com -a\n  add_clus_to_user -c clus1\n  -u {f0735332-1dd1-11b2}\n  -e CPSADM@VCS_SERVICES@cluster_uuid\n  -f cps_operator -g vx
```

Cluster successfully added to user

CPSADM@VCS_SERVICES@cluster_uuid privileges.

Configuring server-based fencing on the VCS cluster manually

The configuration process for the client or VCS 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 214.

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 VCS cluster manually

1 Use a text editor to edit the following file on each node in the cluster:

/etc/sysconfig/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 223.

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

   For example:

   # /etc/init.d/vxfen start

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=customized

vxfen_mechanism=cps

scsi3_disk_policy=dmp

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 16-4 defines the vxfenmode parameters that must be edited.

Table 16-4  vxfenmode file parameters

<table>
<thead>
<tr>
<th>vxfenmode File Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vxfen_mode</td>
<td>Fencing mode of operation. This parameter must be set to “customized”.</td>
</tr>
<tr>
<td>vxfen_mechanism</td>
<td>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”.</td>
</tr>
<tr>
<td>scsi3_disk_policy</td>
<td>Configure the vxfen module to use either DMP devices, &quot;dmp&quot; or the underlying raw character devices, &quot;raw&quot;. <strong>Note:</strong> The configured disk policy is applied on all the nodes.</td>
</tr>
<tr>
<td>security</td>
<td>Security parameter 1 indicates that secure mode is used for CP server communications. Security parameter 0 indicates that communication with the CP server is made in non-secure mode. The default security value is 1.</td>
</tr>
<tr>
<td>fips_mode</td>
<td>[For future use] Set the value to 0.</td>
</tr>
</tbody>
</table>
| cps1, cps2, or vx fendg  | Coordination point parameters. Enter either the virtual IP address or the FQHN (whichever is accessible) of the CP server.  
  
  \[
  \text{cps<number>}=[\text{virtual_ip_address/virtual_host_name}]:\text{port} 
  \]
  
  Where `port` is optional. The default port value is 14250. If you have configured multiple virtual IP addresses or host names over different subnets, you can specify these as comma-separated values. For example:

  \[
  \text{cps1}=[192.168.0.23],[192.168.0.24]:58888, \text{[cps1.company.com]} 
  \]

  **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 16-4 vxfenmode file parameters (continued)

<table>
<thead>
<tr>
<th>vxfenmode File Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port</strong></td>
<td>Default port for the CP server to listen on. 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.</td>
</tr>
<tr>
<td><strong>single_cp</strong></td>
<td>Value 1 for single_cp parameter indicates that the server-based fencing uses a single highly available CP server as its only coordination point. Value 0 for single_cp parameter indicates that the server-based fencing uses at least three coordination points.</td>
</tr>
</tbody>
</table>

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 VCS 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 VCS cluster using the `hares` commands. For example:

```bash
# hares -state coordpoint
```

The following is an example of the command and output:

```bash
# hares -state coordpoint
```

<table>
<thead>
<tr>
<th>Resource</th>
<th>Attribute</th>
<th>System</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>coordpoint</td>
<td>State</td>
<td>sys1</td>
<td>ONLINE</td>
</tr>
<tr>
<td>coordpoint</td>
<td>State</td>
<td>sys2</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>

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:

```bash
# 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 Cluster Server Administrator's Guide*.

2. Verify that I/O fencing is using the specified coordination points by running the `vxfenconfig` command. For example, run the following command:

```
# vxfenconfig -l
```

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

---

**Setting up non-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 218.

2. Make sure that the VCS 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 `/etc/sysconfig/vxfen` file as follows:

   ```
   vxfen_vxfrnd_tmt=25
   ```
6 On each node, edit the /etc/vxfenmode file as follows:

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

- Add the following line to the /etc/llttab file so that the changes remain persistent after any reboot:
  ```bash
  set-timer sendhbcap:3000
  ```

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

- Make the VCS configuration file writable:
  ```bash
  # 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.
  ```bash
  # hares -modify <dg_resource> MonitorReservation 0
  # hares -modify <dg_resource> Reservation "NONE"
  ```

- Run the following command to verify the value:
  ```bash
  # 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.
  ```bash
  # haattr -default DiskGroup Reservation "NONE"
  ```

- Make the VCS configuration file read-only
  ```bash
  # haconf -dump -makero
  ```
9 Make sure that the UseFence attribute in the VCS configuration file main.cf is set to SCSI3.

10 To make these VxFEN changes take effect, stop and restart VxFEN and the dependent modules
   ■ On each node, run the following command to stop VCS:
     
     # /etc/init.d/vcs stop

   ■ After VCS takes all services offline, run the following command to stop VxFEN:
     
     # /etc/init.d/vxfen stop

   ■ On each node, run the following commands to restart VxFEN and VCS:
     
     # /etc/init.d/vxfen start
     # /etc/init.d/vcs start

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
================================
Upgrading VCS

- Chapter 17. Planning to upgrade VCS
- Chapter 18. Performing a typical VCS upgrade using the installer
- Chapter 19. Performing an automated VCS upgrade using response files
Planning to upgrade VCS

This chapter includes the following topics:

- About upgrading to VCS 6.0.2
- Supported VCS upgrade paths
- Upgrading VCS in secure enterprise environments
- Considerations for upgrading secure VCS 5.x clusters to VCS 6.0.2
- Considerations for upgrading secure CP servers
- Considerations for upgrading secure CP clients
- Setting up trust relationship between CP server and CP clients manually

About upgrading to VCS 6.0.2

You can upgrade VCS using one of the following methods:

- Typical upgrade using Veritas product installer or the installvcs program
  See “Upgrading VCS using the script-based installer” on page 246.

- Automated upgrade using response files
  See “Upgrading VCS using response files” on page 249.

You can upgrade VCS 6.0.2 to Storage Foundation High Availability 6.0.2 using Veritas product installer or response files.

See the Veritas Storage Foundation and High Availability Installation Guide.

Note: When you upgrade to VCS 6.0.2, you need not reconfigure application monitoring with VCS. All existing monitoring configurations are preserved.
Supported VCS upgrade paths

Table 17-1 provides the supported scenarios for upgrading to Veritas Cluster Server 6.0.2.

<table>
<thead>
<tr>
<th>Upgrade from</th>
<th>Upgrade to</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCS 5.1</td>
<td>VCS 6.0.2</td>
</tr>
<tr>
<td>VCS 5.1SPx</td>
<td>VCS 6.0.2</td>
</tr>
<tr>
<td>VCS 5.1SP1RP1</td>
<td>VCS 6.0.2</td>
</tr>
<tr>
<td>VCS 5.1SP1RP2</td>
<td>VCS 6.0.2</td>
</tr>
<tr>
<td>VCS 5.1SP1RP3</td>
<td>VCS 6.0.2</td>
</tr>
<tr>
<td>VCS 6.0</td>
<td>VCS 6.0.2</td>
</tr>
<tr>
<td>VCS 6.0RP1</td>
<td>VCS 6.0.2</td>
</tr>
<tr>
<td>VCS 6.0.1</td>
<td>VCS 6.0.2</td>
</tr>
</tbody>
</table>

Note: Rolling upgrade is not supported in VCS 6.0.2.

Upgrading VCS in secure enterprise environments

In secure enterprise environments, ssh or rsh communication is not allowed between systems. In such cases, the installvcs program can upgrade VCS only on systems with which it can communicate (most often the local system only).
To upgrade VCS in secure enterprise environments with no rsh or ssh communication

1 Run the installvcs program on each node to upgrade the cluster to VCS 6.0.2.

   On each node, the installvcs program updates the configuration, stops the
   cluster, and then upgrades VCS on the node. The program also generates a
   cluster UUID on the node. Each node may have a different cluster UUID at
   this point.

2 Start VCS on the first node.

   # hasstart

   VCS generates the cluster UUID on this node. Run the following command
to display the cluster UUID on the local node:

   # /opt/VRTSvcs/bin/uuidconfig.pl -clus -display systemname

3 On each of the other nodes, perform the following steps:

   ■ Set the value of the VCS_HOST environment variable to the name of the
     first node.
   ■ Display the value of the CID attribute that stores the cluster UUID value:

     # haclus -value CID

   ■ Copy the output of the CID attribute to the file /etc/vx/.uuids/clusuuid.
   ■ Update the VCS_HOST environment variable to remove the set value.
   ■ Start VCS.

   The node must successfully join the already running nodes in the cluster.
   See “Verifying LLT, GAB, and cluster operation” on page 270.

Considerations for upgrading secure VCS 5.x clusters to VCS 6.0.2

When you upgrade a secure VCS 5.x cluster to VCS 6.0.2, the upgrade does not
migrate the old broker configuration to the new broker because of the change in
architecture. Both the old broker (/opt/VRTSat/bin/vxatd) and new broker
(/opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver) continue to
run. In such a scenario, you must consider the following:

■ The HA commands that you run in VCS 6.0.2 are processed by the new broker
   by default. To ensure that the HA commands are processed by the old broker,
   set the VCS_REMOTE_BROKER environment variable as follows:
Considerations for upgrading secure CP servers

When you upgrade the CP Server, trust relationships are not migrated.

If you upgrade the CP clients after you upgrade the CP server, the installer recreates the trust relationships that were established by the client. You need not establish the trust relationships manually. However, the CP server and CP clients cannot communicate with each other till trust relationships are established.

If you do not upgrade the CP clients after you upgrade the CP server, you must recreate the trust relationships between the CP server and CP clients.

Considerations for upgrading secure CP clients

Passwordless communication from CP clients to CP server must exist for the installer to reconfigure fencing and to recreate the trust relationships after the upgrade. If passwordless communication does not exist, you must reconfigure fencing manually.

See “Setting up disk-based I/O fencing manually” on page 213.

See “Setting up server-based I/O fencing manually” on page 218.

Setting up trust relationship between CP server and CP clients manually

For each client cluster, run the following command on the CP server:

```bash
# export VCS_REMOTE_BROKER=localhost IP,2821

See “About enabling LDAP authentication for clusters that run in secure mode” on page 255.

- VCS 6.0.2 does not prompt non-root users who run HA commands for passwords. In 5.x, non-root users required a password to run HA commands. If you want non-root users to enter passwords before they run HA commands, set the VCS_DOMAINTYPE environment variable to unixpwd.

- Trust relationships are not migrated during the upgrade. If you had configured secure GCO or secure steward, ensure that trust relationships are recreated between the clusters and the steward.

  See “Setting up trust relationships for your VCS cluster” on page 125.

When the old broker is not used anymore, you can delete the old VRTSat package.
EAT_DATA_DIR=/var/VRTSvcs/vcsauth/data/CPSERVER \
/opt/VRTSvcs/bin/vcsat setuptrust -b client_ip_address:14149 -s high

On each client node, run the following command:

EAT_DATA_DIR=/var/VRTSvcs/vcsauth/data/CPSADM \
/opt/VRTSvcs/bin/vcsat setuptrust -b cpserver_ip_address:14149 -s high
Planning to upgrade VCS

Setting up trust relationship between CP server and CP clients manually
Performing a typical VCS upgrade using the installer

This chapter includes the following topics:

■ Before upgrading using the script-based installer
■ Upgrading VCS using the script-based installer

Before upgrading using the script-based installer

Before you upgrade VCS, perform the following steps. You first need to remove deprecated resource types and modify changed values.

To prepare to upgrade to VCS 6.0.2

◆ Stop the application agents that are installed on the VxVM disk (for example the NBU agent).

Perform the following steps to stop the application agents:

■ Take the resources offline on all systems that you want to upgrade.

  # hares -offline resname -sys sysname

■ Stop the application agents that are installed on VxVM disk on all the systems.

  # haagent -stop agentname -sys sysname

■ Ensure that the agent processes are not running.

  # ps -ef | grep agentname
This command does not list any processes in the VxVM installation directory.

Upgrading VCS using the script-based installer

You can use the product installer to upgrade VCS.

To upgrade VCS using the product installer

1 Log in as superuser and mount the product disc.
2 Start the installer.

```
# ./installer
```

The installer starts the product installation program with a copyright message. It then specifies where it creates the logs. Note the log's directory and name.

3 From the opening Selection Menu, choose: G for "Upgrade a Product."
4 Choose 1 for Full Upgrade.
5 Enter the names of the nodes that you want to upgrade. Use spaces to separate node names. Press the Enter key to proceed.

   The installer runs some verification checks on the nodes.
6 When the verification checks are complete, the installer asks if you agree with the terms of the End User License Agreement. Press y to agree and continue.

   The installer lists the RPMs to upgrade.
7 The installer asks if you want to stop VCS processes. Press the Enter key to continue.

   The installer stops VCS processes, uninstalls RPMs, installs or upgrades RPMs, and configures VCS.

   The installer lists the nodes that Symantec recommends you restart.
8 The installer asks if you would like to send the information about this installation to Symantec to help improve installation in the future. Enter your response.

The installer displays the location of log files, summary file, and response file.

9 If you want to upgrade CP server systems that use VCS or SFHA to VCS 6.0.2, make sure that you first upgrade all application clusters to version VCS 6.0.2. Then, upgrade VCS or SFHA on the CP server systems.

For instructions to upgrade VCS or SFHA, see the *Veritas Cluster Server Installation Guide* or the *Storage Foundation and High Availability Installation Guide*.

If you are upgrading from 4.x, you may need to create new VCS accounts if you used native OS accounts.

See “Creating new VCS accounts if you used native operating system accounts” on page 367.
Performing a typical VCS upgrade using the installer

Upgrading VCS using the script-based installer
Performing an automated VCS upgrade using response files

This chapter includes the following topics:

- Upgrading VCS using response files
- Response file variables to upgrade VCS
- Sample response file for upgrading VCS

Upgrading VCS using response files

Typically, you can use the response file that the installer generates after you perform VCS upgrade on one system to upgrade VCS on other systems. You can also create a response file using the `makeresponsefile` option of the installer.

To perform automated VCS upgrade

1. Make sure the systems where you want to upgrade VCS 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 VCS.
   See “Sample response file for upgrading VCS” on page 251.
4. Edit the values of the response file variables as necessary.
   See “Response file variables to upgrade VCS” on page 250.
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

# ./installvcs<version> -responsefile /tmp/response_file
```

Where /tmp/response_file is the response file's full path name and <version> is the specific release version.

## Response file variables to upgrade VCS

Table 19-1 lists the response file variables that you can define to upgrade VCS.

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[opt][upgrade]</td>
<td>Scalar</td>
<td>Upgrades VCS RPMs. (Required)</td>
</tr>
<tr>
<td>CFG[accepteula]</td>
<td>Scalar</td>
<td>Specifies whether you agree with EULA.pdf on the media. (Required)</td>
</tr>
<tr>
<td>CFG[systems]</td>
<td>List</td>
<td>List of systems on which the product is to be upgraded. (Required)</td>
</tr>
<tr>
<td>CFG[prod]</td>
<td>Scalar</td>
<td>Defines the product to be upgraded. The value is VCS60 for VCS. (Optional)</td>
</tr>
<tr>
<td>CFG[vcs_allowcomms]</td>
<td>Scalar</td>
<td>Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)</td>
</tr>
</tbody>
</table>
### Table 19-1  
Response file variables specific to upgrading VCS (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{opt}{keyfile}</td>
<td>Scalar</td>
<td>Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)</td>
</tr>
<tr>
<td>CFG{opt}{pkgpath}</td>
<td>Scalar</td>
<td>Defines a location, typically an NFS mount, from which all remote systems can install product RPMs. The location must be accessible from all target systems. (Optional)</td>
</tr>
<tr>
<td>CFG{opt}{tmppath}</td>
<td>Scalar</td>
<td>Defines the location where a working directory is created to store temporary files and the RPMs that are needed during the install. The default location is /var/tmp. (Optional)</td>
</tr>
<tr>
<td>CFG{opt}{logpath}</td>
<td>Scalar</td>
<td>Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.</td>
</tr>
<tr>
<td>Note: The installer copies the response files and summary files also to the specified logpath location. (Optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CFG{opt}{rsh}</td>
<td>Scalar</td>
<td>Defines that rsh must be used instead of ssh as the communication method between systems. (Optional)</td>
</tr>
</tbody>
</table>

### Sample response file for upgrading VCS

Review the response file variables and their definitions.

See “Response file variables to upgrade VCS” on page 250.
Performing an automated VCS upgrade using response files

Sample response file for upgrading VCS

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

$CFG{accepteula}=1;
$CFG{vcs_allowcomms}=1;
$CFG{opt}{upgrade}=1;
$CFG{prod}="VCS601";
$CFG{systems}=[ qw( sys1 sys2) ];
1;
```
Post-installation tasks

- Chapter 20. Performing post-installation tasks
- Chapter 21. Installing or upgrading VCS components
- Chapter 22. Verifying the VCS installation
Performing post-installation tasks

This chapter includes the following topics:

- About enabling LDAP authentication for clusters that run in secure mode
- Accessing the VCS documentation
- Removing permissions for communication

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 20-1 depicts the VCS cluster communication with the LDAP servers when clusters run in secure mode.
1. When a user runs HA commands, AT initiates user authentication with the authentication broker.

2. Authentication broker on VCS node performs an LDAP bind operation with the LDAP directory.

3. Upon a successful LDAP bind, AT retrieves group information from the LDAP directory.

4. AT issues the credentials to the user to proceed with the command.

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.

```bash
# /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.

```bash
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showversion
vssat version: 6.1.12.0
```

```bash
# /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.

```bash
# /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.

```bash
# cd /home/user1
# ls
# cat .vcspwd

101 localhost mpise LDAP_SERVER ldap

# unset VCS_DOMAINTYPE
# unset VCS_DOMAIN

# /opt/VRTSvcs/bin/hasys -state

<table>
<thead>
<tr>
<th>System</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1:sysA</td>
<td>SysState</td>
<td>FAULTED</td>
</tr>
<tr>
<td>cluster1:sysB</td>
<td>SysState</td>
<td>FAULTED</td>
</tr>
<tr>
<td>cluster2:sysC</td>
<td>SysState</td>
<td>RUNNING</td>
</tr>
<tr>
<td>cluster2:sysD</td>
<td>SysState</td>
<td>RUNNING</td>
</tr>
</tbody>
</table>
```

## Accessing the VCS documentation

The software disc contains the documentation for VCS in Portable Document Format (PDF) in the `cluster_server/docs` directory. After you install VCS, Symantec recommends that you copy the PDF version of the documents to the `/opt/VRTS/docs` directory on each node to make it available for reference.

**To access the VCS documentation**

- Copy the PDF from the software disc (`cluster_server/docs/`) to the directory `/opt/VRTS/docs`.

## Removing permissions for communication

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

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

This chapter includes the following topics:

- Installing the Java Console
- Upgrading the Java Console
- Installing VCS Simulator
- Upgrading VCS Simulator
- Upgrading the VCS agents

Installing the Java Console

You can administer VCS using the VCS Java-based graphical user interface, Java Console. After VCS has been installed, install the Java Console on a Windows system or Linux system. Review the software requirements for Java Console.

The system from which you run the Java Console can be a system in the cluster or a remote workstation. A remote workstation enables each system in the cluster to be administered remotely.

Review the information about using the Java Console. For more information, refer to the *Veritas Cluster Server Administrator's Guide*.

Software requirements for the Java Console

Cluster Manager (Java Console) is supported on:

- RHEL 4 Update 3 or later, RHEL 5 or later, SLES 9 SP3, and SLES 10
- Windows XP and Windows 2003
Note: Make sure that you are using an operating system version that supports JRE 1.6.

