Veritas™ Cluster Server
Installation Guide

Solaris

6.0
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
Document version: 6.0.0

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

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

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

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

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

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

Symantec’s support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

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

**Licensing and registration**

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

www.symantec.com/business/support/

**Customer service**

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

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

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

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
Section 1 Installation overview and planning

Chapter 1 Introducing VCS

About Veritas Cluster Server .............................. 23
About VCS basics .............................................. 23
  About multiple nodes ................................... 24
  About shared storage .................................... 24
About LLT and GAB ........................................ 25
About network channels for heartbeating .......... 25
About preexisting network partitions .............. 26
About VCS seeding ......................................... 26
About VCS features ........................................ 27
  About VCS notifications ............................... 27
  About global clusters ................................. 27
  About I/O fencing ...................................... 27
About VCS optional components ...................... 28
  About Veritas Operations Manager .............. 29
  About Cluster Manager (Java Console) .......... 29
  About VCS Simulator .................................. 29
Symantec Operations Readiness Tools .......... 30
About configuring VCS clusters for data integrity .... 30
  About I/O fencing for VCS in virtual machines that do not support
    SCSI-3 PR ........................................... 31
  About I/O fencing components .................... 31
  About preferred fencing .............................. 33

Chapter 2 System requirements

Important preinstallation information for VCS .......... 35
Hardware requirements for VCS .......................... 36
Disk space requirements ................................... 36
Supported operating systems ........................... 37
Supported software for VCS .............................. 37
Chapter 3 Planning to install VCS .............................................................. 43
VCS installation methods ........................................................................ 43
   About the VCS installation program .................................................. 44
   About the Web-based installer ......................................................... 46
   About response files ....................................................................... 47
Typical VCS cluster setup models ............................................................ 48
   Typical configuration of two-node VCS cluster ................................ 48
   Typical configuration of VCS clusters in secure mode .................... 49
   Typical configuration of VOM-managed VCS clusters ................... 50

Chapter 4 Licensing VCS ....................................................................... 53
About Veritas product licensing .............................................................. 53
Obtaining VCS license keys ................................................................. 54
Installing Veritas product license keys .................................................. 55

Section 2 Preinstallation tasks ............................................................. 57

Chapter 5 Preparing to install VCS ........................................................ 59
About preparing to install VCS ............................................................. 59
Performing preinstallation tasks .......................................................... 59
   Setting up the private network .......................................................... 60
   About using ssh or rsh with the Veritas installer ............................. 63
   Setting up shared storage ............................................................... 64
   Setting the PATH variable ............................................................. 68
   Setting the MANPATH variable ...................................................... 68
   Disabling the abort sequence on SPARC systems ......................... 69
   Optimizing LLT media speed settings on private NICs ................... 70
Guidelines for setting the media speed of the LLT interconnects ............ 70
Preparation zone environments ........................................................... 70
Mounting the product disc ................................................................. 71
Performing automated preinstallation check ..................................... 72
Reformatting VCS configuration files on a stopped cluster ............... 72
Getting your VCS installation and configuration information ready ................................................................. 73

Section 3

Installation using the script-based installer ................................................................. 81

Chapter 6

Installing VCS ........................................................................................................ 83
Installing VCS using the installer ........................................................................... 83
Installing language packages using the installer .................................................. 87

Chapter 7

Preparing to configure VCS ................................................................................ 89
About planning to configure I/O fencing ................................................................. 89
   Typical VCS cluster configuration with disk-based I/O fencing ......................... 92
   Typical VCS cluster configuration with server-based I/O fencing ..................... 93
Recommended CP server configurations ................................................................. 93
Setting up the CP server ....................................................................................... 96
Planning your CP server setup ............................................................................... 96
Installing the CP server using the installer ............................................................. 97
Configuring the CP server cluster in secure mode ............................................... 98
Setting up shared storage for the CP server database ........................................... 98
Configuring the CP server using the configuration utility .................................... 99
Configuring the CP server manually ................................................................... 109
Verifying the CP server configuration .................................................................. 111

Chapter 8

Configuring VCS .................................................................................................... 113
Overview of tasks to configure VCS using the script-based installer ....................... 113
Starting the software configuration ......................................................................... 114
Specifying systems for configuration ..................................................................... 115
Configuring the cluster name .................................................................................. 116
Configuring private heartbeat links ......................................................................... 116
Configuring the virtual IP of the cluster .................................................................. 119
Configuring the cluster in secure mode ................................................................... 121
Setting up trust relationships for your VCS cluster ................................................ 122
Configuring a secure cluster node by node ............................................................ 123
   Configuring the first node ................................................................................... 123
   Configuring the remaining nodes ....................................................................... 124
Completing the secure cluster configuration ........................................................... 125
Adding VCS users ........................................................................ 126
Configuring SMTP email notification ............................................. 127
Configuring SNMP trap notification ............................................... 129
Configuring global clusters .......................................................... 131
Completing the VCS configuration ................................................. 132
Verifying and updating licenses on the system ......................... 133
  Checking licensing information on the system ...................... 133
  Updating product licenses using vxlicinst .......................... 134

Chapter 9 Configuring VCS clusters for data integrity ............ 137
  Setting up disk-based I/O fencing using installvcs program ........ 137
  Initializing disks as VxVM disks .......................................... 137
  Configuring disk-based I/O fencing using installvcs program ....... 138
  Checking shared disks for I/O fencing ................................... 140
  Setting up server-based I/O fencing using installvcs program ...... 145
  Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installvcs program .................. 154
  Enabling or disabling the preferred fencing policy .................... 155

Section 4 Installation using the Web-based installer .......... 159

Chapter 10 Installing VCS .......................................................... 161
  Before using the Veritas Web-based installer ......................... 161
  Starting the Veritas Web-based installer ............................... 162
  Obtaining a security exception on Mozilla Firefox ................. 162
  Performing a pre-installation check with the Veritas Web-based installer .................................................. 163
  Installing VCS with the Web-based installer ......................... 163