Hardware requirements for the Java Console

The minimum hardware requirements for the Java Console follow:

- Pentium II 300 megahertz
- 256 megabytes of RAM
- 800x600 display resolution
- 8-bit color depth of the monitor
- A graphics card that is capable of 2D images

Note: Symantec recommends using Pentium III 400MHz or higher, 256MB RAM or higher, and 800x600 display resolution or higher.

The version of the Java™ 2 Runtime Environment (JRE) requires 32 megabytes of RAM.

This version is supported on the Intel Pentium platforms that run the Linux kernel v 2.2.12 and glibc v2.1.2-11 (or later).

Symantec recommends using the following hardware:

- 48 megabytes of RAM
- 16-bit color mode
- The KDE and the KWM window managers that are used with displays set to local hosts

Installing the Java Console on Linux

Review the procedure to install the Java console. Before you begin with the procedure, ensure that you have the gunzip utility installed on your system.

To install Java console on Linux

1. Download the Java GUI utility from http://go.symantec.com/vcsm_download to a temporary directory.

2. Install the RPM using rpm -i command.

   # rpm -i VCS_Cluster_Manager_Java_Console_5.5_for_Linux.rpm
Installing the Java Console on a Windows system

Review the procedure to install the Java console on a Windows system.

**To install the Java Console on a Windows system**

1. Download the Java GUI utility from [http://go.symantec.com/vcsm_download](http://go.symantec.com/vcsm_download) to a temporary directory.
2. Extract the zipped file to a temporary folder.
3. From this extracted folder, double-click setup.exe.
4. The Veritas Cluster Manager Install Wizard guides you through the installation process.

Upgrading the Java Console

Use one of the following applicable procedures to upgrade Java Console.

**To upgrade Java console on Linux**

1. Log in as superuser on the node where you intend to install the RPM.
2. Remove the GUI from the previous installation.
   ```
   # rpm -e VRTScsm
   ```
3. Install the VCS Java console.
   See “Installing the Java Console on Linux” on page 264.

**To upgrade the Java Console on a Windows client**

1. Stop Cluster Manager (Java Console) if it is running.
2. Remove Cluster Manager from the system.
   - From the Control Panel, double-click *Add/Remove Programs*.
   - Select *Veritas Cluster Manager*.
   - Click *Add/Remove*.
   - Follow the uninstall wizard instructions.
3. Install the new Cluster Manager.
   See “Installing the Java Console on a Windows system” on page 265.
Installing VCS Simulator

You can administer VCS Simulator from the Java Console or from the command line. For more information, see the Veritas Cluster Server Administrator's Guide.

Review the software requirements for VCS Simulator.

Software requirements for VCS Simulator

VCS Simulator is supported on:


Note: Make sure that you are using an operating system version that supports JRE 1.6 or later.

Installing VCS Simulator on Windows systems

This section describes the procedure to install VCS Simulator on Windows systems.

To install VCS Simulator on Windows systems

2. Extract the compressed files to another directory.
3. Navigate to the path of the Simulator installer file:
   \your_platform_architecture\cluster_server\windows\VCSWindowsInstallers\Simulator
4. Double-click the installer file.
5. Read the information in the Welcome screen and click Next.
6. In the Destination Folders dialog box, click Next to accepted the suggested installation path or click Change to choose a different location.
7. In the Ready to Install the Program dialog box, click Back to make changes to your selections or click Install to proceed with the installation.
8. In the Installshield Wizard Completed dialog box, click Finish.

Reviewing the installation

VCS Simulator installs Cluster Manager (Java Console) and Simulator binaries on the system. The Simulator installation creates the following directories:
Upgrading VCS Simulator

Use the following procedure to upgrade VCS Simulator.

To upgrade VCS Simulator on a Windows client
1. Stop all instances of VCS Simulator.
2. Stop VCS Simulator, if it is running.
3. Remove VCS Simulator from the system.
   - From the Control Panel, double-click **Add/Remove Programs**
   - Select **VCS Simulator**.
   - Click **Add/Remove**.
   - Follow the uninstall wizard instructions.
4. Install the new Simulator.

See “Installing VCS Simulator on Windows systems” on page 266.
Upgrading the VCS agents

The installvcs program does not upgrade the VCS agents for DB2, Oracle, and Sybase. If previous versions of these agents are installed on your cluster, you must uninstall the previous version of the agents and manually install the new agent version.

The Veritas Cluster Server product installer includes the VCS agents for DB2, Oracle, and Sybase as a bundled RPM.

To upgrade the VCS agents

1. Before you install, log in as the superuser. Mount the disc, and copy the files in a temporary folder for installation.

2. Use following command to install the VCS agents RPM:

   ```bash
   # rpm -ivh VRTSvcsea-6.0.100.000-GA_dist.arch.rpm
   ```

   where `dist` is the operating system and takes the values RHEL 5, RHEL 6, SLES 10, or SLES 11.

   `arch` is the architecture. It takes the values i586 or i686 for RHEL5, RHEL 6, SLES 10, and SLES11.

See the agent Installation and Configuration Guide for more information on the agent that you want to upgrade.

See *Veritas Cluster Server Release Notes* for supported versions of the agents.
Verifying the VCS installation

This chapter includes the following topics:

■ About verifying the VCS installation
■ About the cluster UUID
■ Verifying the LLT, GAB, and VCS configuration files
■ Verifying LLT, GAB, and cluster operation
■ Performing a postcheck on a node

About verifying the VCS installation

After you install and configure VCS, you can inspect the contents of the key VCS configuration files that you have installed and modified during the process. These files reflect the configuration that is based on the information you supplied. You can also run VCS commands to verify the status of LLT, GAB, and the cluster.

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/lldtab
   - 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 369.
   See “About the VCS configuration files” on page 373.

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.

   See “Setting the PATH variable” on page 66.

3. Verify LLT operation.

   See “Verifying LLT” on page 271.

4. Verify GAB operation.

   See “Verifying GAB” on page 273.

5. Verify the cluster operation.

   See “Verifying the cluster” on page 274.
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
   ```
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:

<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>Link</th>
<th>Status</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0 sys1</td>
<td>OPEN</td>
<td>eth1</td>
<td>UP</td>
<td>08:00:20:93:0E:34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eth2</td>
<td>UP</td>
<td>08:00:20:93:0E:38</td>
</tr>
<tr>
<td>1 sys2</td>
<td>OPEN</td>
<td>eth1</td>
<td>UP</td>
<td>08:00:20:8F:D1:F2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eth2</td>
<td>DOWN</td>
<td></td>
</tr>
</tbody>
</table>

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.

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:
<table>
<thead>
<tr>
<th>Port</th>
<th>Usage</th>
<th>Cookie</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>gab</td>
<td>0x0</td>
</tr>
<tr>
<td></td>
<td>opens:</td>
<td>0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63</td>
</tr>
<tr>
<td></td>
<td>connects:</td>
<td>0 1</td>
</tr>
<tr>
<td>7</td>
<td>gab</td>
<td>0x7</td>
</tr>
<tr>
<td></td>
<td>opens:</td>
<td>0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63</td>
</tr>
<tr>
<td></td>
<td>connects:</td>
<td>0 1</td>
</tr>
</tbody>
</table>
```
Verifying GAB

Verify the GAB operation using the `gabconfig -a` command. This command returns the GAB port membership information.

The ports indicate the following:

Port a  ■ Nodes have GAB communication.
          ■ `gen a36e0003` is a randomly generated number.
          ■ `membership 01` indicates that nodes 0 and 1 are connected.

Port b  ■ Indicates that the I/O fencing driver is connected to GAB port b.

Note: Port b appears in the `gabconfig` command output only if you had configured I/O fencing after you configured VCS.

          ■ `gen a23da40d` is a randomly generated number.
          ■ `membership 01` indicates that nodes 0 and 1 are connected.

Port h  ■ VCS is started.
          ■ `gen fd570002` is a randomly generated number
          ■ `membership 01` indicates that nodes 0 and 1 are both running VCS

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:

   For a cluster where I/O fencing is not configured:

   ```
   GAB Port Memberships
   __________________________________________________________
   Port a  gen a36e0003  membership 01
   Port h  gen fd570002  membership 01
   ```
For a cluster where I/O fencing is configured:

```
GAB Port Memberships
===================================
Port a gen a36e0003 membership 01
Port b gen a23da40d membership 01
Port h gen fd570002 membership 01
```

Note that port b appears in the `gabconfig` command output only if you had configured I/O fencing. You can also 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
===================================
```

- If only one network is connected, the command returns the following GAB port membership information:

```
GAB Port Memberships
===================================
Port a gen a36e0003 membership 01
Port a gen a36e0003 jeopardy ;1
Port h gen fd570002 membership 01
Port h gen fd570002 jeopardy ;1
```

Verifying the cluster

Verify the status of the cluster using the `hastatus` command. This command returns the system state and the group state.

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

Refer to the *Veritas Cluster Server Administrator’s Guide* for a description of system states and the transitions between them.
To verify the cluster

1. To verify the status of the cluster, type the following command:

   ```
   # hastatus -summary
   ```

   The output resembles:
   
   ```
   -- SYSTEM STATE
   -- System State Frozen
   A sys1 RUNNING 0
   A sys2 RUNNING 0
   
   -- GROUP STATE
   -- Group System Probed AutoDisabled State
   B ClusterService sys1 Y N ONLINE
   B ClusterService sys2 Y N OFFLINE
   ```

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.
   - The ClusterService group state
     In the sample output, the group state lists the ClusterService group, which is ONLINE on sys1 and OFFLINE on sys2.

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.
<table>
<thead>
<tr>
<th>#System</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys1</td>
<td>AgentsStopped</td>
<td>0</td>
</tr>
<tr>
<td>sys1</td>
<td>AvailableCapacity</td>
<td>100</td>
</tr>
<tr>
<td>sys1</td>
<td>CPUThresholdLevel</td>
<td>Critical 90 Warning 80 Note 70 Info 60</td>
</tr>
<tr>
<td>sys1</td>
<td>CPUUsage</td>
<td>0</td>
</tr>
<tr>
<td>sys1</td>
<td>CPUUsageMonitoring</td>
<td>Enabled 0 ActionThreshold 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ActionTimeLimit 0 Action NONE NotifyThreshold 0 NotifyTimeLimit 0</td>
</tr>
<tr>
<td>sys1</td>
<td>Capacity</td>
<td>100</td>
</tr>
<tr>
<td>sys1</td>
<td>ConfigBlockCount</td>
<td>293</td>
</tr>
<tr>
<td>sys1</td>
<td>ConfigCheckSum</td>
<td>37283</td>
</tr>
<tr>
<td>sys1</td>
<td>ConfigDiskState</td>
<td>CURRENT</td>
</tr>
<tr>
<td>sys1</td>
<td>ConfigFile</td>
<td>/etc/VRTSvcs/conf/config</td>
</tr>
<tr>
<td>sys1</td>
<td>ConfigInfoCnt</td>
<td>0</td>
</tr>
<tr>
<td>sys1</td>
<td>ConfigModDate</td>
<td>Mon Sep 03 07:14:23 CDT 2012</td>
</tr>
<tr>
<td>sys1</td>
<td>ConnectorState</td>
<td>Up</td>
</tr>
<tr>
<td>sys1</td>
<td>CurrentLimits</td>
<td></td>
</tr>
<tr>
<td>sys1</td>
<td>DiskHbStatus</td>
<td></td>
</tr>
<tr>
<td>sys1</td>
<td>DynamicLoad</td>
<td>0</td>
</tr>
<tr>
<td>sys1</td>
<td>EngineRestarted</td>
<td>0</td>
</tr>
<tr>
<td>sys1</td>
<td>EngineVersion</td>
<td>6.0.10.0</td>
</tr>
<tr>
<td>sys1</td>
<td>FencingWeight</td>
<td>0</td>
</tr>
<tr>
<td>sys1</td>
<td>Frozen</td>
<td>0</td>
</tr>
<tr>
<td>sys1</td>
<td>GUIIPAddr</td>
<td></td>
</tr>
<tr>
<td>sys1</td>
<td>HostUtilization</td>
<td>CPU 0 Swap 0</td>
</tr>
<tr>
<td>sys1</td>
<td>LLTNodeId</td>
<td>0</td>
</tr>
</tbody>
</table>
Verifying the VCS installation
Verifying LLT, GAB, and cluster operation

sys1  LicenseType PERMANENT_SITE
sys1  Limits
sys1  LinkHbStatus eth1 UP eth2 UP
sys1  LoadTimeCounter 0
sys1  LoadTimeThreshold 600
sys1  LoadWarningLevel 80
sys1  NoAutoDisable 0
sys1  NodeId 0
sys1  OnGrpCnt 7
sys1  PhysicalServer
sys1  ShutdownTimeout 600
sys1  SourceFile ./main.cf
sys1  SwapThresholdLevel Critical 90 Warning 80 Note 70 Info 60
sys1  SysInfo Linux:sys1,#1 SMP Fri Jul 8 17:36:59 EDT 2011,2.6.18-274.el5,x86_64
sys1  SysName sys1
sys1  SysState RUNNING
sys1  SystemLocation
sys1  SystemOwner
sys1  SystemRecipients
sys1  TFrozen 0
sys1  TRSE 0
sys1  UpDownState Up
sys1  UserInt 0
sys1  UserStr
### 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 278.

**To run the postcheck command on a node**

1. Run the installer with the `-postcheck` option.
   
   ```bash
   # ./installer -postcheck system_name
   ```

2. Review the output for installation-related information.

### 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 llttab(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 RPMs are installed.
- The versions of the required RPMs are correct.
- There are no verification issues for the required RPMs.

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 278.
Adding and removing cluster nodes

- Chapter 23. Adding a node to a single-node cluster
- Chapter 24. Adding a node to a multi-node VCS cluster
- Chapter 25. Removing a node from a VCS cluster
Adding a node to a single-node cluster

This chapter includes the following topics:
- Adding a node to a single-node cluster

Adding a node to a single-node cluster

All nodes in the new cluster must run the same version of VCS. The example procedure refers to the existing single-node VCS node as Node A. The node that is to join Node A to form a multiple-node cluster is Node B.

Table 23-1 specifies the activities that you need to perform to add nodes to a single-node cluster.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up Node B to be compatible with Node A.</td>
<td>See “Setting up a node to join the single-node cluster” on page 284.</td>
</tr>
<tr>
<td>- Add Ethernet cards for private heartbeat network for Node B.</td>
<td>See “Installing and configuring Ethernet cards for private network” on page 285.</td>
</tr>
<tr>
<td>- If necessary, add Ethernet cards for private heartbeat network for Node A.</td>
<td></td>
</tr>
<tr>
<td>- Make the Ethernet cable connections between the two nodes.</td>
<td></td>
</tr>
<tr>
<td>Connect both nodes to shared storage.</td>
<td>See “Configuring the shared storage” on page 286.</td>
</tr>
</tbody>
</table>
### Table 23-1  Tasks to add a node to a single-node cluster (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Bring up VCS on Node A.</td>
<td>See &quot;Bringing up the existing node&quot; on page 286.</td>
</tr>
<tr>
<td>■ Edit the configuration file.</td>
<td></td>
</tr>
<tr>
<td>If necessary, install VCS on Node B and add a license key.</td>
<td>See &quot;Installing the VCS software manually when adding a node to a single node cluster&quot; on page 287.</td>
</tr>
<tr>
<td>Make sure Node B is running the same version of VCS as the version on Node A.</td>
<td></td>
</tr>
<tr>
<td>Edit the configuration files on Node B.</td>
<td>See “About the VCS configuration files” on page 373.</td>
</tr>
<tr>
<td>Start LLT and GAB on Node B.</td>
<td>See &quot;Starting LLT and GAB” on page 287.</td>
</tr>
<tr>
<td>■ Start LLT and GAB on Node A.</td>
<td>See “Reconfiguring VCS on the existing node” on page 288.</td>
</tr>
<tr>
<td>■ Copy UUID from Node A to Node B.</td>
<td></td>
</tr>
<tr>
<td>■ Restart VCS on Node A.</td>
<td></td>
</tr>
<tr>
<td>■ Modify service groups for two nodes.</td>
<td></td>
</tr>
<tr>
<td>■ Start VCS on Node B.</td>
<td>See “Verifying configuration on both nodes” on page 289.</td>
</tr>
<tr>
<td>■ Verify the two-node cluster.</td>
<td></td>
</tr>
</tbody>
</table>

### Setting up a node to join the single-node cluster

The new node to join the existing single node that runs VCS must run the same operating system.

**To set up a node to join the single-node cluster**

1. Do one of the following tasks:
   - If VCS is not currently running on Node B, proceed to step 2.
   - If the node you plan to add as Node B is currently part of an existing cluster, remove the node from the cluster. After you remove the node from the cluster, remove the VCS RPMs and configuration files. See “Removing a node from a VCS cluster” on page 307.
   - If the node you plan to add as Node B is also currently a single VCS node, uninstall VCS. See “Uninstalling VCS using the script-based installer” on page 319.
   - If you renamed the LLT and GAB startup files, remove them.
2 If necessary, install VxVM and VxFS.

See “Installing VxVM or VxFS if necessary” on page 285.

Installing VxVM or VxFS if necessary

If you have either VxVM or VxFS with the cluster option installed on the existing node, install the same version on the new node.

Refer to the appropriate documentation for VxVM and VxFS to verify the versions of the installed products. Make sure the same version runs on all nodes where you want to use shared storage.

Installing and configuring Ethernet cards for private network

Both nodes require Ethernet cards (NICs) that enable the private network. If both Node A and Node B have Ethernet cards installed, you can ignore this step.

For high availability, use two separate NICs on each node. The two NICs provide redundancy for heartbeating.

See “Setting up the private network” on page 60.

To install and configure Ethernet cards for private network

1 Shut down VCS on Node A.

   # hastop -local

2 Shut down the node to get to the OK prompt:

   # shutdown -r now

3 Install the Ethernet card on Node A.

   If you want to use aggregated interface to set up private network, configure aggregated interface.

4 Install the Ethernet card on Node B.

   If you want to use aggregated interface to set up private network, configure aggregated interface.

5 Configure the Ethernet card on both nodes.

6 Make the two Ethernet cable connections from Node A to Node B for the private networks.

7 Restart the nodes.
Configuring the shared storage

Make the connection to shared storage from Node B. Configure VxVM on Node B and reboot the node when you are prompted.

See “Setting up shared storage” on page 63.

See “Setting up shared storage: Fibre Channel” on page 65.

Bringing up the existing node

Bring up the node.

To bring up the node

1. Restart Node A.
2. Log in as superuser.
3. Make the VCS configuration writable.

```bash
# haconf -makerw
```
4. Display the service groups currently configured.

```bash
# hagrp -list
```
5. Freeze the service groups.

```bash
# hagrp -freeze group -persistent
```
Repeat this command for each service group in step 4.

6. Make the configuration read-only.

```bash
# haconf -dump -makero
```
7. Stop VCS on Node A.