Chapter 11 Configuring VCS ....................................................... 167
  Configuring VCS using the Web-based installer .................... 167
  Configuring VCS for data integrity using the Web-based installer ................................................................. 172
<table>
<thead>
<tr>
<th>Section 5</th>
<th>Installation using response files</th>
<th>177</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 12</td>
<td>Performing automated VCS installation</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>Installing VCS using response files</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>Response file variables to install VCS</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>Sample response file for installing VCS</td>
<td>182</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>Performing automated VCS configuration</td>
<td>185</td>
</tr>
<tr>
<td></td>
<td>Configuring VCS using response files</td>
<td>185</td>
</tr>
<tr>
<td></td>
<td>Response file variables to configure Veritas Cluster Server</td>
<td>186</td>
</tr>
<tr>
<td></td>
<td>Sample response file for configuring VCS</td>
<td>195</td>
</tr>
<tr>
<td>Chapter 14</td>
<td>Performing automated I/O fencing configuration for VCS</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>Configuring I/O fencing using response files</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>Response file variables to configure disk-based I/O fencing</td>
<td>198</td>
</tr>
<tr>
<td></td>
<td>Sample response file for configuring disk-based I/O fencing</td>
<td>199</td>
</tr>
<tr>
<td></td>
<td>Response file variables to configure server-based I/O fencing</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>Sample response file for configuring server-based I/O fencing</td>
<td>201</td>
</tr>
<tr>
<td></td>
<td>Response file variables to configure non-SCSI-3 server-based I/O fencing</td>
<td>202</td>
</tr>
<tr>
<td></td>
<td>Sample response file for configuring non-SCSI-3 server-based I/O fencing</td>
<td>203</td>
</tr>
<tr>
<td>Section 6</td>
<td>Manual installation</td>
<td>205</td>
</tr>
<tr>
<td>Chapter 15</td>
<td>Performing preinstallation tasks</td>
<td>207</td>
</tr>
<tr>
<td></td>
<td>Preparing for a manual installation</td>
<td>207</td>
</tr>
<tr>
<td></td>
<td>Requirements for installing VCS</td>
<td>207</td>
</tr>
<tr>
<td>Chapter 16</td>
<td>Manually installing VCS</td>
<td>209</td>
</tr>
<tr>
<td></td>
<td>About VCS manual installation</td>
<td>209</td>
</tr>
<tr>
<td></td>
<td>Installing VCS software manually</td>
<td>209</td>
</tr>
<tr>
<td></td>
<td>Viewing the list of VCS packages</td>
<td>210</td>
</tr>
<tr>
<td></td>
<td>Installing VCS packages for a manual installation</td>
<td>211</td>
</tr>
<tr>
<td></td>
<td>Installing language packages in a manual installation</td>
<td>212</td>
</tr>
<tr>
<td></td>
<td>Adding a license key for a manual installation</td>
<td>213</td>
</tr>
<tr>
<td></td>
<td>Copying the installation guide to each node</td>
<td>215</td>
</tr>
<tr>
<td></td>
<td>Installing using JumpStart</td>
<td>216</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Overview of JumpStart installation tasks</td>
<td>216</td>
<td></td>
</tr>
<tr>
<td>Generating the finish scripts</td>
<td>217</td>
<td></td>
</tr>
<tr>
<td>Preparing installation resources</td>
<td>217</td>
<td></td>
</tr>
<tr>
<td>Adding language pack information to the finish file</td>
<td>218</td>
<td></td>
</tr>
<tr>
<td>Using a Flash archive to install VCS and the operating system</td>
<td>219</td>
<td></td>
</tr>
<tr>
<td>Chapter 17 Manually configuring VCS</td>
<td>223</td>
<td></td>
</tr>
<tr>
<td>About configuring VCS manually</td>
<td>223</td>
<td></td>
</tr>
<tr>
<td>Configuring LLT manually</td>
<td>223</td>
<td></td>
</tr>
<tr>
<td>Setting up <code>/etc/llthosts</code> for a manual installation</td>
<td>224</td>
<td></td>
</tr>
<tr>
<td>Setting up <code>/etc/llttab</code> for a manual installation</td>
<td>224</td>
<td></td>
</tr>
<tr>
<td>About LLT directives in <code>/etc/llttab</code> file</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>Additional considerations for LLT for a manual installation</td>
<td>227</td>
<td></td>
</tr>
<tr>
<td>Configuring GAB manually</td>
<td>227</td>
<td></td>
</tr>
<tr>
<td>Configuring VCS manually</td>
<td>228</td>
<td></td>
</tr>
<tr>
<td>Configuring the cluster UUID when creating a cluster manually</td>
<td>229</td>
<td></td>
</tr>
<tr>
<td>Configuring VCS in single node mode</td>
<td>230</td>
<td></td>
</tr>
<tr>
<td>Starting LLT, GAB, and VCS after manual configuration</td>
<td>230</td>
<td></td>
</tr>
<tr>
<td>Modifying the VCS configuration</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>Configuring the ClusterService group</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>Chapter 18 Manually configuring the clusters for data integrity</td>
<td>233</td>
<td></td>
</tr>
<tr>
<td>Setting up disk-based I/O fencing manually</td>
<td>233</td>
<td></td>
</tr>
<tr>
<td>Identifying disks to use as coordinator disks</td>
<td>234</td>
<td></td>
</tr>
<tr>
<td>Setting up coordinator disk groups</td>
<td>234</td>
<td></td>
</tr>
<tr>
<td>Creating I/O fencing configuration files</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td>Modifying VCS configuration to use I/O fencing</td>
<td>236</td>
<td></td>
</tr>
<tr>
<td>Verifying I/O fencing configuration</td>
<td>238</td>
<td></td>
</tr>
<tr>
<td>Setting up server-based I/O fencing manually</td>
<td>238</td>
<td></td>
</tr>
<tr>
<td>Preparing the CP servers manually for use by the VCS cluster</td>
<td>239</td>
<td></td>
</tr>
<tr>
<td>Configuring server-based fencing on the VCS cluster manually</td>
<td>242</td>
<td></td>
</tr>
<tr>
<td>Configuring CoordPoint agent to monitor coordination points</td>
<td>248</td>
<td></td>
</tr>
<tr>
<td>Verifying server-based I/O fencing configuration</td>
<td>249</td>
<td></td>
</tr>
<tr>
<td>Setting up non-SCSI-3 fencing in virtual environments manually</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>Sample <code>/etc/vxfenmode</code> file for non-SCSI-3 fencing</td>
<td>252</td>
<td></td>
</tr>
</tbody>
</table>
Section 7  Upgrading VCS ................................................................. 257

Chapter 19  Planning to upgrade VCS .............................................. 259

  About upgrading to VCS 6.0 .......................................................... 259
  VCS supported upgrade paths ....................................................... 260
  Upgrading VCS in secure enterprise environments .................. 262

Chapter 20  Performing a typical VCS upgrade using the installer ......................................................... 265

  Before upgrading using the script-based or Web-based installer .... 265
  Upgrading VCS using the script-based installer ......................... 265
  Upgrading Veritas Cluster Server using the Veritas Web-based installer ......................................................... 267

Chapter 21  Performing a phased upgrade .......................................... 269

  About phased upgrade ............................................................... 269
  Prerequisites for a phased upgrade ......................................... 269
  Planning for a phased upgrade ................................................. 269
  Phased upgrade limitations ...................................................... 270
  Phased upgrade example ......................................................... 270
  Phased upgrade example overview ......................................... 271
  Performing a phased upgrade .................................................... 272
  Moving the service groups to the second subcluster ............... 272
  Upgrading the operating system on the first subcluster ........... 276
  Upgrading the first subcluster ............................................... 276
  Preparing the second subcluster ............................................. 278
  Activating the first subcluster ............................................... 283
  Upgrading the operating system on the second subcluster ....... 284
  Upgrading the second subcluster ............................................. 285
  Finishing the phased upgrade ................................................ 286

Chapter 22  Performing an automated VCS upgrade using response files ......................................................... 291

  Upgrading VCS using response files ......................................... 291
  Response file variables to upgrade VCS ..................................... 292
  Sample response file for upgrading VCS ................................... 293
Chapter 23  Performing a rolling upgrade ........................................ 295
   About rolling upgrades ................................................................. 295
   Performing a rolling upgrade using the installer ............................ 297
      Performing a rolling upgrade using the script-based installer .......... 297
   Performing a rolling upgrade of VCS using the Web-based installer .... 299

Chapter 24  Upgrading using Live Upgrade ...................................... 301
   About Live Upgrade .................................................................... 301
   Veritas Cluster Server exceptions for Live Upgrade ..................... 302
   Supported upgrade paths for Live Upgrade .................................. 302
   Before you upgrade VCS using Solaris Live Upgrade .................... 303
   Upgrading VCS and Solaris using Live Upgrade ............................. 306
      Creating a new boot environment on the alternate boot disk .............. 307
      Upgrading VCS using the installer for a Live Upgrade .................. 308
      Upgrading VCS manually .......................................................... 309
      Completing the Live Upgrade .................................................. 311
      Verifying Live Upgrade of VCS ............................................... 312
   Upgrading Solaris using Live Upgrade ......................................... 313
      Removing and reinstalling VCS using the installer ....................... 314
   Upgrading VCS using Live Upgrade ............................................ 315
   Administering boot environments .............................................. 315
      Reverting to the primary boot environment .................................. 316
      Switching the boot environment for Solaris SPARC .................... 316
      Switching the boot environment for Solaris x86-64 ..................... 317

Chapter 25  Upgrading the Solaris operating system .............................. 321
   Upgrading Solaris versions .......................................................... 321
   Upgrading Solaris on a node ....................................................... 321

Section 8  Post-installation tasks ..................................................... 327

Chapter 26  Performing post-installation tasks ................................... 329
   About enabling LDAP authentication for clusters that run in secure mode .......................................................... 329
      Enabling LDAP authentication for clusters that run in secure mode .......................................................... 331
   Accessing the VCS documentation ............................................. 337
Chapter 27  Installing or upgrading VCS components ................. 339