```bash
# hastop -local -force
```
8 Edit the VCS system configuration file /etc/sysconfig/vcs as follows:
   Change the line:
   
   ONENODE=yes
   
   To:
   
   ONENODE=no

9 Enable the GAB and LLT startup files so they can be used.

   # mv /etc/init.d/gab.old /etc/init.d/gab
   # mv /etc/init.d/llt.old /etc/init.d/llt

Installing the VCS software manually when adding a node to a single node cluster

Install the VCS 6.0.2 RPMs manually and install the license key.
Refer to the following sections:
■ See “Preparing for a manual installation” on page 193.
■ See “Adding a license key for a manual installation” on page 199.

Creating configuration files

Create the configuration files for your cluster.

To create the configuration files
1 Create the file /etc/llttab for a two-node cluster
   See “Setting up /etc/llttab for a manual installation” on page 204.
2 Create the file /etc/llthosts that list both the nodes.
   See “Setting up /etc/llthosts for a manual installation” on page 204.
3 Create the file /etc/gabtab.
   See “Configuring GAB manually” on page 207.

Starting LLT and GAB

On the new node, start LLT and GAB.
To start LLT and GAB

1. Start LLT on Node B.
   
   ```bash
   # /etc/init.d/llt start
   ```

2. Start GAB on Node B.
   
   ```bash
   # /etc/init.d/gab start
   ```

Reconfiguring VCS on the existing node

Reconfigure VCS on the existing nodes.

To reconfigure VCS on existing nodes

1. On Node A, create the files `/etc/llttab, /etc/llthosts, and /etc/gabtab`. Use the files that are created on Node B as a guide, customizing the `/etc/llttab` for Node A.

2. Start LLT on Node A.
   
   ```bash
   # /etc/init.d/llt start
   ```

3. Start GAB on Node A.
   
   ```bash
   # /etc/init.d/gab start
   ```

4. Check the membership of the cluster.
   
   ```bash
   # gabconfig -a
   ```

5. Copy the cluster UUID from the existing node to the new node:
   
   ```bash
   # /opt/VRTSvcs/bin/uuidconfig.pl -clus -copy -from_sys node_name_in_running_cluster -to_sys new_sys1 ... new_sysn
   ```
   
   Where you are copying the cluster UUID from a node in the cluster (*node_name_in_running_cluster*) to systems from *new_sys1* through *new_sysn* that you want to join the cluster.

6. Start VCS on Node A.
   
   ```bash
   # hastart
   ```

7. Make the VCS configuration writable.
   
   ```bash
   # haconf -makerw
   ```
8  Add Node B to the cluster.
   # hasys -add sysB

9  Add Node B to the system list of each service group.
   ■ List the service groups.
      # hagrp -list
   ■ For each service group that is listed, add the node.
      # hagrp -modify group SystemList -add sysB 1

Verifying configuration on both nodes
   Verify the configuration for the nodes.
   To verify the nodes' configuration
   1  On Node B, check the cluster membership.
      # gabconfig -a
   2  Start the VCS on Node B.
      # hastart
   3  Verify that VCS is up on both nodes.
      # hastatus
   4  List the service groups.
      # hagrp -list
   5  Unfreeze the service groups.
      # hagrp -unfreeze group -persistent
   6  Implement the new two-node configuration.
      # haconf -dump -makero
Adding a node to a single-node cluster

Adding a node to a single-node cluster
Adding a node to a multi-node VCS cluster

This chapter includes the following topics:

- Adding nodes using the VCS installer
- Manually adding a node to a cluster

Adding nodes using the VCS installer

The VCS installer performs the following tasks:

- Verifies that the node and the existing cluster meet communication requirements.
- Verifies the products and RPMs installed on the new node.
- Discovers the network interfaces on the new node and checks the interface settings.
- Creates the following files on the new node:
  /etc/llttab
  /etc/VRTSvcs/conf/sysname
- Updates the following configuration files and copies them on the new node:
  /etc/llthosts
  /etc/gabtab
  /etc/VRTSvcs/conf/config/main.cf
- Copies the following files from the existing cluster to the new node:
  /etc/vxffenmode
  /etc/vxffendg
  /etc/vx/.uuids/clusuuuid
/etc/sysconfig/llt
/etc/sysconfig/gab
/etc/sysconfig/vxfen

- Configures disk-based or server-based fencing depending on the fencing mode in use on the existing cluster.

At the end of the process, the new node joins the VCS 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 VCS cluster using the VCS installer**

1. Log in as the root user on one of the nodes of the existing cluster.
2. Run the VCS installer with the `-addnode` option.

```
# cd /opt/VRTS/install

# ./installvcs<version> -addnode
```

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

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 VCS cluster. The installer uses the node information to identify the existing cluster.

```
Enter a node name in the VCS cluster to which you want to add a node: galaxy
```

4. Review and confirm the cluster information.

5. Enter the name of the systems that you want to add as new nodes to the cluster.

```
Enter the system names separated by spaces to add to the cluster: saturn
```

The installer checks the installed products and RPMs 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 LLT configuration for the new node must be the same as that of the existing cluster. If your existing cluster uses LLT over UDP, the installer asks questions related to LLT over UDP for the new node.

See “Configuring private heartbeat links” on page 118.

Enter the NIC for the first private heartbeat link on saturn: `eth1`

7 Enter y to configure a second private heartbeat link.

**Note:** At least two private heartbeat links must be configured for high availability of the cluster.

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

8 Enter the name of the network interface that you want to configure as the second private heartbeat link.

Enter the NIC for the second private heartbeat link on saturn: `[b,q,?]` `eth2`

9 Depending on the number of LLT links configured in the existing cluster, configure additional private heartbeat links for the new node.

The installer verifies the network interface settings and displays the information.

10 Review and confirm the information.

11 If you have configured SMTP, SNMP, or the global cluster option in the existing cluster, you are prompted for the NIC information for the new node.

Enter the NIC for VCS to use on saturn: `eth3`

---

**Manually adding a node to a cluster**

The system you add to the cluster must meet the hardware and software requirements.
See “Hardware requirements for VCS” on page 34.

**Table 24-1** specifies the tasks that are involved in adding a cluster. The example demonstrates how to add a node saturn to already existing nodes, galaxy and nebula.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the hardware.</td>
<td>See “Setting up the hardware” on page 294.</td>
</tr>
<tr>
<td>Install the software manually.</td>
<td>See “Preparing for a manual installation” on page 193.</td>
</tr>
<tr>
<td>Add a license key.</td>
<td>See “Adding a license key for a manual installation” on page 199.</td>
</tr>
<tr>
<td>Configure LLT and GAB.</td>
<td>See “Configuring LLT and GAB when adding a node to the cluster” on page 299.</td>
</tr>
<tr>
<td>Copy the UUID.</td>
<td>See “Reconfiguring VCS on the existing node” on page 288.</td>
</tr>
<tr>
<td>If the existing cluster is configured for I/O fencing,</td>
<td>See “Configuring I/O fencing on the new node” on page 302.</td>
</tr>
<tr>
<td>configure I/O fencing on the new node.</td>
<td></td>
</tr>
<tr>
<td>Add the node to the existing cluster.</td>
<td>See “Adding the node to the existing cluster” on page 305.</td>
</tr>
<tr>
<td>Start VCS and verify the cluster.</td>
<td>See “Starting VCS and verifying the cluster” on page 306.</td>
</tr>
</tbody>
</table>

**Setting up the hardware**

**Figure 24-1** shows that before you configure a new system on an existing cluster, you must physically add the system to the cluster.
To set up the hardware

1. Connect the VCS private Ethernet controllers.

   Perform the following tasks as necessary:
   - When you add nodes to a two-node 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 24-1 illustrates a new node being added to an existing two-node cluster using two independent hubs.

2. Connect the system to the shared storage, if required.

Installing the VCS software manually when adding a node

Install the VCS 6.0.2 RPMs manually and add a license key.

For more information, see the following:
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.

See “Configuring LLT and GAB when adding a node to the cluster” on page 299.

Table 24-2 uses the following information for the following command examples.

Table 24-2  The command examples definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>Fully-qualified host name (FQHN)</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys5</td>
<td>sys5.nodes.example.com</td>
<td>The new node that you are adding to the cluster.</td>
</tr>
</tbody>
</table>
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 \ 
    /VRTSvlocal.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
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
```

Create the `/etc/VRTSvcs/conf/config/.secure` file:

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

### Configuring LLT and GAB when adding a node to the cluster

Create the LLT and GAB configuration files on the new node and update the files on the existing nodes.

**To configure LLT when adding a node to the cluster**

1. Create the file `/etc/llthosts` on the new node. You must also update it on each of the current nodes in the cluster.

   For example, suppose you add saturn to a cluster consisting of galaxy and nebulan:
   - If the file on one of the existing nodes resembles:

   ```
   0 sys1
   1 sys2
   ```
   - Update the file for all nodes, including the new one, resembling:
Adding a node to a multi-node VCS cluster

Manually adding a node to a cluster

2 Create the file `/etc/llttab` on the new node, making sure that line beginning "set-node" specifies the new node.

The file `/etc/llttab` on an existing node can serve as a guide.

The following example describes a system where node `saturn` is the new node on cluster ID number 2:

```
set-node saturn
set-cluster 2
link eth1 eth-00:04:23:AC:12:C4 - ether - -
link eth2 eth-00:04:23:AC:12:C5 - ether - -
```

3 Copy the following file from one of the nodes in the existing cluster to the new node:

```
/etc/sysconfig/llt
```

4 On the new system, run the command:

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

In a setup that uses LLT over UDP, new nodes automatically join the existing cluster if the new nodes and all the existing nodes in the cluster are not separated by a router. However, if you use LLT over UDP6 link with IPv6 address and if the new node and the existing nodes are separated by a router, then do the following:

- Edit the `/etc/llttab` file on each node to reflect the link information about the new node.

- Specify the IPv6 address for UDP link of the new node to all existing nodes. Run the following command on each existing node for each UDP link:

```
# /sbin/lltconfig -a set systemid device_tag address
```

To configure GAB when adding a node to the cluster

1 Create the file `/etc/gabtab` on the new system.

- If the `/etc/gabtab` file on the existing nodes resembles:

```
/sbin/gabconfig -c
```
The file on the new node should be the same. Symantec recommends that you use the 
\(-c \ -n N\) option, where \(N\) is the total number of cluster nodes.

- If the \(/etc/gabtab\) file on the existing nodes resembles:

```
/sbin/gabconfig -c -n2
```

The file on all nodes, including the new node, should change to reflect the change in the number of cluster nodes. For example, the new file on each node should resemble:

```
/sbin/gabconfig -c -n3
```

The 
\(-n\)
flag indicates to VCS the number of nodes that must be ready to form a cluster before VCS starts.

2 Copy the following file from one of the nodes in the existing cluster to the new node:

```
/etc/sysconfig/gab
```

3 On the new node, to configure GAB run the command:

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

To verify GAB

1 On the new node, run the command:

```
# /sbin/gabconfig -a
```

The output should indicate that port a membership shows all nodes including the new node. The output should resemble:

```
GAB Port Memberships
====================================
Port a gen a3640003 membership 012
```

See “Verifying GAB” on page 273.

2 Run the same command on the other nodes (galaxy and nebula) to verify that the port a membership includes the new node:

```
# /sbin/gabconfig -a
GAB Port Memberships
====================================
Port a gen a3640003 membership 012
Port h gen fd570002 membership 01
Port h gen fd570002 visible ; 2
```
Configuring I/O fencing on the new node

If the existing cluster is configured for I/O fencing, perform the following tasks on the new node:

- Prepare to configure I/O fencing on the new node.
  See “Preparing to configure I/O fencing on the new node” on page 302.

- If the existing cluster runs server-based fencing, configure server-based fencing on the new node.
  See “Configuring server-based fencing on the new node” on page 303.
  If the existing cluster runs disk-based fencing, you need not perform any additional step. Skip to the next task. After you copy the I/O fencing files and start I/O fencing, disk-based fencing automatically comes up.

- Copy the I/O fencing files from an existing node to the new node and start I/O fencing on the new node.
  See “Starting I/O fencing on the new node” on page 304.

If the existing cluster is not configured for I/O fencing, perform the procedure to add the new node to the existing cluster.
See “Adding the node to the existing cluster” on page 305.

Preparing to configure I/O fencing on the new node

Perform the following tasks before you configure and start I/O fencing on the new node.

To prepare to configure I/O fencing on the new node

1. Determine whether the existing cluster runs disk-based or server-based fencing mechanism. On one of the nodes in the existing cluster, run the following command:

   ```bash
   # vxfenadm -d
   ```

   If the fencing mode in the output is SCSI3, then the cluster uses disk-based fencing.

   If the fencing mode in the output is CUSTOMIZED, then the cluster uses server-based fencing.

2. In the following cases, install and configure Veritas Volume Manager (VxVM) on the new node.

   - The existing cluster uses disk-based fencing.
   - The existing cluster uses server-based fencing with at least one coordinator disk.
You need not perform this step if the existing cluster uses server-based fencing with all coordination points as CP servers.

See the *Veritas Storage Foundation and High Availability Installation Guide* for installation instructions.

**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 VCS 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 VCS cluster:

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

Starting I/O fencing on the new node

Copy the I/O fencing files from an existing node to the new node and start I/O fencing on the new node. This task starts I/O fencing based on the fencing mechanism that is configured in the existing cluster.

To start I/O fencing on the new node

1. Copy the following I/O fencing configuration files from one of the nodes in the existing cluster to the new node:
Adding a node to a multi-node VCS cluster

Manually adding a node to a cluster

Adding the node to the existing cluster

Perform the tasks on one of the existing nodes in the cluster.

To add the new node to the existing cluster

1. Copy the cluster UUID from the one of the nodes in the existing cluster to the new node:

   ```
   # /opt/VRTSvcs/bin/uuidconfig.pl -clus -copy -from_sys node_name_in_running_cluster -to_sys new_sys1 ... new_sysn
   ```

   Where you are copying the cluster UUID from a node in the cluster (node_name_in_running_cluster) to systems from new_sys1 through new_sysn that you want to join the cluster.

2. Copy the following file from one of the nodes in the existing cluster to the new node:

   /etc/sysconfig/vcs

3. Enter the command:

   ```
   # haconf -makerw
   ```

4. Add the new system to the cluster:

   ```
   # hasys -add saturn
   ```

5. Copy the main.cf file from an existing node to your new node:

   ```
   # rcp /etc/VRTSvcs/conf/config/main.cf \
   saturn:/etc/VRTSvcs/conf/config/
   ```
Check the VCS configuration file. No error message and a return value of zero indicates that the syntax is legal.

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

If necessary, modify any new system attributes.

Enter the command:

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

**Starting VCS and verifying the cluster**

Start VCS after adding the new node to the cluster and verify the cluster.

**To start VCS and verify the cluster**

1. Start VCS on the newly added system:

   ```
   # hastart
   ```

2. Run the GAB configuration command on each node to verify that port a and port h include the new node in the membership:

   ```
   # /sbin/gabconfig -a
   GAB Port Memberships
   ================
   Port a gen a3640003 membership 012
   Port h gen fd570002 membership 012
   ```

   If the cluster uses I/O fencing, then the GAB output also shows port b membership.
Removing a node from a VCS cluster

This chapter includes the following topics:

- Removing a node from a VCS cluster

Table 25-1 specifies the tasks that are involved in removing a node from a cluster. In the example procedure, the cluster consists of nodes sys1, sys2, and sys5; node sys5 is to leave the cluster.

Table 25-1  Tasks that are involved in removing a node

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up the configuration file.</td>
<td>See “Verifying the status of nodes and service groups” on page 308.</td>
</tr>
<tr>
<td>Check the status of the nodes and the service groups.</td>
<td></td>
</tr>
<tr>
<td>Switch or remove any VCS service groups on the node departing the cluster.</td>
<td>See “Deleting the departing node from VCS configuration” on page 309.</td>
</tr>
<tr>
<td>Delete the node from VCS configuration.</td>
<td></td>
</tr>
<tr>
<td>Modify the llthosts(4) and gatbtab(4) files to reflect the change.</td>
<td>See “Modifying configuration files on each remaining node” on page 312.</td>
</tr>
<tr>
<td>If the existing cluster is configured to use server-based I/O fencing, remove the node configuration from the CP server.</td>
<td>See “Removing the node configuration from the CP server” on page 312.</td>
</tr>
</tbody>
</table>
Table 25-1  Tasks that are involved in removing a node (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a cluster that is running in a secure mode, remove the security</td>
<td>See “Removing security credentials from the leaving node” on page 313.</td>
</tr>
<tr>
<td>credentials from the leaving node.</td>
<td></td>
</tr>
<tr>
<td>On the node departing the cluster:</td>
<td></td>
</tr>
<tr>
<td>■ Modify startup scripts for LLT, GAB, and VCS to allow reboot of</td>
<td>See “Unloading LLT and GAB and removing VCS on the departing node” on</td>
</tr>
<tr>
<td>the node without affecting the cluster.</td>
<td>page 314.</td>
</tr>
<tr>
<td>■ Unconfigure and unload the LLT and GAB utilities.</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the status of nodes and service groups

Start by issuing the following commands from one of the nodes to remain in the cluster node sys1 or node sys2 in our example.
To verify the status of the nodes and the service groups

1  Make a backup copy of the current configuration file, main.cf.

    # cp -p /etc/VRTSvcs/conf/config/main.cf
    /etc/VRTSvcs/conf/config/main.cf.goodcopy

2  Check the status of the systems and the service groups.

    # hastatus -summary

    -- SYSTEM STATE
    -- System State Frozen
    A sys1 RUNNING 0
    A sys2 RUNNING 0
    A sys5 RUNNING 0

    -- GROUP STATE
    -- Group System Probed AutoDisabled State
    B grp1 sys1 Y N ONLINE
    B grp1 sys2 Y N OFFLINE
    B grp2 sys1 Y N ONLINE
    B grp3 sys2 Y N OFFLINE
    B grp3 sys5 Y N ONLINE
    B grp4 sys5 Y N ONLINE

The example output from the hastatus command shows that nodes sys1, sys2, and sys5 are the nodes in the cluster. Also, service group grp3 is configured to run on node sys2 and node sys5, the departing node. Service group grp4 runs only on node sys5. Service groups grp1 and grp2 do not run on node sys5.

Deleting the departing node from VCS configuration

Before you remove a node from the cluster you need to identify the service groups that run on the node.

You then need to perform the following actions:

■ Remove the service groups that other service groups depend on, or
■ Switch the service groups to another node that other service groups depend on.
To remove or switch service groups from the departing node

1. Switch failover service groups from the departing node. You can switch grp3 from node sys5 to node sys2.
   ```
   # hagrp -switch grp3 -to sys2
   ```

2. Check for any dependencies involving any service groups that run on the departing node; for example, grp4 runs only on the departing node.
   ```
   # hagrp -dep
   ```

3. If the service group on the departing node requires other service groups—if it is a parent to service groups on other nodes—unlink the service groups.
   ```
   # haconf -makerw
   # hagrp -unlink grp4 grp1
   ```

These commands enable you to edit the configuration and to remove the requirement grp4 has for grp1.

4. Stop VCS on the departing node:
   ```
   # hastop -sys sys5
   ```

5. Check the status again. The state of the departing node should be EXITED. Make sure that any service group that you want to fail over is online on other nodes.

   ```
   # hastatus -summary
   ```

   --- SYSTEM STATE
   -- System State Frozen
   A sys1 RUNNING 0
   A sys2 RUNNING 0
   A sys5 EXITED 0

   --- GROUP STATE
   -- Group System Probed AutoDisabled State
   B grp1 sys1 Y N ONLINE
   B grp1 sys2 Y N OFFLINE
   B grp2 sys1 Y N ONLINE
   B grp3 sys2 Y N ONLINE
   B grp3 sys5 Y Y OFFLINE
   B grp4 sys5 Y N OFFLINE
6  Delete the departing node from the SystemList of service groups grp3 and grp4.

```bash
# haconf -makerw
# hagrp -modify grp3 SystemList -delete sys5
# hagrp -modify grp4 SystemList -delete sys5
```

**Note:** If sys5 was in the autostart list, then you need to manually add another system in the autostart list so that after reboot, the group comes online automatically.

7  For the service groups that run only on the departing node, delete the resources from the group before you delete the group.

```bash
# hagrp -resources grp4
  processx_grp4
  processy_grp4
# hares -delete processx_grp4
# hares -delete processy_grp4
```

8  Delete the service group that is configured to run on the departing node.

```bash
# hagrp -delete grp4
```

9  Check the status.

```bash
# hastatus -summary

```

```text
-- SYSTEM STATE
-- System  State  Frozen
A  sys1    RUNNING  0
A  sys2    RUNNING  0
A  sys5    EXITED  0

-- GROUP STATE
-- Group  System  Probed  AutoDisabled  State
B  grp1  sys1    Y    N    ONLINE
B  grp1  sys2    Y    N    OFFLINE
B  grp2  sys1    Y    N    ONLINE
B  grp3  sys2    Y    N    ONLINE
```
10 Delete the node from the cluster.

```bash
# hasys -delete sys5
```

11 Save the configuration, making it read only.

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

### Modifying configuration files on each remaining node

Perform the following tasks on each of the remaining nodes of the cluster.

**To modify the configuration files on a remaining node**

1. If necessary, modify the `/etc/gatbtab` file.

   No change is required to this file if the `/sbin/gabconfig` command has only the argument `-c`. Symantec recommends using the `-n N` option, where `N` is the number of cluster systems.

   If the command has the form `/sbin/gabconfig -c -n N`, where `N` is the number of cluster systems, make sure that `N` is not greater than the actual number of nodes in the cluster. When `N` is greater than the number of nodes, GAB does not automatically seed.

   Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`.

2. Modify `/etc/llthosts` file on each remaining nodes to remove the entry of the departing node.

   For example, change:

   ```
   0 sys1
   1 sys2
   2 sys5
   ```

   To:

   ```
   0 sys1
   1 sys2
   ```

### Removing the node configuration from the CP server

After removing a node from a VCS cluster, perform the steps in the following procedure to remove that node's configuration from the CP server.
Note: The `cpsadm` command is used to perform the steps in this procedure. For detailed information about the `cpsadm` command, see the *Veritas Cluster Server Administrator’s Guide*.

To remove the node configuration from the CP server

1. Log into the CP server as the root user.

2. View the list of VCS users on the CP server, using the following command:

   ```bash
   # 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:

   ```bash
   # cpsadm -s cp_server -a rm_user
   -e cpsclient@sys5 -f cps_operator -g vx
   ```

4. Remove the node entry from the CP server:

   ```bash
   # 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:

   ```bash
   # 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.

   ```bash
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh \ stop
   ```

2. Remove the credentials.

   ```bash
   # rm -rf /var/VRTSvcs/vcsauth/data/
   ```
Unloading LLT and GAB and removing VCS on the departing node

Perform the tasks on the node that is departing the cluster.
You can use script-based installer to uninstall VCS on the departing node or perform the following manual steps.

If you have configured VCS as part of the Storage Foundation and High Availability products, you may have to delete other dependent RPMs before you can delete all of the following ones.

To stop LLT and GAB and remove VCS

1. If you had configured I/O fencing in enabled mode, then stop I/O fencing.
   
   # /etc/init.d/vxfen stop

2. Stop GAB and LLT:
   
   # /etc/init.d/gab stop
   # /etc/init.d/llt stop

3. To determine the RPMs to remove, enter:

   # rpm -qa | grep VRTS

4. To permanently remove the VCS RPMs from the system, use the `rpm -e` command. Start by removing the following RPMs, which may have been optionally installed, in the order shown:

   # rpm -e VRTSvcsea
   # rpm -e VRTSatServer
   # rpm -e VRTSatClient
   # rpm -e VRTSvcsdr
   # rpm -e VRTSvcsag
   # rpm -e VRTScps
   # rpm -e VRTSvcs
   # rpm -e VRTSamf
   # rpm -e VRTSvxfen
   # rpm -e VRTSvxfen
   # rpm -e VRTSvxfen
   # rpm -e VRTSllt
   # rpm -e VRTSspt
   # rpm -e VRTSfcpip60
# rpm -e VRTSperl
# rpm -e VRTSvlic

5 Remove the LLT and GAB configuration files.

# rm /etc/llttab
# rm /etc/gabtab
# rm /etc/llthosts
Removing a node from a VCS cluster
Uninstallation of VCS

- Chapter 26. Uninstalling VCS using the installer
- Chapter 27. Uninstalling VCS using response files
- Chapter 28. Manually uninstalling VCS
Uninstalling VCS using the installer

This chapter includes the following topics:

- Preparing to uninstall VCS
- Uninstalling VCS using the script-based installer
- Removing the CP server configuration using the installer program

Preparing to uninstall VCS

Review the following prerequisites before you uninstall VCS:

- Before you remove VCS from any node in the cluster, shut down the applications that depend on VCS. For example, applications such as Java Console or any high availability agents for VCS.
- Before you remove VCS from fewer than all nodes in a cluster, stop the service groups on the nodes from which you uninstall VCS. You must also reconfigure VCS on the remaining nodes.
- If you have manually edited any of the VCS configuration files, you need to reformat them.
  
  See “Reformatting VCS configuration files on a stopped cluster” on page 69.

Uninstalling VCS using the script-based installer

You must meet the following conditions to use the uninstallvcs program to uninstall VCS on all nodes in the cluster at one time:
Make sure that the communication exists between systems. By default, the uninstaller uses ssh.

Make sure you can execute `ssh` or `rsh` commands as superuser on all nodes in the cluster.

Make sure that the `ssh` or `rsh` is configured to operate without requests for passwords or passphrases.

If you cannot meet the prerequisites, then you must run the `uninstallvcs` program on each node in the cluster.

The `uninstallvcs` program removes all VCS RPMs.

The example demonstrates how to uninstall VCS using the `uninstallvcs` program. The `uninstallvcs` program uninstalls VCS on two nodes: sys1 sys2. The example procedure uninstalls VCS from all nodes in the cluster.

---

**Note:** If already present on the system, the uninstallation does not remove the VRTSacclib RPM.

---

**Removing VCS 6.0.2 RPMs**

The program stops the VCS processes that are currently running during the uninstallation process.

**To uninstall VCS**

1. Log in as superuser from the node where you want to uninstall VCS.
2. Start `uninstallvcs` program.

   ```
   # cd /opt/VRTS/install
   # ./uninstallvcs<version>
   ```

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

   The program specifies the directory where the logs are created. The program displays a copyright notice and a description of the cluster:

3. Enter the names of the systems from which you want to uninstall VCS.
   The program performs system verification checks and asks to stop all running VCS processes.

4. Enter `y` to stop all the VCS processes.
   The program stops the VCS processes and proceeds with uninstalling the software.

5. Review the output as the `uninstallvcs` program continues to do the following:
Uninstalling VCS using the installer

Verifies the communication between systems
Checks the installations on each system to determine the RPMs to be uninstalled.

6 Review the output as the uninstaller stops processes, unloads kernel modules, and removes the RPMs.

7 Note the location of summary, response, and log files that the uninstaller creates after removing all the RPMs.

Running uninstallvcs from the VCS 6.0.2 disc

You may need to use the uninstallvcs program on the VCS 6.0.2 disc in one of the following cases:
- You need to uninstall VCS after an incomplete installation.
- The uninstallvcs program is not available in /opt/VRTS/install.

If you mounted the installation media to /mnt, access the uninstallvcs program by changing directory to:

```
cd /mnt/cluster_server/
./uninstallvcs
```

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 VCS 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:

```bash
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 SPHA 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 vxcpserver 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.
Uninstalling VCS using the installer

Removing the CP server configuration using the installer program
Uninstalling VCS using response files

This chapter includes the following topics:

- Uninstalling VCS using response files
- Response file variables to uninstall VCS
- Sample response file for uninstalling VCS

Uninstalling VCS using response files

Typically, you can use the response file that the installer generates after you perform VCS uninstallation on one cluster to uninstall VCS on other clusters.

To perform an automated uninstallation

1. Make sure that you meet the prerequisites to uninstall VCS.
2. Copy the response file to the system where you want to uninstall VCS.
   
   See “Sample response file for uninstalling VCS” on page 327.

3. Edit the values of the response file variables as necessary.
   See “Response file variables to uninstall VCS” on page 326.

4. Start the uninstallation from the system to which you copied the response file. For example:

   ```
   # /opt/VRTS/install/uninstallvcs<version>
   -responsefile /tmp/response_file
   ```

   Where `<version>` is the specific release version, and `/tmp/response_file` is the response file’s full path name.
## Response file variables to uninstall VCS

Table 27-1 lists the response file variables that you can define to uninstall VCS.

### Table 27-1  
Response file variables specific to uninstalling VCS

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[opt][uninstall]</td>
<td>Scalar</td>
<td>Uninstalls VCS RPMs. (Required)</td>
</tr>
<tr>
<td>CFG[systems]</td>
<td>List</td>
<td>List of systems on which the product is to be uninstalled. (Required)</td>
</tr>
<tr>
<td>CFG[prod]</td>
<td>Scalar</td>
<td>Defines the product to be uninstalled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value is VCS60 for VCS. (Required)</td>
</tr>
<tr>
<td>CFG[opt][keyfile]</td>
<td>Scalar</td>
<td>Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)</td>
</tr>
<tr>
<td>CFG[opt][rsh]</td>
<td>Scalar</td>
<td>Defines that rsh must be used instead of ssh as the communication method between systems. (Optional)</td>
</tr>
<tr>
<td>CFG[opt][logpath]</td>
<td>Scalar</td>
<td>Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. Note: The installer copies the response files and summary files also to the specified logpath location. (Optional)</td>
</tr>
</tbody>
</table>
Sample response file for uninstalling VCS

Review the response file variables and their definitions.
See “Response file variables to uninstall VCS” on page 326.

# Configuration Values:
our %CFG;

$CFG{opt}{uninstall}=1;
$CFG{prod}="VCS601";
$CFG{systems}=[ qw(sys1 sys2) ];
1;
Manually uninstalling VCS

This chapter includes the following topics:

■ Removing VCS RPMs manually
■ Manually remove the CP server fencing configuration
■ Manually deleting cluster details from a CP server

Removing VCS RPMs manually

You must remove the VCS RPMs from each node in the cluster to uninstall VCS.

To manually remove VCS RPMs on a node

1. Shut down VCS on the local system using the hastop command.
   
   # hastop -local

2. Stop the CmdServer.
   
   # /opt/VRTSvcs/bin/CmdServer -stop

3. Unconfigure the fencing, GAB, LLT, and AMF modules.
   
   # /sbin/vxfenconfig -U
   # /sbin/gabconfig -U
   # /sbin/lltconfig -U
   # /opt/VRTSamf/bin/amfconfig -U

4. Unload the VxFEN driver:
   
   # /etc/init.d/vxfen stop
5  Unload the GAB driver:
   
   # /etc/init.d/gab stop

6  Unload the LLT driver:
   
   # /etc/init.d/llt stop

7  Unload the AMF driver:
   
   # /etc/init.d/amf stop

8  Remove the VCS 6.0.2 RPMs in the following order:
   
   # rpm -e VRTSvbs
   # rpm -e VRTSsfmh
   # rpm -e VRTSat (if exists)
   # rpm -e VRTSvcsfa
   # rpm -e VRTSvcsdr
   # rpm -e VRTSvcsag
   # rpm -e VRTScps
   # rpm -e VRTSvcs
   # rpm -e VRTSamf
   # rpm -e VRTSvxfen
   # rpm -e VRTSgab
   # rpm -e VRTSllt
   # rpm -e VRTSspt
   # rpm -e VRTSfcp602
   # rpm -e VRTSper1
   # rpm -e VRTSvlic

Note: The VRTScps RPM should be removed after manually removing the CP server fencing configuration. See “Manually remove the CP server fencing configuration” on page 330.

Manually remove the CP server fencing configuration

The following procedure describes how to manually remove the CP server fencing configuration from the CP server. This procedure is performed as part of the process to stop and remove server-based IO fencing.
Note: This procedure must be performed after the VCS cluster has been stopped, but before the VCS cluster software is uninstalled.

This procedure is required so that the CP server database can be reused in the future for configuring server-based fencing on the same VCS cluster(s).

Perform the steps in the following procedure to manually remove the CP server fencing configuration.

Note: The `cpsadm` command is used in the following procedure. For detailed information about the `cpsadm` command, see the *Veritas Cluster Server Administrator's Guide*.

**To manually remove the CP server fencing configuration**

1. Unregister all VCS cluster nodes from all CP servers using the following command:

   ```bash
   # cpsadm -s cp_server -a unreg_node -u uuid -n nodeid
   ```

2. Remove the VCS cluster from all CP servers using the following command:

   ```bash
   # cpsadm -s cp_server -a rm_clus -u uuid
   ```

3. Remove all the VCS cluster users communicating to CP servers from all the CP servers using the following command:

   ```bash
   # cpsadm -s cp_server -a rm_user -e user_name -g domain_type
   ```

4. Proceed to uninstall the VCS cluster software.

**Manually deleting cluster details from a CP server**

You can manually delete the cluster details from a coordination point server (CP server) using the following procedure.
To manually delete cluster details from a CP server

1. List the nodes in the CP server cluster:

   ```
   # cpsadm -s cps1 -a list_nodes
   ```

<table>
<thead>
<tr>
<th>ClusterName</th>
<th>UUID</th>
<th>Hostname (Node ID)</th>
<th>Registered</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1</td>
<td>{3719a60a-1dd2-11b2-b8dc-197f8305ff0c0}</td>
<td>node0(0)</td>
<td>1</td>
</tr>
</tbody>
</table>

2. List the CP server users:

   ```
   # cpsadm -s cps1 -a list_users
   ```

<table>
<thead>
<tr>
<th>Username/Domain</th>
<th>Type</th>
<th>Cluster Name/UUID</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpsclient@hostname/vx</td>
<td></td>
<td>cluster1/{3719a60a-1dd2-11b2-b8dc-197f8305ff0c0}</td>
<td>Operator</td>
</tr>
</tbody>
</table>

3. Remove the privileges for each user of the cluster that is listed in step 2 from the CP server cluster. For example:

   ```
   # cpsadm -s cps1 -a rm_clus_from_user
   -c cluster1 -e cpsclient@hostname -g vx -f cps_operator
   Cluster successfully deleted from user cpsclient@hostname privileges.
   ```

4. Remove each user of the cluster that is listed in step 2. For example:

   ```
   # cpsadm -s cps1 -a rm_user -e cpsclient@hostname -g vx
   User cpsclient@hostname successfully deleted
   ```

5. Unregister each node that is registered to the CP server cluster. See the output of step 1 for registered nodes. For example:

   ```
   # cpsadm -s cps1 -a unreg_node -c cluster1 -n 0
   Node 0 (node0) successfully unregistered
   ```

6. Remove each node from the CP server cluster. For example:

   ```
   # cpsadm -s cps1 -a rm_node -c cluster1 -n 0
   Node 0 (node0) successfully deleted
   ```
7 Remove the cluster.

    # cpsadm -s cps1 -a rm_clus -c cluster1
Cluster cluster1 deleted successfully

8 Verify that the cluster details are removed successfully.

    # cpsadm -s cps1 -a list_nodes

    ClusterName   UUID     Hostname(Node ID)  Registered
    ===========   ===========  ===========

    # cpsadm -s cps1 -a list_users

    Username/Domain Type Cluster Name/UUID    Role
    ===========  ===========  ===========
Manually uninstalling VCS
Manually deleting cluster details from a CP server
Installation reference

- Appendix A. Services and ports
- Appendix B. VCS installation RPMs
- Appendix C. Installation command options
- Appendix D. Changes to bundled agents in VCS 6.0.2
- Appendix E. Configuration files
- Appendix F. Installing VCS on a single node
- Appendix G. Configuring LLT over UDP
- Appendix H. Configuring the secure shell or the remote shell for communications
- Appendix I. Troubleshooting VCS installation
- Appendix J. Sample VCS cluster setup diagrams for CP server-based I/O fencing
- Appendix K. Compatibility issues when installing Veritas Cluster Server with other products
Services and ports

This appendix includes the following topics:

- About SFHA services and ports

About SFHA services and ports

If you have configured a firewall, ensure that the firewall settings allow access to the services and ports used by SFHA.

Table A-1 lists the services and ports used by SFHA.

Note: The port numbers that appear in bold are mandatory for configuring SFHA.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocol</th>
<th>Description</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>2148 (TCP)</td>
<td>TCP</td>
<td>Veritas Enterprise Administrator (VEA) Server</td>
<td>vxsvc.exe</td>
</tr>
<tr>
<td>4145</td>
<td>TCP/UDP</td>
<td>VVR Connection Server VCS Cluster Heartbeats</td>
<td>vxio.sys</td>
</tr>
<tr>
<td>4888</td>
<td>TCP</td>
<td>Veritas Scheduler Service Use to launch the configured schedule.</td>
<td>VxSchedService.exe</td>
</tr>
<tr>
<td>5634</td>
<td>HTTPS</td>
<td>Veritas Storage Foundation Messaging Service</td>
<td>xprtl.exe</td>
</tr>
<tr>
<td>Port Number</td>
<td>Protocol</td>
<td>Description</td>
<td>Process</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>7419</td>
<td>TCP</td>
<td>Symantec Plugin Host Service Solutions Configuration Center (SFWConfigPanel.exe) CCF Engine (CEngineDriver.exe)</td>
<td>pluginHost.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vras.dll Volume Replicator Administrative Service</td>
<td>vras.dll</td>
</tr>
<tr>
<td>8199</td>
<td>TCP</td>
<td>VVR Resync Utility</td>
<td>vxreserver.exe</td>
</tr>
<tr>
<td>14141</td>
<td>TCP</td>
<td>Veritas High Availability Engine Veritas Cluster Manager (Java console) (ClusterManager.exe) VCS Agent driver (VCSAgDriver.exe)</td>
<td>had</td>
</tr>
<tr>
<td>14144</td>
<td>TCP/UDP</td>
<td>VCS Notification</td>
<td>Notifier.exe</td>
</tr>
<tr>
<td>14149</td>
<td>TCP/UDP</td>
<td>VCS Authentication</td>
<td>vcsauthserver</td>
</tr>
<tr>
<td>14150</td>
<td>TCP</td>
<td>Veritas Command Server</td>
<td>CmdServer</td>
</tr>
<tr>
<td>14153, 15550 - 15558</td>
<td>TCP/UDP</td>
<td>VCS Cluster Simulator</td>
<td>hasim.exe For more information about the ports used by the VCS Simulator, see the Veritas Cluster Server Administrator's Guide.</td>
</tr>
<tr>
<td>14155</td>
<td>TCP/UDP</td>
<td>VCS Global Cluster Option (GCO)</td>
<td>wac</td>
</tr>
<tr>
<td>14156</td>
<td>TCP/UDP</td>
<td>VCS Steward for GCO</td>
<td>steward</td>
</tr>
<tr>
<td>14250</td>
<td>TCP</td>
<td>Coordination Point Server</td>
<td>Vxcpserv</td>
</tr>
</tbody>
</table>
Table A-1  SFHA services and ports (continued)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocol</th>
<th>Description</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>49152-65535</td>
<td>TCP/UDP</td>
<td>Volume Replicator Packets</td>
<td>User configurable ports created at kernel level by vxio.sys file</td>
</tr>
</tbody>
</table>
About SFHA services and ports
This appendix includes the following topics:

- **Veritas Cluster Server installation RPMs**

## Veritas Cluster Server installation RPMs

Table B-1 shows the RPM name and contents for each Veritas Cluster Server RPM.