Installing the Java Console .................................................. 339
  Software requirements for the Java Console ....................... 339
  Hardware requirements for the Java Console ..................... 340
  Installing the Java Console on Solaris ............................... 340
  Installing the Java Console on a Windows system ............... 341
Upgrading the Java Console .................................................. 341
Installing VCS Simulator .................................................... 342
  Software requirements for VCS Simulator ......................... 342
  Installing VCS Simulator on Windows systems .................. 342
  Reviewing the installation .............................................. 343
Upgrading VCS Simulator .................................................... 344

Chapter 28  Verifying the VCS installation .................................. 345

About verifying the VCS installation ..................................... 345
About the cluster UUID ....................................................... 345
Verifying the LLT, GAB, and VCS configuration files .............. 346
Verifying LLT, GAB, and cluster operation ............................ 346
  Verifying LLT .................................................................. 347
  Verifying GAB .................................................................. 349
  Verifying the cluster ..................................................... 351
  Verifying the cluster nodes .......................................... 351
Performing a postcheck on a node ........................................ 354
  About using the postcheck option .................................... 354

Section 9  Uninstalling VCS ...................................................... 357

Chapter 29  Uninstalling VCS using the installer ....................... 359

Preparing to uninstall VCS .................................................. 359
Uninstalling VCS using the script-based installer .................. 360
  Removing VCS 6.0 packages ........................................... 360
  Running uninstallvcs from the VCS 6.0 disc ..................... 361
Uninstalling VCS with the Veritas Web-based installer .......... 361
Removing language packages using the uninstaller program .... 362
Removing the CP server configuration using the removal script .. 362
Chapter 30  Uninstalling VCS using response files ........................................... 365
Uninstalling VCS using response files .................................................... 365
Response file variables to uninstall VCS ............................................ 366
Sample response file for uninstalling VCS ........................................ 367

Chapter 31  Manually uninstalling VCS .................................................. 369
Removing VCS packages manually ...................................................... 369
Manually remove the CP server fencing configuration ...................... 372
Manually deleting cluster details from a CP server .......................... 372

Section 10  Adding and removing nodes .............................................. 375

Chapter 32  Adding a node to a single-node cluster .............................. 377
Adding a node to a single-node cluster ............................................. 377
Setting up a node to join the single-node cluster ............................. 378
Installing and configuring Ethernet cards for private network .............. 379
Configuring the shared storage ....................................................... 380
Bringing up the existing node ........................................................ 380
Installing the VCS software manually when adding a node to a single node cluster .................................................. 381
Creating configuration files ............................................................ 381
Starting LLT and GAB ................................................................. 381
Reconfiguring VCS on the existing node ........................................ 381
Verifying configuration on both nodes .......................................... 383

Chapter 33  Adding and removing cluster nodes .................................. 385
About adding and removing nodes .................................................... 385
Adding nodes using the VCS installer .............................................. 385
Adding a node using the Web-based installer ................................. 388
Manually adding a node to a cluster ................................................. 389
Setting up the hardware ............................................................... 389
Installing the VCS software manually when adding a node to the cluster .......................................................... 390
Setting up the node to run in secure mode ................................... 391
Configuring LLT and GAB when adding a node to the cluster ............... 394
Configuring I/O fencing on the new node ...................................... 397
Adding the node to the existing cluster ......................................... 400
Starting VCS and verifying the cluster ......................................... 401
Removing a node from a cluster .................................................... 401
Appendix E  Installing VCS on a single node ............................................. 471
  About installing VCS on a single node ............................................. 471
  Creating a single-node cluster using the installer program .................. 472
    Preparing for a single node installation ...................................... 472
    Starting the installer for the single node cluster .......................... 472
  Creating a single-node cluster manually ........................................ 473
  Setting the path variable for a manual single node installation .......... 473
  Installing VCS software manually on a single node .......................... 474
  Configuring VCS ......................................................................... 474
  Verifying single-node operation .................................................. 474