<table>
<thead>
<tr>
<th>RPM</th>
<th>Contents</th>
<th>Required/Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRTSamf</td>
<td>Contains the binaries for the Veritas Asynchronous Monitoring Framework kernel driver functionality for the Process and Mount based agents.</td>
<td>Required</td>
</tr>
<tr>
<td>VRTScps</td>
<td>Contains the binaries for the Veritas Coordination Point Server.</td>
<td>Optional. Required to Coordination Point Server (CPS).</td>
</tr>
<tr>
<td>VRTSgab</td>
<td>Contains the binaries for Veritas Cluster Server group membership and atomic broadcast services.</td>
<td>Required Depends on VRTSllt.</td>
</tr>
<tr>
<td>VRTSllt</td>
<td>Contains the binaries for Veritas Cluster Server low-latency transport.</td>
<td>Required</td>
</tr>
<tr>
<td>VRTSperl</td>
<td>Contains Perl binaries for Veritas.</td>
<td>Required</td>
</tr>
<tr>
<td>RPM</td>
<td>Contents</td>
<td>Required/Optional</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
| VRTSfcpip602 | Veritas Storage Foundation Common Product Installer  
  The Storage Foundation Common Product installer RPM contains the scripts that perform the following:  
  ■ installation  
  ■ configuration  
  ■ upgrade  
  ■ uninstallation  
  ■ adding nodes  
  ■ removing nodes  
  ■ etc.  
  You can use this script to simplify the native operating system installations, configurations, and upgrades. | Required                    |
| VRTSvcsvmw     | Contents the Veritas Cluster Server virtual machine wizards for application monitoring configurations by Symantec.                                                                                     | Required                    |
| VRTSspt        | Contains the binaries for Veritas Software Support Tools.                                                                                                                                               | Recommended RPM, optional   |
| VRTSvcs        | VRTSvcs contains the following components:  
  ■ Contains the binaries for Veritas Cluster Server.  
  ■ Contains the binaries for Veritas Cluster Server manual pages.  
  ■ Contains the binaries for Veritas Cluster Server message catalogs.  
  ■ Contains the binaries for Veritas Cluster Server utilities. These utilities include security services. | Required                    |

**Table B-1**  
Veritas Cluster Server RPMs (continued)
<table>
<thead>
<tr>
<th>RPM</th>
<th>Contents</th>
<th>Required/Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRTSvcsag</td>
<td>Contains the binaries for Veritas Cluster Server bundled agents.</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depends on VRTSvcs.</td>
</tr>
<tr>
<td>VRTSvcsdr</td>
<td>Contains the binaries for Veritas Cluster Server disk reservation.</td>
<td>Required</td>
</tr>
<tr>
<td>VRTSvcssea</td>
<td>VRTSvcssea contains the binaries for Veritas high availability agents for DB2, Sybase, and Oracle.</td>
<td>Optional for VCS. Required to use VCS with the high availability agents for DB2, Sybase, or Oracle.</td>
</tr>
<tr>
<td>VRTSvlic</td>
<td>Contains the binaries for Symantec License Utilities.</td>
<td>Required</td>
</tr>
<tr>
<td>VRTSvxfen</td>
<td>Contains the binaries for Veritas I/O Fencing.</td>
<td>Required to use fencing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depends on VRTSgab.</td>
</tr>
<tr>
<td>VRTSsfmh</td>
<td>Veritas Storage Foundation Managed Recommended Host</td>
<td>Recommended</td>
</tr>
<tr>
<td></td>
<td>DisCOVERs configuration information on a Storage Foundation managed host.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This information is stored on a central database, which is not part of this release. You must download the database separately at:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.symantec.com/business/storage-foundation-manager">http://www.symantec.com/business/storage-foundation-manager</a></td>
<td></td>
</tr>
<tr>
<td>VRTSvbs</td>
<td>Enables fault management and VBS command line operations on VCS nodes managed by Veritas Operations Manager.</td>
<td>Recommended</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Virtual Business Service–Availability User’s Guide.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Depends on VRTSsfmh. VRTSsfmh version must be 4.1 or later for VRTSvbs to get installed.</td>
<td></td>
</tr>
</tbody>
</table>
VCS installation RPMs
Veritas Cluster Server installation RPMs
Installation command options

This appendix includes the following topics:

- Installation script options
- Command options for uninstallvcs program

Installation script options

Table C-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.

Table C-1 Available command line options

<table>
<thead>
<tr>
<th>Commandline Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>-allpkgs</td>
<td>Displays all RPMs required for the specified product. The RPMs are listed in correct installation order. The output can be used to create scripts for command line installs, or for installations over a network.</td>
</tr>
<tr>
<td>-comcleanup</td>
<td>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.</td>
</tr>
<tr>
<td>Commandline Option</td>
<td>Function</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-configure</td>
<td>Configures the product after installation.</td>
</tr>
<tr>
<td>-hostfile full_path_to_file</td>
<td>Specifies the location of a file that contains a list of hostnames on which to install.</td>
</tr>
<tr>
<td>-installallpkgs</td>
<td>The -installallpkgs option is used to select all RPMs.</td>
</tr>
<tr>
<td>-installrecpkgs</td>
<td>The -installrecpkgs option is used to select the recommended RPMs set.</td>
</tr>
<tr>
<td>-installminpkgs</td>
<td>The -installminpkgs option is used to select the minimum RPMs set.</td>
</tr>
<tr>
<td>-ignorepatchreqs</td>
<td>The -ignorepatchreqs option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.</td>
</tr>
<tr>
<td>-keyfile ssh_key_file</td>
<td>Specifies a key file for secure shell (SSH) installs. This option passes -i ssh_key_file to every SSH invocation.</td>
</tr>
<tr>
<td>-license</td>
<td>Registers or updates product licenses on the specified systems.</td>
</tr>
<tr>
<td>-logpath log_path</td>
<td>Specifies a directory other than /opt/VRTS/install/logs as the location where installer log files, summary files, and response files are saved.</td>
</tr>
<tr>
<td>-makeresponsefile</td>
<td>Use the -makeresponsefile option only to generate response files. No actual software installation occurs when you use this option.</td>
</tr>
<tr>
<td>-minpkgs</td>
<td>Displays the minimal RPMs required for the specified product. The RPMs are listed in correct installation order. Optional RPMs are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See allpkgs option.</td>
</tr>
<tr>
<td>-nolic</td>
<td>Allows installation of product RPMs without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.</td>
</tr>
<tr>
<td>Commandline Option</td>
<td>Function</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
</tr>
<tr>
<td><code>-pkginfo</code></td>
<td>Displays a list of RPMs and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the <code>-pkginfo</code> option with the installvcs script to display VCS RPMs.</td>
</tr>
<tr>
<td><code>-pkgpath package_path</code></td>
<td>Designates the path of a directory that contains all RPMs to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.</td>
</tr>
<tr>
<td><code>-pkgset</code></td>
<td>Discovers and displays the RPM group (minimum, recommended, all) and RPMs that are installed on the specified systems.</td>
</tr>
<tr>
<td><code>-pkgtbale</code></td>
<td>Displays product's RPMs in correct installation order by group.</td>
</tr>
<tr>
<td><code>-postcheck</code></td>
<td>Checks for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups.</td>
</tr>
<tr>
<td><code>-precheck</code></td>
<td>Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.</td>
</tr>
<tr>
<td><code>-recpkgs</code></td>
<td>Displays the recommended RPMs required for the specified product. The RPMs are listed in correct installation order. Optional RPMs are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See <code>allpkgs</code> option.</td>
</tr>
<tr>
<td><code>-redirect</code></td>
<td>Displays progress details without showing the progress bar.</td>
</tr>
<tr>
<td><code>-requirements</code></td>
<td>The <code>-requirements</code> option displays required OS version, required RPMs and patches, file system space, and other system requirements in order to install the product.</td>
</tr>
<tr>
<td>Commandline Option</td>
<td>Function</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
</tr>
<tr>
<td>-responsefile <em>response_file</em></td>
<td>Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The <em>response_file</em> 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.</td>
</tr>
<tr>
<td>-rsh</td>
<td>Specify this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.</td>
</tr>
<tr>
<td>-serial</td>
<td>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.</td>
</tr>
<tr>
<td>-settunables</td>
<td>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.</td>
</tr>
<tr>
<td>-start</td>
<td>Starts the daemons and processes for the specified product.</td>
</tr>
<tr>
<td>-stop</td>
<td>Stops the daemons and processes for the specified product.</td>
</tr>
<tr>
<td>-timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table C-1  Available command line options (continued)

<table>
<thead>
<tr>
<th>Commandline Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>-tmppath tmp_path</td>
<td>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 RPMs are copied on remote systems before installation.</td>
</tr>
<tr>
<td>-tunables</td>
<td>Lists all supported tunables and create a tunables file template.</td>
</tr>
<tr>
<td>-tunables_file tunables_file</td>
<td>Specify this option when you specify a tunables file. The tunables file should include tunable parameters.</td>
</tr>
<tr>
<td>-upgrade</td>
<td>Specifies that an existing version of the product exists and you plan to upgrade it.</td>
</tr>
<tr>
<td>-version</td>
<td>Checks and reports the installed products and their versions. Identifies the installed and missing RPMs and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing RPMs and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.</td>
</tr>
<tr>
<td>-yumgroupxml</td>
<td>The -yumgroupxml option is used to generate a yum group definition XML file. The createrepo command can use the file on Redhat Linux to create a yum group for automated installation of all RPMs for a product. An available location to store the XML file should be specified as a complete path. The -yumgroupxml option is supported on Redhat Linux only.</td>
</tr>
</tbody>
</table>

Command options for uninstallvcs program

The uninstallvcs command usage takes the following form:

uninstallvcs [ system1 system2... ]
    [ -responsefile response_file ]
    [ -logpath log_path ]
    [ -tmppath tmp_path]
Installation command options

Command options for uninstallvcs program

[ -timeout timeout_value ]
[ -keyfile ssh_key_file ]
[ -hostfile hostfile_path ]
[ -serial | -rsh | -redirect | -makeresponsefile | -comcleanup | -version ]

For description of the uninstallvcs command options:
Changes to bundled agents in VCS 6.0.2

This appendix includes the following topics:

- Deprecated agents
- New agents
- New and modified attributes for 6.0.1 agents
- Manually removing deprecated resource types and modifying attributes
- Creating new VCS accounts if you used native operating system accounts

Deprecated agents

The following agents are no longer supported:

- CampusCluster
- ClusterMonitorConfig
- SANVolume
- Service group heartbeat (ServiceGroupHB)
- VRTSWebApp
- Scsi3PR

Note: No agents were deprecated since the 5.1 SP1 release.
New agents

New agent added in VCS 6.0.2 release.

- VMwareDisks: Enables vMotion and VMware Distributed Resource Scheduler (DRS) in VCS clusters, configured and deployed on virtual machines in VMware environment.

New agents added in VCS 6.0.1 release

- VFRJob: Veritas File Replicator Job (VFRJob) agent provides high availability for Veritas File System Replicator Job (VFR Job). VFR Job supports replication of VxFS and CFS type file system.

The following new agent is added in the 6.0 release:

- KVMGuest—Monitors Linux kernel-based virtual machines (KVM guests), brings them online, and takes them offline.

The following agents were added in the 5.1 SP1 release:

- VolumeSet—Brings Veritas Volume Manager (VxVM) volume sets online and offline, and monitors them.

The following agents were added in the 5.1 release:

- CoordPoint—Provides server-based I/O fencing.

The following agents were added in the 5.0 MP3 release:

- DiskGroupSnap—Verifies the configuration and the data integrity in a campus cluster environment.

The following agents were added in the 5.0 release:

- NFSRestart—Provides high availability for NFS record locks.
- RemoteGroup—Monitors and manages a service group on another system.

Refer to the Veritas Cluster Server Bundled Agents Reference Guide for more information on these new agents.

New and modified attributes for 6.0.1 agents

Table D-1 lists the attributes that VCS adds or modifies when you upgrade from VCS 6.0 to VCS 6.0.1

<table>
<thead>
<tr>
<th>Agent</th>
<th>New/Modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>New/Modified attributes</td>
<td>Default value</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>DiskGroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attribute modified:</td>
<td>{ MonitorProcesses, User,</td>
</tr>
<tr>
<td></td>
<td>IMFRegList</td>
<td>PidFiles, MonitorProgram,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StartProgram }</td>
</tr>
<tr>
<td></td>
<td>New attribute added:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IMFRegList</td>
<td>{ DiskGroup, Reservation }</td>
</tr>
<tr>
<td></td>
<td>New attribute added:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IMF</td>
<td>{ Mode = 3, MonitorFreq = 5,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RegisterRetryLimit = 3 }</td>
</tr>
<tr>
<td></td>
<td>Deprecated attribute:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DiskGroupType</td>
<td></td>
</tr>
<tr>
<td>New agent:</td>
<td>VFRJob</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ArgList</td>
<td>{ JobName, SrcMountPoint,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SrcAddress }</td>
</tr>
<tr>
<td></td>
<td>JobName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SrcMountPoint</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SrcAddress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IntentionalOffline</td>
<td>1</td>
</tr>
<tr>
<td>KVMGuest</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attribute added:</td>
<td>&quot;GuestName&quot;,</td>
</tr>
<tr>
<td></td>
<td>RegList</td>
<td>&quot;DelayAfterGuestOnline&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;DelayAfterGuestOffline&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;RHEVMInfo&quot; }</td>
</tr>
<tr>
<td></td>
<td>New attribute added:</td>
<td>{ Enabled=0, URL=NONE,</td>
</tr>
<tr>
<td></td>
<td>RHEVMInfo</td>
<td>User=NONE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password=NONE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cluster=NONE }</td>
</tr>
<tr>
<td></td>
<td>New attribute added:</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ResyncVMCfg</td>
<td>Do not set ResyncVMCfg</td>
</tr>
<tr>
<td></td>
<td></td>
<td>attribute manually.</td>
</tr>
</tbody>
</table>
Table D-2 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.1 SP1 to VCS 6.0.2.

Table D-3 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.1 to VCS 5.1 SP1.

Table D-4 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.0 MP3 or later to VCS 5.1.

Table D-5 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.0 or later to VCS 5.0 MP3.

Table D-6 lists the attributes that VCS adds or modifies when you upgrade from VCS 4.1 to VCS 5.0.

### Table D-2  Changes to attributes from VCS 5.1 SP1 to 6.0

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SupportedActions</td>
<td>{ &quot;program.vfd&quot;, &quot;user.vfd&quot;, &quot;cksum.vfd&quot;, getcksum, propcv }</td>
</tr>
<tr>
<td>DNS</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UseGSSAPI</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>RefreshInterval</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>CleanRRKeys</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ArgList</td>
<td>{ Domain, TTL, TSIGKeyFile, StealthMasters, ResRecord, CreatePTR, OffDelRR, UseGSSAPI, RefreshInterval, CleanRRKeys }</td>
</tr>
<tr>
<td>DiskGroup</td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>New and modified attributes</td>
<td>Default value</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>PanicSystemOnDGLOss</td>
<td>int PanicSystemOnDGLOss = 0</td>
<td>(attribute data type change)</td>
</tr>
<tr>
<td>ArgList</td>
<td>{DiskGroup, StartVolumes, StopVolumes, MonitorOnly, MonitorReservation, PanicSystemOnDGLOss, tempUseFence, DiskGroupType, UmountVolumes, Reservation, ConfidenceLevel }</td>
<td>(new attribute added to list)</td>
</tr>
<tr>
<td>DiskGroupSnap</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>New attribute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FDType</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified attribute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ArgList</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ TargetResName, FDSiteName, FDType }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(new attribute added to list)</td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified attribute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RegList</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ NetMask }</td>
</tr>
<tr>
<td>Mount</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AEPTTimeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IMF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ Mode = 3, MonitorFreq = 1, RegisterRetryLimit = 3 }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SecondLevelMonitor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(deprecated attribute)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SecondLevelTimeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(deprecated attribute)</td>
</tr>
</tbody>
</table>
Table D-2  Changes to attributes from VCS 5.1 SP1 to 6.0 (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArgList</td>
<td>static str ArgList[] = { MountPoint, BlockDevice, FSType, MountOpt, FsckOpt, SnapUmount, CkptUmount, OptCheck, CreateMntPt, MntPtPermission, MntPtOwner, MntPtGroup, AccessPermissionChk, RecursiveMnt, VxFSMountLock }</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(list updated for deprecated attributes)</td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td>IMF</td>
<td>{ Mode = 3, MonitorFreq = 5, RegisterRetryLimit = 3 }</td>
<td></td>
</tr>
<tr>
<td>KVMGuest</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SupportedActions { &quot;guestmigrated&quot; }</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ArgList { GuestName, DelayAfterGuestOnline, DelayAfterGuestOffline, SyncDir, GuestConfigFilePath, CEInfo }</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CEInfo { Enabled=0, CESystem=NONE, FaultOnHBLoss=1 }</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IntentionalOffline 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GuestName &quot;&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DelayAfterGuestOnline 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DelayAfterGuestOffline 30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SyncDir &quot;&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GuestConfigFilePath &quot;&quot;</td>
<td></td>
</tr>
</tbody>
</table>

Table D-3  Changes to attributes from VCS 5.1 to VCS 5.1 SP1

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table D-3

Changes to attributes from VCS 5.1 to VCS 5.1 SP1 *(continued)*

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>New attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EnvFile</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>UseSUDash</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>IMFRegList</td>
<td>{ MonitorProcesses, User, PidFiles, MonitorProgram }</td>
<td></td>
</tr>
<tr>
<td>Modified attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>&quot;root&quot;</td>
<td></td>
</tr>
<tr>
<td>(change in default value)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ User, StartProgram, StopProgram, CleanProgram, MonitorProgram, PidFiles, MonitorProcesses, EnvFile, UseSUDash }</td>
<td></td>
</tr>
<tr>
<td>(new attribute added to list)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DiskGroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reservation</td>
<td>&quot;ClusterDefault&quot;</td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{DiskGroup, StartVolumes, StopVolumes, MonitorOnly, MonitorReservation, tempUseFence, PanicSystemOnDGLoss, UmountVolumes, Reservation }</td>
<td></td>
</tr>
<tr>
<td>(new attribute added to list)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LVMVolumeGroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EnableLVMTagging</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{VolumeGroup, StartVolumes, EnableLVMTagging }</td>
<td></td>
</tr>
<tr>
<td>(new attribute added to list)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mount</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>New and modified attributes</td>
<td>Default value</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IMFRegList</td>
<td>{ MountPoint, BlockDevice, FSType }</td>
<td></td>
</tr>
<tr>
<td>MultiNICA</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mii</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ Device, DualDevice, NetMask, PrefixLen, Options, RouteOptions, PingOptimize, MonitorOnly, NetworkHosts, Failback, LinkOptions, IPv4AddrOptions, IPv6AddrOptions, IPv4RouteOptions, IPv6RouteOptions, Mii }</td>
<td>(new attribute added to list)</td>
</tr>
<tr>
<td>NFSRestart</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lower</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ &quot;NFSRes:Nproc&quot;, &quot;NFSRes:GracePeriod&quot;, &quot;NFSRes:NFSv4Support&quot;, NFSLockFailover, LocksPathName, Lower, State }</td>
<td>(new attribute added to list)</td>
</tr>
<tr>
<td>NetBios</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PidFile</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
</tbody>
</table>
### Table D-3  Changes to attributes from VCS 5.1 to VCS 5.1 SP1 (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotifierMngr</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NotifierSourceIP</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ArgList</td>
<td>{ EngineListeningPort, MessagesQueue, NotifierListeningPort, NotifierSourceIP, SnmpdTrapPort, SnmpCommunity, SnmpConsoles, SmtpServer, SmtpServerVrfyOff, SmtpServerTimeout, SmtpReturnPath, SmtpFromPath, SmtpRecipients }</td>
</tr>
<tr>
<td></td>
<td>(new attribute added to list)</td>
<td></td>
</tr>
<tr>
<td>RemoteGroup</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ReturnIntOffline</td>
<td>{ }</td>
</tr>
<tr>
<td></td>
<td>OfflineMonitoringNode</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IntentionalOffline</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>(change in default value, RemoteGroup agent now supports intentional offline feature.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ArgList</td>
<td>{ IpAddress, Port, Username, Password, GroupName, VCSSysName, ControlMode, OfflineWaitTime, DomainType, BrokerIp, ReturnIntOffline }</td>
</tr>
<tr>
<td></td>
<td>(new attribute added to list)</td>
<td></td>
</tr>
<tr>
<td>RVGPrimary</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BunkerSyncTimeOut</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>BunkerSyncElapsedTime</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Modified attributes</td>
<td></td>
</tr>
</tbody>
</table>
### Table D-3