Appendix F  Configuring LLT over UDP .................................................. 475
  Using the UDP layer for LLT ......................................................... 475
    When to use LLT over UDP ......................................................... 475
  Manually configuring LLT over UDP using IPv4 ................................ 475
    Broadcast address in the /etc/llttab file .................................... 476
    The link command in the /etc/llttab file .................................... 477
    The set-addr command in the /etc/llttab file ............................... 477
    Selecting UDP ports ............................................................... 478
    Configuring the netmask for LLT ................................................ 479
    Configuring the broadcast address for LLT .................................. 479
    Sample configuration: direct-attached links .................................. 480
    Sample configuration: links crossing IP routers .............................. 482
  Manually configuring LLT over UDP using IPv6 ................................ 484
    The link command in the /etc/llttab file .................................... 485
    The set-addr command in the /etc/llttab file ................................ 486
    Selecting UDP ports ............................................................... 486
    Sample configuration: direct-attached links .................................. 487
    Sample configuration: links crossing IP routers .............................. 489
  LLT over UDP sample /etc/llttab .................................................. 491

Appendix G  Configuring the secure shell or the remote shell for communications .......................................................... 493
  Setting up inter-system communication ........................................... 493
    Setting up ssh on cluster systems .............................................. 493
    Configuring ssh ...................................................................... 494

Appendix H  Troubleshooting VCS installation ........................................ 499
  What to do if you see a licensing reminder ...................................... 499
  Restarting the installer after a failed connection ............................... 500
Installation overview and planning

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

This chapter includes the following topics:

■ About Veritas Cluster Server
■ About VCS basics
■ About VCS features
■ About VCS optional components
■ 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.
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 a seed. A seed 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 27.
- **VCS global clusters**
  - See “About global clusters” on page 27.
- **I/O fencing**
  - See “About I/O fencing” on page 27.

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. The installer installs the I/O fencing driver, VRTSvxfen, when you install VCS. 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 multiple clusters.
- In virtualized environments that do not support SCSI-3 PR, VCS supports non-SCSI-3 server-based I/O fencing.

See “About planning to configure I/O fencing” on page 89.

**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 29.

- **Cluster Manager (Java console)**  
  See “About Cluster Manager (Java Console)” on page 29.

- **VCS Simulator**  
  See About VCS Simulator on page 29.
About Veritas Operations Manager

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

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.

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/vcsm_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 clusters and VCS objects, including service groups, systems, resources, and resource types. You cannot manage the new features of this release using the Java Console.

See Veritas Cluster Server Administrator's Guide.

You can download the console from http://go.symantec.com/vcsm_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 on Windows, AIX, HP-UX, Linux, and Solaris operating systems. VCS Simulator also enables creating and testing global clusters.
You can administer VCS Simulator from the Java Console or from the command line.

To download VCS Simulator, go to http://go.symantec.com/vcsm_download.

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.

See “About planning to configure I/O fencing” on page 89.

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 154.

See “Setting up non-SCSI-3 fencing in virtual environments manually” on page 250.

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 32.
- Coordination points—Act as a global lock during membership changes
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 as follows:

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

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

See “Enabling or disabling the preferred fencing policy” on page 155.
Introducing VCS

About configuring VCS clusters for data integrity
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
  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

- 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 SPARC or x64 systems running Solaris 10 as appropriate.</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>
<tr>
<td>Disks</td>
<td>Typical VCS configurations require that shared disks support the applications that migrate between systems in the cluster. The VCS I/O fencing feature requires that all data and coordinator disks support SCSI-3 Persistent Reservations (PR). See “About planning to configure I/O fencing” on page 89.</td>
</tr>
<tr>
<td>Disk space</td>
<td>See “Disk space requirements” on page 36. <strong>Note:</strong> VCS may require more temporary disk space during installation than the specified disk space.</td>
</tr>
<tr>
<td>Ethernet controllers</td>
<td>In addition to the built-in public Ethernet controller, VCS requires at least one more Ethernet interface per system. Symantec recommends two additional network interfaces for private interconnects. You can also configure aggregated interfaces. Symantec recommends that you turn off the spanning tree algorithm on the switches used to connect private network interfaces.</td>
</tr>
<tr>
<td>Fibre Channel or SCSI host bus adapters</td>
<td>Typical VCS configuration requires at least one SCSI or Fibre Channel Host Bus Adapter per system for shared data disks.</td>
</tr>
<tr>
<td>RAM</td>
<td>Each VCS node requires at least 1024 megabytes.</td>
</tr>
</tbody>
</table>

**Disk space requirements**

Before installing your products, confirm that your system has enough free disk space.
Use the "Perform a Preinstallation Check" (P) menu for the Web-based installer or the -precheck option of the script-based installer to determine whether there is sufficient space.

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

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

```
# ./installvcs -precheck
```

**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:

- Veritas Storage Foundation (SF): Veritas Volume Manager (VxVM) with Veritas File System (VxFS)
  - VCS 6.0 supports the following versions of SF:
    - SF 6.0
      - VxVM 6.0 with VxFS 6.0
    - SF5.1SP1
      - VxVM 5.1SP1 with VxFS 5.1SP1

*Note:* VCS supports the previous and the current versions of SF 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 38.
- CP servers
  - See “CP server requirements” on page 38.
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.

See “Non-SCSI-3 I/O fencing requirements” on page 41.

### Coordinator disk requirements for I/O fencing

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

- For disk-based I/O fencing, you must have three coordinator disks.
- The coordinator disks can be raw devices, DMP devices, or iSCSI devices.
- Each of the coordinator disks must use a physically separate disk or LUN. Symantec recommends using the smallest possible LUNs for coordinator disks.
- Each of the coordinator disks should exist on a different disk array, if possible.
- The coordinator disks must support SCSI-3 persistent reservations.
- Symantec recommends using hardware-based mirroring for coordinator disks.
- Coordinator disks must not be used to store data or must not be included in disk groups that store user data.
- Coordinator disks cannot be the special devices that array vendors use. For example, you cannot use EMC gatekeeper devices as coordinator disks.

### CP server requirements

VCS 6.0 clusters (application clusters) support coordination point servers (CP servers) which are hosted on the following VCS and SFHA versions:

- VCS 6.0, 5.1SP1, or 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, 5.1SP1, or 5.1 cluster
Warning: Before you upgrade 5.1 CP server nodes to use VCS or SFHA 6.0, you must upgrade all the application clusters that use this CP server to version 6.0. 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 36.

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>
<thead>
<tr>
<th>Hardware required</th>
<th>Description</th>
</tr>
</thead>
</table>
| Disk space         | To host the CP server on a VCS cluster or SFHA cluster, each host requires the following file system space:  
  - 550 MB in the /opt directory (additionally, the language pack requires another 15 MB)  
  - 300 MB in /usr  
  - 20 MB in /var  
  - 10 MB in /etc (for the CP server database) |
| Storage            | When CP server is hosted on an SFHA cluster, there must be shared storage between the CP servers. |
| RAM                | Each CP server requires at least 512 MB. |
Table 2-2 CP server hardware requirements (continued)

<table>
<thead>
<tr>
<th>Hardware required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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</th>
<th>Operating system and version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP server hosted on a VCS</td>
<td>CP server supports any of the following operating systems:</td>
</tr>
<tr>
<td>single-node cluster or on an SFHA cluster</td>
<td>■ AIX 6.1 and 7.1</td>
</tr>
<tr>
<td></td>
<td>■ HP-UX 11i v3</td>
</tr>
<tr>
<td></td>
<td>■ Linux:</td>
</tr>
<tr>
<td></td>
<td>■ RHEL 5</td>
</tr>
<tr>
<td></td>
<td>■ RHEL 6</td>
</tr>
<tr>
<td></td>
<td>■ SLES 10</td>
</tr>
<tr>
<td></td>
<td>■ SLES 11</td>
</tr>
<tr>
<td></td>
<td>■ Solaris 10</td>
</tr>
<tr>
<td></td>
<td>Review other details such as supported operating system levels and architecture for the supported operating systems.</td>
</tr>
<tr>
<td></td>
<td>See the Veritas Cluster Server Release Notes or the Veritas Storage Foundation High Availability Release Notes for that platform.</td>
</tr>
</tbody>
</table>

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 one of 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 being hosted.

When placing the CP servers within a specific network configuration, you must take into consideration the number of hops from the different application cluster nodes to the CP servers. As a best practice, Symantec recommends that the number of hops 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 the number of hops between the nodes.