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArgList</td>
<td>{ RvgResourceName,</td>
<td>{ RvgResourceName, &quot;RvgResourceName:RVG&quot;, &quot;RvgResourceName:DiskGroup&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;RvgResourceName:DiskGroup&quot;,</td>
<td>AutoTakeover, AutoResync, BunkerSyncTimeOut, BunkerSyncElapsedTime }</td>
</tr>
<tr>
<td></td>
<td>(new attribute added to list)</td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td></td>
<td>{ fbsync, ElectPrimary }</td>
</tr>
<tr>
<td>(new action added to keylist)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RVGSnapshot</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td>VCSResLock</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>SambaServer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PidFile</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>SocketAddress</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>SambaTopDir</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ArgList</td>
<td>{ ConfFile, SambaTopDir, LockDir, Ports, IndepthMonitorCyclePeriod, ResponseTimeout, PidFile, SocketAddress }</td>
</tr>
<tr>
<td>(new attribute added to list)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SambaShare</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td>(dependent attributes added to list)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table D-3
Changes to attributes from VCS 5.1 to VCS 5.1 SP1 (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VolumeSet</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DiskGroup</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>VolumeSet</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>ArgList</td>
<td>{DiskGroup, VolumeSet}</td>
</tr>
</tbody>
</table>

### Table D-4
Changes to attributes from VCS 5.0 MP3 to VCS 5.1

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alias</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
<tr>
<td>DiskGroup</td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PanicSystemOnDGLoss</td>
<td>0</td>
</tr>
<tr>
<td>IP</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPOptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPRouteOptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PrefixLen</td>
<td>1000</td>
</tr>
<tr>
<td>IPMultiNIC</td>
<td>New attributes</td>
<td></td>
</tr>
</tbody>
</table>
### Table D-4

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrefixLen</td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>IPOptions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Mount**

New attributes

- OptCheck: 0
- CreateMountPt: 0
- ReuseMntPt: 0
- MntPtPermission
- MntPtOwner
- MntPtGroup
- AccessPermissionChk: 0
- RecursiveMnt: 0

**MultiNICA**

New attributes

- DualDevice

<table>
<thead>
<tr>
<th>PrefixLen</th>
<th>1000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>LinkOptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4AddrOptions</td>
</tr>
<tr>
<td>IPv6AddrOptions</td>
</tr>
<tr>
<td>IPv4RouteOptions</td>
</tr>
<tr>
<td>IPv6RouteOptions</td>
</tr>
</tbody>
</table>

**NFS**

Modified attribute

- Address
  - (deleted attribute)
### Table D-4
Changes to attributes from VCS 5.0 MP3 to VCS 5.1 (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NFSRes</td>
<td></td>
</tr>
</tbody>
</table>

### Table D-5
Changes to attributes from VCS 5.0 to VCS 5.0 MP3

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PidFile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IntentionalOffline</td>
<td>0</td>
</tr>
<tr>
<td>DiskGroup</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UmountVolumes</td>
<td>0</td>
</tr>
<tr>
<td>Modified attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ &quot;license.vfd&quot;, &quot;disk.vfd&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;udid.vfd&quot;, &quot;verifyplex.vfd&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>checkudid, numdisks, campusplex,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>joindg, splitdg, getvxxvminfo,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>volinuse }</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SupportedActions</td>
<td>{ &quot;dig.vfd&quot;, &quot;keyfile.vfd&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;master.vfd&quot; }</td>
</tr>
<tr>
<td>ResRecord</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CreatePTR</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>OffDelRR</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LVMVolumeGroup</td>
<td>New attributes</td>
<td></td>
</tr>
</tbody>
</table>
### Table D-5  Changes to attributes from VCS 5.0 to VCS 5.0 MP3 (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SupportedActions</td>
<td>{ volinuse }</td>
<td></td>
</tr>
<tr>
<td>Mount</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td>RegList</td>
<td>{ VxFSMountLock }</td>
<td></td>
</tr>
<tr>
<td>VxFSMountLock</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Modified attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>[ &quot;mountpoint.vfd&quot;, &quot;mounted.vfd&quot;, &quot;vxfslic.vfd&quot;, &quot;chgmntlock&quot;, &quot;mountentry.vfd&quot; ]</td>
<td></td>
</tr>
<tr>
<td>NFSRestart</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ &quot;lockdir.vfd&quot;,&quot;nfsconf.vfd&quot; }</td>
<td></td>
</tr>
<tr>
<td>Share</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ &quot;direxists.vfd&quot; }</td>
<td></td>
</tr>
</tbody>
</table>

### Table D-6  Changes to attributes from VCS 4.1 to VCS 5.0 MP3

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ &quot;program.vfd&quot;, &quot;user.vfd&quot;, &quot;cksum.vfd&quot;, getcksum }</td>
<td></td>
</tr>
<tr>
<td>DiskGroup</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td>DiskGroupType</td>
<td>private</td>
<td></td>
</tr>
<tr>
<td>Modified attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>New and modified attributes</td>
<td>Default value</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>StopVolumes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>StartVolumes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ &quot;license.vfd&quot;, &quot;disk.vfd&quot;, numdisks }</td>
<td></td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ &quot;device.vfd&quot;, &quot;route.vfd&quot; }</td>
<td></td>
</tr>
<tr>
<td><strong>LVMVolumeGroup</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ volinuse }</td>
<td></td>
</tr>
<tr>
<td><strong>Mount</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ volinuse }</td>
<td></td>
</tr>
<tr>
<td><strong>NFS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFSSecurity</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>NFSv4Support</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LockFileTimeout</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>OnOnly</td>
<td></td>
</tr>
<tr>
<td>RestartLimit</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td><strong>Modified attributes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPResName: Renamed Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table D-6  Changes to attributes from VCS 4.1 to VCS 5.0 MP3 (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LockRecovery:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Replaced by NFSLockFailover</td>
<td></td>
</tr>
<tr>
<td></td>
<td>attribute in NFSRestart agent</td>
<td></td>
</tr>
<tr>
<td>NIC</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SupportedActions</td>
<td>{&quot;device.vfd&quot;}</td>
</tr>
<tr>
<td>Process</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SupportedActions</td>
<td>{&quot;program.vfd&quot;, getcksum}</td>
</tr>
</tbody>
</table>

---

### Manually removing deprecated resource types and modifying attributes

With VCS 6.0, certain resource type definitions are no longer used. Before you start the upgrade process, you must remove the resources of the deprecated resource types from your cluster configuration.

If you use the resource type ServiceGroupHB, Symantec recommends the use of I/O fencing.

VCS 5.1 does not support gabdiskhb. So, the installvcs program removes the gabdiskhb entry from the /etc/gabtab file.

**Note:** Make sure you start VCS on the local node before starting on the other nodes. This standard ensures that HAD reads the configuration from the local node and updates it on the remaining nodes.

**To remove the deprecated resource types and modify attributes**

1. Save the VCS configuration and stop the VCS engine.

   ```
   # haconf -dump -makero
   # hastop -all -force
   ```

2. Back up the configuration file, main.cf to a location on the cluster node.
3 Edit the main.cf located under /etc/VRTSvcs/conf/config.

Perform the following instructions:

■ Remove the resource of the deprecated resource types.
  You must modify the resource dependencies to ensure that the configuration works properly.

■ Modify attribute values that might have changed.

■ Save the main.cf.

■ Reformat the main.cf file.

  # hacf -cftocmd config
  # hacf -cmdtoci config

4 Verify the configuration.

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

5 Start VCS on the local node.

6 Start VCS on other nodes.

Creating new VCS accounts if you used native operating system accounts

VCS has deprecated the AllowNativeCliUsers attribute. To use native OS accounts with VCS, use the halogin command. After you run the halogin command, VCS encrypts and stores your VCS credentials in your home directory for a specific time period. After you run the halogin command, you need not authenticate yourself every time you run a VCS command. In secure clusters, the command also sets up a trust relationship and retrieves a certificate from an authentication broker.

See the Veritas Cluster Server Administrator’s Guide for information on assigning user privileges to OS user groups for clusters running in secure mode and clusters not running in secure mode.

Perform the following procedure if you used the AllowNativeCliUsers attribute. Ensure that each native user running VCS commands has a home directory on the system from which the user runs VCS commands.
To set up VCS authentication for clusters running in secure mode

1. Set the configuration (main.cf) mode to read/write.

   `# haconf -makerw`

2. Assign proper privileges to the OS users or user groups. Each operating system user must perform steps 3 and 4.

3. If the user executes VCS commands from a remote host, set the following environment variables:
   - VCS_HOST: Name of the VCS node on which you run commands. You may specify the virtual IP address associated with the cluster.
   - VCS_DOMAIN: Name of the VxSS domain to which the user belongs.
   - VCS_DOMAINTYPE: Type of VxSS domain: unixpwd, ldap, nt, nis, nisplus, or vx.

4. Run the halogin command:

   `$ halogin vcsusername password`

To set up VCS authentication for clusters not running in secure mode

1. Set the configuration (main.cf) mode to read/write.

   `# haconf -makerw`

2. Create VCS user accounts for all users and assign privileges to these users.

3. Each VCS user must run the halogin command:

   `$ halogin vcsusername password`
This appendix includes the following topics:

- About the LLT and GAB configuration files
- About the AMF configuration files
- About the VCS configuration files
- About I/O fencing configuration files
- Sample configuration files for CP server

About the LLT and GAB configuration files

Low Latency Transport (LLT) and Group Membership and Atomic Broadcast (GAB) are VCS communication services. LLT requires /etc/llthosts and /etc/llttab files. GAB requires /etc/gabtab file.

Table E-1 lists the LLT configuration files and the information that these files contain.
### Table E-1  
**LLT configuration files**

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
</table>
| /etc/sysconfig/llt | This file stores the start and stop environment variables for LLT:  
  - **LLT_START**—Defines the startup behavior for the LLT module after a system reboot. Valid values include:  
    1—Indicates that LLT is enabled to start up.  
    0—Indicates that LLT is disabled to start up.  
  - **LLT_STOP**—Defines the shutdown behavior for the LLT module during a system shutdown. Valid values include:  
    1—Indicates that LLT is enabled to shut down.  
    0—Indicates that LLT is disabled to shut down.  
  The installer sets the value of these variables to 1 at the end of VCS configuration.  
  If you manually configured VCS, make sure you set the values of these environment variables to 1. |
| /etc/llthosts   | The file **llthosts** is a database that contains one entry per system. This file links the LLT system ID (in the first column) with the LLT host name. This file must be identical on each node in the cluster. A mismatch of the contents of the file can cause indeterminate behavior in the cluster.  
  For example, the file /etc/llthosts contains the entries that resemble:  
  
  | 0       | sys1  |
  | 1       | sys2  |
Table E-1  LLT configuration files (continued)

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
</table>
| /etc/llttab | The file `llttab` contains the information that is derived during installation and used by the utility `lltconfig(1M)`. After installation, this file lists the LLT network links that correspond to the specific system.  

```
set-node sys1
set-cluster 2
link eth1 eth1 - ether - -
link eth2 eth2 - ether - -
```

For example, the file `/etc/llttab` contains the entries that resemble:

```
set-node sys1
set-cluster 2
link eth1 eth-00:04:23:AC:12:C4 - ether - -
link eth2 eth-00:04:23:AC:12:C5 - ether - -
```

If you use aggregated interfaces, then the file contains the aggregated interface name instead of the `eth-MAC_address`.

The first line identifies the system. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines begin with the `link` command. These lines identify the two network cards that the LLT protocol uses.

If you configured a low priority link under LLT, the file also includes a "link-lowpri" line.

Refer to the `llttab(4)` manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the `llttab` file.

Table E-2 lists the GAB configuration files and the information that these files contain.
### Table E-2  
**GAB configuration files**

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
</table>
| /etc/sysconfig/gab | This file stores the start and stop environment variables for GAB:  
|                    | - **GAB_START**— Defines the startup behavior for the GAB module after a system reboot. Valid values include:  
|                    |   1— Indicates that GAB is enabled to start up.  
|                    |   0— Indicates that GAB is disabled to start up.  
|                    | - **GAB_STOP**— Defines the shutdown behavior for the GAB module during a system shutdown. Valid values include:  
|                    |   1— Indicates that GAB is enabled to shut down.  
|                    |   0— Indicates that GAB is disabled to shut down.  
|                    | The installer sets the value of these variables to 1 at the end of VCS configuration.  
|                    | If you manually configured VCS, make sure you set the values of these environment variables to 1.  
| /etc/gabtab        | After you install VCS, the file /etc/gabtab contains a `gabconfig(1)` command that configures the GAB driver for use.  
|                    | The file /etc/gabtab contains a line that resembles:  
|                    | `/sbin/gabconfig -c -nN`  
|                    | The `-c` option configures the driver for use. The `-nN` specifies that the cluster is not formed until at least `N` nodes are ready to form the cluster.  
|                    | Symantec recommends that you set `N` to be the total number of nodes in the cluster.  
|                    | **Note:** Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`. Using `-c -x` can lead to a split-brain condition. Use the `-c` option for `/sbin/gabconfig` to avoid a split-brain condition.  
|                    | **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 E-3 lists the AMF configuration files.
Table E-3 AMF configuration files

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
</table>
| /etc/sysconfig/amf | This file stores the start and stop environment variables for AMF:  
  - **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:
    1—Indicates that AMF is enabled to start up. (default)  
    0—Indicates that AMF is disabled to start up.  
  - **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:
    1—Indicates that AMF is enabled to shut down. (default)  
    0—Indicates that AMF is disabled to shut down. |
| /etc/amftab | After you install VCS, the file /etc/amftab contains a amfconfig command that configures the AMF driver for use.  
  The AMF init script uses this /etc/amftab file to configure the AMF driver. The /etc/amftab file contains the following line by default:  
  /opt/VRTSamf/bin/amfconfig -c |

About the VCS configuration files

VCS configuration files include the following:

- **main.cf**  
The installer creates the VCS configuration file in the /etc/VRTSvcs/conf/config folder by default during the VCS configuration. The main.cf file contains the minimum information that defines the cluster and its nodes.  
  See “Sample main.cf file for VCS clusters” on page 375.  
  See “Sample main.cf file for global clusters” on page 376.

- **types.cf**  
The file types.cf, which is listed in the include statement in the main.cf file, defines the VCS bundled types for VCS resources. The file types.cf is also located in the folder /etc/VRTSvcs/conf/config.  
  Additional files similar to types.cf may be present if agents have been added, such as OracleTypes.cf.

- **/etc/sysconfig/vcs**  
  This file stores the start and stop environment variables for VCS engine:
- **VCS_START**—Defines the startup behavior for VCS engine after a system reboot. Valid values include:
  1—Indicates that VCS engine is enabled to start up.
  0—Indicates that VCS engine is disabled to start up.

- **VCS_STOP**—Defines the shutdown behavior for VCS engine during a system shutdown. Valid values include:
  1—Indicates that VCS engine is enabled to shut down.
  0—Indicates that VCS engine is disabled to shut down.
  
The installer sets the value of these variables to 1 at the end of VCS configuration.
  
  If you manually configured VCS, make sure you set the values of these environment variables to 1.

- **ONENODE**—Option for VCS to form a single node cluster. Valid values include:
  1—Indicates that VCS is started as a single-node cluster.
  0—Indicates that VCS is not set to form a single-node cluster.

Note the following information about the VCS configuration file after installing and configuring VCS:

- The cluster definition includes the cluster information that you provided during the configuration. This definition includes the cluster name, cluster address, and the names of users and administrators of the cluster.

  Notice that the cluster has an attribute UserNames. The installvcs program creates a user "admin" whose password is encrypted; the word "password" is the default password.

- If you set up the optional I/O fencing feature for VCS, then the UseFence = SCSI3 attribute is present.

- If you configured the cluster in secure mode, the main.cf includes "SecureClus = 1" cluster attribute.

- The installvcs program creates the ClusterService service group if you configured the virtual IP, SMTP, SNMP, or global cluster options.

  The service group also has the following characteristics:

  - The group includes the IP and NIC resources.
  - The service group also includes the notifier resource configuration, which is based on your input to installvcs program prompts about notification.
  - The installvcs program also creates a resource dependency tree.
  - If you set up global clusters, the ClusterService service group contains an Application resource, wac (wide-area connector). This resource’s attributes...
contain definitions for controlling the cluster in a global cluster environment.
Refer to the *Veritas Cluster Server Administrator's Guide* for information about managing VCS global clusters.

Refer to the *Veritas Cluster Server Administrator's Guide* to review the configuration concepts, and descriptions of main.cf and types.cf files for Linux systems.

**Sample main.cf file for VCS clusters**

The following sample main.cf file is for a cluster in secure mode.

```
include "types.cf"
include "OracleTypes.cf"
include "OracleASMTypes.cf"
include "Db2udbTypes.cf"
include "SybaseTypes.cf"

cluster vcs_cluster2 {
  UserNames = { admin = cDRpdxPmHpzS, smith = dKLhKJkHLh }
  ClusterAddress = "192.168.1.16"
  Administrators = { admin, smith }
  CounterInterval = 5
  SecureClus = 1
}

system sys1 {
}

system sys2 {
}

group ClusterService {
  SystemList = { sys1 = 0, sys2 = 1 }
  UserStrGlobal = "LocalCluster@https://10.182.2.76:8443;"
  AutoStartList = { sys1, sys2 }
  OnlineRetryLimit = 3
  OnlineRetryInterval = 120
}

IP webip {
  Device = eth0
```
Address = "192.168.1.16"
NetMask = "255.255.240.0"
)

NIC csgnic (  
  Device = eth0
  NetworkHosts = { "192.168.1.17", "192.168.1.18" }  
)

NotifierMngr ntfr (  
  SnmpConsoles = { "sys5" = Error, "sys4" = SevereError }  
  SmtpServer = "smtp.example.com"
  SmtpRecipients = { "ozzie@example.com" = Warning,
                   "harriet@example.com" = Error }  
)

webip requires csgnic
  ntfr requires csgnic

  // resource dependency tree
  //
  //  group ClusterService
  //    {  
  //      NotifierMngr ntfr
  //      {
  //        NIC csgnic
  //      }
  //  }

Sample main.cf file for global clusters

If you installed VCS with the Global Cluster option, note that the ClusterService
group also contains the Application resource, wac. The wac resource is required
to control the cluster in a global cluster environment.

  .
  .

group ClusterService (  
  SystemList = { sys1 = 0, sys2 = 1 }  
  UserStrGlobal = "LocalCluster@https://10.182.2.78:8443;"
  AutoStartList = { sys1, sys2 }  
  OnlineRetryLimit = 3  
  OnlineRetryInterval = 120
In the following main.cf file example, bold text highlights global cluster specific entries.

```plaintext
include "types.cf"

cluster vcs03 {
    ClusterAddress = "10.182.13.50"
    SecureClus = 1
}

system sysA {
}

system sysB {
}

system sysC {
}

group ClusterService {
    SystemList = { sysA = 0, sysB = 1, sysC = 2 }
    AutoStartList = { sysA, sysB, sysC }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
}

Application wac {
    StartProgram = "/opt/VRTSvcs/bin/wacstart -secure"
    StopProgram = "/opt/VRTSvcs/bin/wacstop"
    MonitorProcesses = { "/opt/VRTSvcs/bin/wac -secure" }
    RestartLimit = 3
}
```
IP gcoip {
  Device = eth0
  Address = "10.182.13.50"
  NetMask = "255.255.240.0"
}

NIC csgnic {
  Device = eth0
  NetworkHosts = { "10.182.13.1" }
}

NotifierMngr ntfr {
  SnmpConsoles = { sys4" = SevereError }  
  SmtpServer = "smtp.example.com"
  SmtpRecipients = { "ozzie@example.com" = SevereError }
}

gcoip requires csgnic
ntfr requires csgnic
wac requires gcoip

  // resource dependency tree
  //
  //   group ClusterService
  //   {
  //     NotifierMngr ntfr
  //     {
  //       NIC csgnic
  //     }
  //   }
  // Application wac
  //   {
  //     IP gcoip
  //     {
  //       NIC csgnic
  //     }
  //   }
  // }
## About I/O fencing configuration files

Table E-4 lists the I/O fencing configuration files.

### Table E-4  I/O fencing configuration files

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/etc/sysconfig/vxfen</code></td>
<td>This file stores the start and stop environment variables for I/O fencing:</td>
</tr>
<tr>
<td></td>
<td>- VXFEN_START—Defines the startup behavior for the I/O fencing module after a system reboot. Valid values include:</td>
</tr>
<tr>
<td></td>
<td>1—Indicates that I/O fencing is enabled to start up.</td>
</tr>
<tr>
<td></td>
<td>0—Indicates that I/O fencing is disabled to start up.</td>
</tr>
<tr>
<td></td>
<td>- VXFEN_STOP—Defines the shutdown behavior for the I/O fencing module during a system shutdown. Valid values include:</td>
</tr>
<tr>
<td></td>
<td>1—Indicates that I/O fencing is enabled to shut down.</td>
</tr>
<tr>
<td></td>
<td>0—Indicates that I/O fencing is disabled to shut down.</td>
</tr>
<tr>
<td></td>
<td>The installer sets the value of these variables to 1 at the end of VCS configuration.</td>
</tr>
<tr>
<td></td>
<td>If you manually configured VCS, you must make sure to set the values of these environment variables to 1.</td>
</tr>
<tr>
<td><code>/etc/vxfendg</code></td>
<td>This file includes the coordinator disk group information.</td>
</tr>
<tr>
<td></td>
<td>This file is not applicable for server-based fencing.</td>
</tr>
</tbody>
</table>
# Table E-4 I/O fencing configuration files (continued)

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/vxfenmode</td>
<td>This file contains the following parameters:</td>
</tr>
<tr>
<td></td>
<td>■ vxfen_mode</td>
</tr>
<tr>
<td></td>
<td>■ scsi3—For disk-based fencing</td>
</tr>
<tr>
<td></td>
<td>■ customized—For server-based fencing</td>
</tr>
<tr>
<td></td>
<td>■ disabled—To run the I/O fencing driver but not do any fencing operations.</td>
</tr>
<tr>
<td></td>
<td>■ vxfen_mechanism</td>
</tr>
<tr>
<td></td>
<td>This parameter is applicable only for server-based fencing. Set the value as cps.</td>
</tr>
<tr>
<td></td>
<td>■ scsi3_disk_policy</td>
</tr>
<tr>
<td></td>
<td>■ dmp—Configure the vxfen module to use DMP devices</td>
</tr>
<tr>
<td></td>
<td>The disk policy is dmp by default. If you use iSCSI devices, you must set the disk policy as dmp.</td>
</tr>
<tr>
<td></td>
<td>■ raw—Configure the vxfen module to use the underlying raw character devices</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must use the same SCSI-3 disk policy on all the nodes.</td>
</tr>
<tr>
<td></td>
<td>■ security</td>
</tr>
<tr>
<td></td>
<td>This parameter is applicable only for server-based fencing.</td>
</tr>
<tr>
<td></td>
<td>1—Indicates that communication with the CP server is in secure mode. This setting is the default.</td>
</tr>
<tr>
<td></td>
<td>0—Indicates that communication with the CP server is in non-secure mode.</td>
</tr>
<tr>
<td></td>
<td>■ List of coordination points</td>
</tr>
<tr>
<td></td>
<td>This list is required only for server-based fencing configuration.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ single_cp</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ autoseed_gab_timeout</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>-1—Turns the GAB auto-seed feature off. This setting is the default.</td>
</tr>
</tbody>
</table>
Table E-4  I/O fencing configuration files (continued)

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
</table>
| /etc/vxfentab | When I/O fencing starts, the vxfen startup script creates this /etc/vxfentab file on each node. The startup script uses the contents of the /etc/vxfendg and /etc/vxfenmode files. Any time a system is rebooted, the fencing driver reinitializes the vxfentab file with the current list of all the coordinator points.  
  **Note:** The /etc/vxfentab file is a generated file; do not modify this file.  
  For disk-based I/O fencing, the /etc/vxfentab file on each node contains a list of all paths to each coordinator disk 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:  
  - **Raw disk:**
    ```
    /dev/sdx  HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6
    00A0B8000215A5D000006804E795D075
    /dev/sdy  HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6
    00A0B8000215A5D000006814E795D076
    /dev/sdz  HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6
    00A0B8000215A5D000006824E795D077
    ```
  - **DMP disk:**
    ```
    /dev/vx/rdmp/sdx3  HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6
    00A0B8000215A5D000006804E795D0A3
    /dev/vx/rdmp/sdy3  HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6
    00A0B8000215A5D000006814E795D0B3
    /dev/vx/rdmp/sdz3  HITACHI%5F1724-100%20%20FAStT%5FDISKS%5F6
    00A0B8000215A5D000006824E795D0C3
    ```
  For server-based fencing, the /etc/vxfentab file also includes the security settings information. 
  For server-based fencing with single CP server, the /etc/vxfentab file also includes the single_cp settings information.

---

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 387.
The following are example main.cf files for a CP server that is hosted on a single node, and a CP server that is hosted on an SFHA cluster.

- The main.cf file for a CP server that is hosted on a single node:
  See “Sample main.cf file for CP server hosted on a single node that runs VCS” on page 382.

- The main.cf file for a CP server that is hosted on an SFHA cluster:
  See “Sample main.cf file for CP server hosted on a two-node SFHA cluster” on page 384.

Note: The CP server supports Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with VCS clusters (application clusters). The example main.cf files use IPv4 addresses.

Sample main.cf file for CP server hosted on a single node that runs VCS

The following is an example of a single CP server node main.cf.

For this CP server single node main.cf, note the following values:

- Cluster name: cps1
- Node name: 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 = eth0
    Address = "10.209.3.1"
    NetMask = "255.255.252.0"
}

IP cpsvip2 {
    Critical = 0
    Device @cps1 = eth1
    Address = "10.209.3.2"
    NetMask = "255.255.252.0"
}

NIC cpsnic1 {
    Critical = 0
    Device @cps1 = eth0
    PingOptimize = 0
    NetworkHosts @cps1 = { "10.209.3.10"
}

NIC cpsnic2 {
    Critical = 0
    Device @cps1 = eth1
    PingOptimize = 0
}

Process vxcpserv {
    PathName = "/opt/VRTScps/bin/vxcpserv"
    ConfInterval = 30
    RestartLimit = 3
}

Quorum quorum {
    QuorumResources = { cpsvip1, cpsvip2 }
}
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

```bash
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 = eth0
    Device @cps2 = eth0
    Address = "10.209.81.88"
    NetMask = "255.255.252.0"
}

IP cpsvip2 {
    Critical = 0
    Device @cps1 = eth1
    Device @cps2 = eth1
    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 = eth0
    Device @cps2 = eth0
    PingOptimize = 0
    NetworkHosts @cps1 = { "10.209.81.10" }
}

NIC cpsnic2 {
    Critical = 0
    Device @cps1 = eth1
    Device @cps2 = eth1
    PingOptimize = 0
}

Process vxcpser (  
    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
vxcpser requires cpsmount
vxcpser requires quorum

// resource dependency tree
//
// group CPSSG
// {
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.

```bash
## 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
```
Sample configuration files for CP server
Installing VCS on a single node

This appendix includes the following topics:

■ About installing VCS on a single node
■ Creating a single-node cluster using the installer program
■ Creating a single-node cluster manually
■ Setting the path variable for a manual single node installation
■ Installing VCS software manually on a single node
■ Modifying the startup files
■ Configuring VCS
■ Verifying single-node operation

About installing VCS on a single node

You can install VCS 6.0.2 on a single node. You can subsequently add another node to the single-node cluster to form a multinode cluster. You can also prepare a single node cluster for addition into a multi-node cluster. Single node clusters can be used for testing as well.

You can install VCS onto a single node using the installer program or you can add it manually.

See “Creating a single-node cluster using the installer program” on page 390.
See “Creating a single-node cluster manually” on page 391.
Creating a single-node cluster using the installer program

Table F-1 specifies the tasks that are involved to install VCS on a single node using the installer program.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare for installation.</td>
<td>See “Preparing for a single node installation” on page 390.</td>
</tr>
<tr>
<td>Install the VCS software on the system using the installer.</td>
<td>See “Starting the installer for the single node cluster” on page 390.</td>
</tr>
</tbody>
</table>

Preparing for a single node installation

You can use the installer program to install a cluster on a single system for either of the two following purposes:

- To prepare the single node cluster to join a larger cluster
- To prepare the single node cluster to be a stand-alone single node cluster

When you prepare it to join a larger cluster, enable it with LLT and GAB. For a stand-alone cluster, you do not need to enable LLT and GAB.

For more information about LLT and GAB:

See “About LLT and GAB” on page 23.

Starting the installer for the single node cluster

When you install VCS on a single system, follow the instructions in this guide for installing VCS using the product installer.

During the installation, you need to answer two questions specifically for single node installations. When the installer asks:

```
Enter the system names separated by spaces on which to install VCS[q,?]
```

Enter a single system name. While you configure, the installer asks if you want to enable LLT and GAB:

```
If you plan to run VCS on a single node without any need for adding cluster node online, you have an option to proceed
```
without starting GAB and LLT.
Starting GAB and LLT is recommended.
Do you want to start GAB and LLT? [y,n,q,?] (y)

Answer n if you want to use the single node cluster as a stand-alone cluster.
Answer y if you plan to incorporate the single node cluster into a multi-node cluster in the future.
Continue with the installation.

Creating a single-node cluster manually

Table F-2 specifies the tasks that you need to perform to install VCS on a single node.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the PATH variable</td>
<td>See “Setting the path variable for a manual single node installation” on page 391.</td>
</tr>
<tr>
<td>Install the VCS software manually and add a license key</td>
<td>See “Installing VCS software manually on a single node” on page 392.</td>
</tr>
<tr>
<td>Remove any LLT or GAB configuration files and rename LLT and GAB startup files.</td>
<td>A single-node cluster does not require the node-to-node communication service, LLT, or the membership communication service, GAB.</td>
</tr>
<tr>
<td>Modify the VCS startup file for single-node operation.</td>
<td>See “Modifying the startup files” on page 392.</td>
</tr>
<tr>
<td>Create and modify the VCS configuration files.</td>
<td>See “Configuring VCS” on page 392.</td>
</tr>
<tr>
<td>Start VCS and verify single-node operation.</td>
<td>See “Verifying single-node operation” on page 392.</td>
</tr>
</tbody>
</table>

Setting the path variable for a manual single node installation

Set the path variable.
See “Setting the PATH variable” on page 66.

Installing VCS software manually on a single node

Install the VCS 6.0.2 RPMs manually and install the license key.
Refer to the following sections:
- See “Installing VCS software manually” on page 195.
- See “Adding a license key for a manual installation” on page 199.

Modifying the startup files

Modify the VCS startup file /etc/sysconfig/vcs as follows:
Change the line:

```
ONENODE=no
```
To:

```
ONENODE=yes
```

Configuring VCS

You now need to configure VCS.
See “Configuring VCS manually” on page 207.

Verifying single-node operation

After successfully creating a single-node cluster, start VCS and verify the cluster.
To verify single-node cluster

1. Bring up VCS manually as a single-node cluster using `hastart` with the `-onenode` option:

   ```
   # hastart -onenode
   ```

2. Verify that the `had` and `hashadow` daemons are running in single-node mode:

   ```
   # ps -ef | grep had
   root  285  1 0 14:49:31 ?  0:02 /opt/VRTSvcs/bin/had -onenode
   root  288  1 0 14:49:33 ?  0:00 /opt/VRTSvcs/bin/hashadow
   ```
Configuring LLT over UDP

This appendix includes the following topics:

- Using the UDP layer for LLT
- Manually configuring LLT over UDP using IPv4
- Manually configuring LLT over UDP using IPv6
- LLT over UDP sample /etc/llttab

Using the UDP layer for LLT

VCS 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/llttab explicitly depending on the subnet for each link.
Make sure that each NIC has an IP address that is configured before configuring LLT.

- Make sure that each link has a unique not well-known UDP port.

- Set the broadcast address correctly for direct-attached (non-routed) links.
  
  The broadcast address is set explicitly for each link in the following example.

- 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.

Broadcast address in the /etc/llttab file

- 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 udp - udp  50000  -  192.168.9.1  192.168.9.255
link link2 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 udp - udp  50000  -  192.168.9.2  192.168.9.255
link link2 udp - udp  50001  -  192.168.10.2  192.168.10.255
```

Verify the subnet mask using the ifconfig command to ensure that the two links are on separate subnets.
The link command in the /etc/llttab file

Review the link command information in this section for the /etc/llttab file. See the following information for sample configurations:

- See “Sample configuration: direct-attached links” on page 397.
- See “Sample configuration: links crossing IP routers” on page 399.

Table G-1 describes the fields of the link command that are shown in the /etc/llttab file examples. Note that some of the fields differ from the command for standard LLT links.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag-name</td>
<td>A unique string that is used as a tag by LLT; for example link1, link2,...</td>
</tr>
<tr>
<td>device</td>
<td>The device path of the UDP protocol; for example udp.</td>
</tr>
<tr>
<td></td>
<td>A placeholder string. On other Unix platforms like Solaris or HP, this entry points to a device file (for example, /dev/udp). Linux does not have devices for protocols. So this field is ignored.</td>
</tr>
<tr>
<td>node-range</td>
<td>Nodes using the link. &quot;-&quot; indicates all cluster nodes are to be configured for this link.</td>
</tr>
<tr>
<td>link-type</td>
<td>Type of link; must be &quot;udp&quot; for LLT over UDP.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Unique UDP port in the range of 49152-65535 for the link.</td>
</tr>
<tr>
<td></td>
<td>See “Selecting UDP ports” on page 396.</td>
</tr>
<tr>
<td>MTU</td>
<td>&quot;-&quot; 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.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the link on the local node.</td>
</tr>
</tbody>
</table>
| bcast-address | ■ For clusters with enabled broadcasts, specify the value of the subnet broadcast address.  
            | ■ "-" is the default for clusters spanning routers.                          |

The set-addr command in the /etc/llttab file

The set-addr command in the /etc/llttab file is required when the broadcast feature of LLT is disabled, such as when LLT must cross IP routers.

See “Sample configuration: links crossing IP routers” on page 399.
Table G-2 describes the fields of the set-addr command.

Table G-2  Field description for set-addr command in /etc/littab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-id</td>
<td>The ID of the cluster node; for example, 0.</td>
</tr>
<tr>
<td>link tag-name</td>
<td>The string that LLT uses to identify the link; for example link1, link2,....</td>
</tr>
<tr>
<td>address</td>
<td>IP address assigned to the link for the peer node.</td>
</tr>
</tbody>
</table>

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:

```bash
# netstat -au | more
```

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the /etc/services file, its associated name is displayed rather than the port number in the output.

Configuring the netmask for LLT

For nodes on different subnets, set the netmask so that the nodes can access the subnets in use. Run the following command and answer the prompt to set the netmask:
# ifconfig interface_name netmask netmask

For example:

- For the first network interface on the node sys1:
  
  IP address=192.168.9.1, Broadcast address=192.168.9.255, Netmask=255.255.255.0

  For the first network interface on the node sys2:
  
  IP address=192.168.9.2, Broadcast address=192.168.9.255, Netmask=255.255.255.0

- For the second network interface on the node sys1:
  
  IP address=192.168.10.1, Broadcast address=192.168.10.255, Netmask=255.255.255.0

  For the second network interface on the node sys2:
  
  IP address=192.168.10.2, Broadcast address=192.168.10.255, Netmask=255.255.255.0

### Configuring the broadcast address for LLT

For nodes on different subnets, set the broadcast address in /etc/llttab depending on the subnet that the links are on.

An example of a typical /etc/llttab file when nodes are on different subnets. Note the explicitly set broadcast address for each link.

```bash
# cat /etc/llttab
set-node nodexyz
set-cluster 100

link link1 udp - udp 50000 - 192.168.30.1 192.168.30.255
link link2 udp - udp 50001 - 192.168.31.1 192.168.31.255
```

### Sample configuration: direct-attached links

Figure G-1 depicts a typical configuration of direct-attached links employing LLT over UDP.
The configuration that the /etc/llttab file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT broadcasts requests peer nodes to discover their addresses. So the addresses of peer nodes do not need to be specified in the /etc/llttab file using the set-addr command. For direct attached links, you do need to set the broadcast address of the links in the /etc/llttab file. Verify that the IP addresses and broadcast addresses are set correctly by using the `ifconfig -a` command.

```plaintext
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 udp - udp 50000 - 192.1.2.1 192.1.2.255
link link2 udp - udp 50001 - 192.1.3.1 192.1.3.255
```

The file for Node 1 resembles:

```plaintext
set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \ IP-address bcast-address
```

Figure G-1  A typical configuration of direct-attached links that use LLT over UDP
Sample configuration: links crossing IP routers

Figure G-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.

The configuration that the following /etc/llttab file represents for Node 1 has links crossing IP routers. Notice that IP addresses are shown for each link on each peer node. In this configuration broadcasts are disabled. Hence, the broadcast address does not need to be set in the link command of the /etc/llttab file.

set-node Node1
set-cluster 1

link link1 udp - udp 50000 - 192.1.2.2 -
link link2 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 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
```plaintext
set-addr 3 link1 192.1.7.3
set-addr 3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb 0
set-arp 0

The /etc/llttab file on Node 0 resembles:

set-node Node0
set-cluster 1

link link1 udp - udp 50000 - 192.1.1.1 -
link link2 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
```

**Manually configuring LLT over UDP using IPv6**

The following checklist is to configure LLT over UDP:

- For UDP6, the multicast address is set to ".".
- Make sure that each NIC has an IPv6 address that is configured before configuring LLT.
- Make sure the IPv6 addresses in the /etc/llttab files are consistent with the IPv6 addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port. See “Selecting UDP ports” on page 402.
- For the links that cross an IP router, disable multicast features and specify the IPv6 address of each link manually in the /etc/llttab file. See “Sample configuration: links crossing IP routers” on page 404.
The link command in the /etc/llttab file

Review the link command information in this section for the /etc/llttab file. See the following information for sample configurations:

- See “Sample configuration: direct-attached links” on page 402.
- See “Sample configuration: links crossing IP routers” on page 404.

Note that some of the fields in Table G-3 differ from the command for standard LLT links.

Table G-3 describes the fields of the link command that are shown in the /etc/llttab file examples.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag-name</td>
<td>A unique string that is used as a tag by LLT; for example link1, link2,....</td>
</tr>
<tr>
<td>device</td>
<td>The device name of the UDP protocol; for example udp6.</td>
</tr>
<tr>
<td>node-range</td>
<td>Nodes using the link. &quot;-&quot; indicates all cluster nodes are to be configured for this link.</td>
</tr>
<tr>
<td>link-type</td>
<td>Type of link; must be &quot;udp6&quot; for LLT over UDP.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Unique UDP port in the range of 49152-65535 for the link.</td>
</tr>
<tr>
<td></td>
<td>See “Selecting UDP ports” on page 402.</td>
</tr>
<tr>
<td>IPv6 address</td>
<td>IPv6 address of the link on the local node.</td>
</tr>
<tr>
<td>mcast-address</td>
<td>&quot;-&quot; is the default for clusters spanning routers.</td>
</tr>
</tbody>
</table>

The set-addr command in the /etc/llttab file

The set-addr command in the /etc/llttab file is required when the multicast feature of LLT is disabled, such as when LLT must cross IP routers.

See “Sample configuration: links crossing IP routers” on page 404.

Table G-4 describes the fields of the set-addr command.
Table G-4  Field description for set-addr command in /etc/llttab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-id</td>
<td>The ID of the cluster node; for example, 0.</td>
</tr>
<tr>
<td>link tag-name</td>
<td>The string that LLT uses to identify the link; for example link1, link2,...</td>
</tr>
<tr>
<td>address</td>
<td>IPv6 address assigned to the link for the peer node.</td>
</tr>
</tbody>
</table>

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 -au | more
```

Active Internet connections (servers and established)

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>*:32768</td>
<td><em>:</em></td>
<td><em>:</em></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>*:956</td>
<td><em>:</em></td>
<td><em>:</em></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>*:tftp</td>
<td><em>:</em></td>
<td><em>:</em></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>*:sunrpc</td>
<td><em>:</em></td>
<td><em>:</em></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>*:ipp</td>
<td><em>:</em></td>
<td><em>:</em></td>
</tr>
</tbody>
</table>

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 G-3 depicts a typical configuration of direct-attached links employing LLT over UDP.
Figure G-3  A typical configuration of direct-attached links that use LLT over UDP

The configuration that the /etc/llttab file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT uses IPv6 multicast requests for peer node address discovery. So the addresses of peer nodes do not need to be specified in the /etc/llttab file using the set-addr command. Use the ifconfig -a command to verify that the IPv6 address is set correctly.

set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \ 
  IP-address mcast-address
link link1 udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 - 
link link1 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
Sample configuration: links crossing IP routers

Figure G-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.

The configuration that the following `/etc/llttab` file represents for Node 1 has links crossing IP routers. Notice that IPv6 addresses are shown for each link on each peer node. In this configuration multicasts are disabled.

```bash
set-node Node1
set-cluster 1

link link1 udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 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 udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link2 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 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

**LLT over UDP sample /etc/llttab**

The following is a sample of LLT over UDP in the etc/llttab file.

set-node sys1
set-cluster clus1
link eth1 udp - udp 50000 - 192.168.10.1 -
link eth2 udp - udp 50001 - 192.168.11.1 -
link-lowpri eth0 udp - udp 50004 - 10.200.58.205 -
set-addr 1 eth1 192.168.10.2
set-addr 1 eth2 192.168.11.2
set-addr 1 eth0 10.200.58.206
set-bcasthb 0
set-arp 0
Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

- Setting up inter-system communication

Setting up inter-system communication

If you manually need to set up a communication mode, refer to these procedures. You must have root privilege to issue ssh or rsh commands on all systems in the cluster. If ssh is used to communicate between systems, it must be configured in a way such that it operates without requests for passwords or passphrases. Similarly, rsh must be configured in such a way to not prompt for passwords.

If system communication is not possible between systems using ssh or rsh, contact Symantec Support. See http://support.symantec.com.

__Warning__: The rsh and ssh commands to the remote systems, where VCS is to be installed, must not print any extraneous characters.

Setting up ssh on cluster systems

Use the Secure Shell (ssh) to install VCS on all systems in a cluster from a system outside of the cluster. Before you start the installation process, verify that ssh is configured correctly.

Use Secure Shell (ssh) to do the following:
Log on to another system over a network
Execute commands on a remote system
Copy files from one system to another

The `ssh` shell provides strong authentication and secure communications over channels. It is intended to replace `rlogin`, `rsh`, and `rcp`.

The Remote Shell (`rsh`) is disabled by default to provide better security. Use `ssh` for remote command execution.

## Configuring ssh

The procedure to configure `ssh` uses OpenSSH example file names and commands.

---

**Note:** You can configure `ssh` in other ways. Regardless of how `ssh` is configured, complete the last step in the example to verify the configuration.

---

### To configure ssh

1. Log on to the system from which you want to install VCS.
2. Generate a DSA key pair on this system by running the following command:
   ```bash
   # ssh-keygen -t dsa
   ```
3. Accept the default location of `~/.ssh/id_dsa`.
4. When the command prompts, enter a passphrase and confirm it.
5. Change the permissions of the `.ssh` directory by typing:
   ```bash
   # chmod 755 ~/.ssh
   ```
6. The file `~/.ssh/id_dsa.pub` contains a line that begins with `ssh-dss` and ends with the name of the system on which it was created. Copy this line to the `~/root/.ssh/authorized_keys2` file on all systems where you plan to install VCS.
   If the local system is part of the cluster, make sure to edit the `authorized_keys2` file on that system.
7. Run the following commands on the system where you are installing:
   ```bash
   # exec /usr/bin/ssh-agent $SHELL
   # ssh-add
   ```
   This step is shell-specific and is valid for the duration the shell is alive.
8. When the command prompts, enter your DSA passphrase.
You are ready to install VCS on several systems in one of the following ways:

- Run the installvcs program on any one of the systems
- Run the installvcs program on an independent system outside the cluster

To avoid running the ssh-agent on each shell, run the X-Window system and configure it so that you are not prompted for the passphrase. Refer to the documentation for your operating system for more information.

To verify that you can connect to the systems where you plan to install VCS, type:

```
# ssh -x -l root north ls
# ssh -x -l root south date
```

The commands should execute on the remote system without having to enter a passphrase or password.
Configuring the secure shell or the remote shell for communications

Setting up inter-system communication
Troubleshooting VCS installation

This appendix includes the following topics:

- What to do if you see a licensing reminder
- Restarting the installer after a failed connection
- Starting and stopping processes for the Veritas products
- Installer cannot create UUID for the cluster
- LLT startup script displays errors
- The vxfentsthdw utility fails when SCSI TEST UNIT READY command fails
- Issues during fencing startup on VCS cluster nodes set up for server-based fencing

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.
  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

### Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

### Starting and stopping processes for the Veritas products

After the installation and configuration is complete, the Veritas product installer starts the processes that are used by the installed products. You can use the product installer to stop or start the processes, if required.
To stop the processes

◆ Use the -stop option to stop the product installation script.
   
   For example, to stop the product’s processes, enter the following command:

   
   ```
   # ./installer -stop
   
   or
   
   # /opt/VRTS/install/installvcs program<version> -stop
   ```

   Where <version> is the specific release version.

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/installvcs program<version> -start
   ```

   Where <version> is the specific release version.

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 VCS configuration, upgrade, or when you add a node to the cluster using the installer.

Workaround: To start VCS, 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.

```
# /optVRTSvcs/bin/uuidconfig.pl -clus -configure nodeA nodeB ... nodeN
```

Where nodeA, nodeB, through nodeN are the names of the cluster nodes.

LLT startup script displays errors

If more than one system on the network has the same clusterid-nodeid pair and the same Ethernet sap/UDP port, then the LLT startup script displays error messages similar to the following:

```
LLT lltconfig ERROR V-14-2-15238 node 1 already exists in cluster 8383 and has the address - 00:18:8B:E4:DE:27
LLT lltconfig ERROR V-14-2-15241 LLT not configured, use -o to override this warning
LLT lltconfig ERROR V-14-2-15664 LLT could not configure any link
LLT lltconfig ERROR V-14-2-15245 cluster id 1 is already being used by nid 0 and has the address - 00:04:23:AC:24:2D
LLT lltconfig ERROR V-14-2-15664 LLT could not configure any link
```

Recommended action: Ensure that all systems on the network have unique clusterid-nodeid pair. You can use the lltdump -f device -D command to get the list of unique clusterid-nodeid pairs connected to the network. This utility is available only for LLT-over-ethernet.

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.

### Issues during fencing startup on VCS cluster nodes set up for server-based fencing

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description and resolution</th>
</tr>
</thead>
</table>
| **cpsadm command on the VCS cluster gives connection error** | If you receive a connection error message after issuing the `cpsadm` command on the VCS cluster, perform the following actions:  
- Ensure that the CP server is reachable from all the VCS cluster nodes.  
- Check that the VCS cluster nodes use the correct CP server virtual IP or virtual hostname and the correct port number.  
- Check the `/etc/vxfenmode` file.  
- Ensure that the running CP server is using the same virtual IP/virtual hostname and port number. |
| **Authorization failure** | Authorization failure occurs when the CP server’s nodes or users are not added in the CP server configuration. Therefore, fencing on the VCS cluster (client cluster) node is not allowed to access the CP server and register itself on the CP server. Fencing fails to come up if it fails to register with a majority of the coordination points.  
To resolve this issue, add the CP server node and user in the CP server configuration and restart fencing.  
See “Preparing the CP servers manually for use by the VCS cluster” on page 219. |
| **Authentication failure** | If you had configured secure communication between the CP server and the VCS cluster (client cluster) nodes, authentication failure can occur due to the following causes:  
- Symantec Product Authentication Services (AT) is not properly configured on the CP server and/or the VCS cluster.  
- The CP server and the VCS cluster nodes use different root brokers, and trust is not established between the authentication brokers: |
Troubleshooting VCS installation

Issues during fencing startup on VCS cluster nodes set up for server-based fencing
Sample VCS 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 J-1 on page 418.

- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:

- Two node campus cluster that served by remote CP server and 2 SCSI-3 disks:

- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:

Two unique client clusters served by 3 CP servers

Figure J-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 J-1**  Two unique client clusters served by 3 CP servers

Client cluster served by highly available CPS and 2 SCSI-3 disks

**Figure J-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 J-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 J-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 J-3  Two node campus cluster served by remote CP server and 2 SCSI-3

SITE 1

SITE 2

SITE 3

On the client cluster:

vxfenmode=customized
cps1=[VIP]:14250
cps1dg=vxfencordg

The coordinator disk group specified in /etc/vxfenmode should have one SCSI 3 disk from site 1 and another from site 2.

CPS database

/etc/VRadmin cpstab

Legends

Private Interconnects (GigE)
Public Links (GigE)
Dark Fiber
Connections
San 1 Connections
San 2 Connections
Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

Figure J-4 displays a configuration where multiple client clusters are being served by one highly available CP server and 2 local SCSI-3 LUNS (disks).

In the vxfenmode file on the client nodes, vxfenmode is set to customized with vxfen mechanism set to cps.

The two SCSI-3 disks are part of the disk group vxfencoorddg. The third coordination point is a CP server, hosted on an SFHA cluster, with its own shared database and coordinator disks.
Figure J-4  Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

The coordinator disk group specified in /etc/vxffenmode should have these 2 disks.
Sample VCS cluster setup diagrams for CP server-based I/O fencing

Configuration diagrams for setting up server-based I/O fencing
Compatibility issues when installing Veritas Cluster Server 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 ApplicationHA 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, if the existing VRTSsfmh binary is of a lower version, the installer automatically upgrades it.
- 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 upgrades VRTSsfmh.

Installing, uninstalling, or upgrading Storage Foundation products when ApplicationHA is already present

If you plan to install or upgrade Storage Foundation on systems where ApplicationHA has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where ApplicationHA is present, the installer does not consider VCS as an installed product even though it uses the bundled VRTSvcs RPM.
- When you install or upgrade Storage Foundation products where ApplicationHA is present, the installer does not allow the installation or upgrade for products that use VCS. The following products cannot be installed or upgrade: VCS, SFHA, SFCFS, SFCFSHA, SFRAC, SFCFSRAC or SYSYBASECE.
- When you install or upgrade Storage Foundation products where ApplicationHA is present, the installer allows the installation or upgrade of VM, FS, SF, or DMP.
- When you uninstall Storage Foundation products where ApplicationHA is present, the installer does not uninstall 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.
Compatibility issues when installing Veritas Cluster Server with other products
Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present
Symbols
/etc/llttab
  LLT directives 205

A
about
  global clusters 25
adding
  ClusterService group 211
  users 130
adding node
  to a one-node cluster 283
attributes
  UseFence 216

B
bundled agents
  types.cf file 207

C
cables
  cross-over Ethernet 295
cluster
  creating a single-node cluster
    installer 390
    manual 391
  four-node configuration 22
  removing a node from 307
  verifying operation 274
Cluster Manager 27
  installing Java Console 263
ClusterService group
  adding manually 211
cold start
  running VCS 24
commands
  gabconfig 207, 273
  hastart 306
  hastatus 274
  hastop 329
  commands (continued)
    hasys 275
    lltconfig 369
    lltstat 271
    vxdisksetup (initializing disks) 139
    vxlicinst 138, 199
    vxlicrep 137, 201
communication channels 23
communication disk 23
configuration files
  types.cf 207
configuring
  GAB 207
  hardware 34
  LLT
    manual 203
  private network 60
  rsh 63
  ssh 63, 407
  switches 60
configuring VCS
  adding users 130
  event notification 131–132
  global clusters 134
  required information 70
  script-based installer 116
  starting 117
controllers
  private Ethernet 60
coordinator disks
  DMP devices 30
  for I/O fencing 30
  setting up 214

D
data disks
  for I/O fencing 30
demo key 201
directives
  LLT 205
disk space
  directories 34
  required 34
disks
  adding and initializing 139
  coordinator 214
  testing with vxfentshdw 143
  verifying node access 144
documentation
  accessing 262

E
eeprom
  parameters 60
  Ethernet controllers 60, 295

F
  fibre channel 34

G
  GAB
    description 23
    manual configuration 207
    port membership information 273
    starting 210
    verifying 273
  gabconfig command 207, 273
    -a (verifying GAB) 273
  gabtab file
    creating 207
    verifying after installation 369
  global clusters 25
    configuration 134

H
  hardware
    configuration 22
    configuring network and storage 34
  hastart 306
  hastatus -summary command 274
  hastop command 329
  hasys -display command 275
  hubs 60
    independent 295

I
  I/O fencing
    checking disks 143
    setting up 213
    shared storage 143
  I/O fencing requirements
    non-SCSI-3 40
  installing
    manual 195
    post 135
    required disk space 34
    simulator 266
  installing VCS
    required information 70
  installvcs
    options 47
  installvcs prompts
    b 47
    n 47
    y 47

J
  Java Console 27
  installing 263
  installing on UNIX 263

K
  kernel.panic tunable
    setting 67

L
  license keys
    adding with vxlicinst 138, 199
    obtaining 54
    replacing demo key 138, 201
  licenses
    information about 137
    showing information 201
  links
    private network 369
  LLT
    description 23
    directives 205
    interconnects 68
    manual configuration 203
    starting 210
    verifying 271
LLT directives
- link 205
- link-lowpri 205
- set-cluster 205
- set-node 205
lltconfig command 369
llthosts file
  verifying after installation 369
lltstat command 271
llttab file
  verifying after installation 369

M
MAC addresses 60
main.cf file
  contents after installation 375
main.cf files 381
MANPATH variable
  setting 66
manual installation
  preparing 193
media speed 68
  optimizing 67
membership information 273
mounting
  software disc 68

N
network partition
  preexisting 24
  protecting against 22
Network partitions
  protecting against 23
network switches 60
NFS 21
non-SCSI-3 fencing
  manual configuration 231
  setting up 231
non-SCSI-3 I/O fencing
  requirements 40
non-SCSI3 fencing
  setting up 156
  using installvcs program 156

O
optimizing
  media speed 67

overview
  VCS 21

P
parameters
  eeprom 60
PATH variable
  setting 66
  VCS commands 270
persistent reservations
  SCSI-3 63
port a
  membership 273
port h
  membership 273
port membership information 273
preparing
  manual installation 193
prerequisites
  uninstalling 319
private network
  configuring 60

R
RAM
  installation requirement 34
removing a system from a cluster 307
requirements
  Ethernet controllers 34
  fibre channel 34
  hardware 34
  RAM Ethernet controllers 34
  SCSI host bus adapter 34
response files 48
rsh 117, 407
  configuration 63

S
script-based installer
  VCS configuration overview 116
SCSI host bus adapter 34
SCSI-3
  persistent reservations 63
SCSI-3 persistent reservations
  verifying 213
seeding 24
  automatic 24
  manual 24
setting
  kernel.panic tunable 67
  MANPATH variable 66
  PATH variable 66
simulator
  installing 266
single-node cluster
  adding a node to 283
single-system cluster
  creating 390–391
  modifying startup files 392
SMTP email notification 131
SNMP trap notification 132
ssh 117, 407
  configuration 63
  configuring 407
starting configuration
  installvcs program 117
  Veritas product installer 117
starting VCS after manual upgrade 209
starting VCS after rpm -i 210
storage
  fully shared vs. distributed 22
  shared 22
switches 60
system communication using rsh
  ssh 407
system state attribute value 274

T
types.cf 207
  bundled agents 207
types.cf file 207

U
uninstalling
  prerequisites 319

V
variables
  MANPATH 66
  PATH 66
VCS
  basics 21
  command directory path variable 270
  configuration files
    main.cf 373
    configuring 116
  (continued)
    coordinator disks 214
    documentation 262
    manually installing 195
    notifications 25
    replicated states on each system 22
    starting 209–210
VCS features 25
VCS installation
  verifying
    cluster operations 270
    GAB operations 270
    LLT operations 270
VCS notifications
  SMTP notification 25
  SNMP notification 25
verifying
  NIC configuration 136
  Veritas Operations Manager 27
vxdisksetup command 139
vxlicinst command 138, 199
vxlicrep command 137, 201