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

<table>
<thead>
<tr>
<th></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>
<tr>
<td>CP server cluster in secure mode</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>CP server cluster in non-secure mode</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

- In a secure communication environment, all CP servers that are used by the application cluster must be configured with security enabled. A configuration where the application cluster uses some CP servers running with security enabled and other CP servers running with security disabled is not supported.

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

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

- 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.

Information the `version` option or the `showversion` script discovers on systems includes the following:

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

**To run the version checker**

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

   ```
   # ./installer -version system1 system2
   ```
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>
<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.
  
  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 web-based installer | You can use a web-interface to install and configure VCS. |
### Table 3-1 VCS installation methods (*continued*)

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 Solaris commands and utilities | You can install VCS using the operating system pkgadd command and then manually configure VCS as described in the section on Manual installation.  
  You can also install VCS using the JumpStart utility. |

### 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 packages 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 packages.

See “Preparing to uninstall VCS” on page 359.

**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 72.

- Upgrade VCS if a previous version of VCS currently runs on a cluster.
  See “Upgrading VCS using the script-based installer” on page 265.

- Start or stop VCS processes
  See “Starting and stopping processes for the Veritas products” on page 500.

- 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 137.
  See “Setting up server-based I/O fencing using installvcs program” on page 145.
  See “Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installvcs program” on page 154.

- Create a single-node cluster
  See “Creating a single-node cluster using the installer program” on page 472.

- Add a node to an existing cluster
  See “Adding nodes using the VCS installer” on page 385.

- Create a jumpstart finish script to install VCS using the JumpStart utility.
  See “Installing using JumpStart” on page 216.

- Perform automated installations using the values that are stored in a configuration file.
  See “Installing VCS using response files” on page 179.
  See “Configuring VCS using response files” on page 185.
  See “Upgrading VCS using response files” on page 291.

**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 packages 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 359.

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 339.

About the Web-based installer

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

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

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

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

The location of the Veritas XPortal Server configuration file is /var/opt/webinstaller/xprtlwid.conf.
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, webinstaller, 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 179.
- To upgrade VCS on multiple systems in a large VCS cluster.
  See “Upgrading VCS using response files” on page 291.
- To uninstall VCS from multiple systems in a large VCS cluster.
  See “Uninstalling VCS using response files” on page 365.
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:

```perl
$CFG{Scalar_variable} = "value";
```

or, in the case of an integer value:

```perl
$CFG{Scalar_variable} = 123;
```

or, in the case of a list:

```perl
$CFG{List_variable} = ["value", "value", "value"];
```

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 48.

- VCS clusters in secure mode
  See “Typical configuration of VCS clusters in secure mode” on page 49.

- VCS clusters centrally managed using Veritas Operations Manager (VOM)
  See “Typical configuration of VOM-managed VCS clusters” on page 50.

- VCS clusters with I/O fencing for data protection
  See “Typical VCS cluster configuration with disk-based I/O fencing” on page 92.
  See “Typical VCS cluster configuration with server-based I/O fencing” on page 93.

- 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 Solaris SPARC systems.
Figure 3-1  Typical two-node VCS cluster (Solaris SPARC systems)

Node: galaxy
qfe:0
qfe:1

Node: nebula
qfe:0
qfe:1

VCS private network

hme0

Public network

Cluster name: vcs_cluster2
Cluster id: 7

Figure 3-2 illustrates a simple VCS cluster setup with two Solaris x64 systems.

Figure 3-2  Typical two-node VCS cluster (Solaris x64 systems)

Node: galaxy
e1000g:0
e1000g:1

Node: nebula
e1000g:0
e1000g:1

VCS private network

bge0

Public network

Cluster name: vcs_cluster2
Cluster id: 7

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 3-3 illustrates typical configuration of VCS clusters in secure mode.
Figure 3-3  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 29.

Figure 3-4 illustrates a typical setup of VCS clusters that are centrally managed using Veritas Operations Manager.
Figure 3-4 Typical configuration of VOM-managed clusters

VOM Central Server and Symantec Product Authentication Service

Cluster 1

Cluster 2
Planning to install VCS

Typical VCS cluster setup models
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 or continue with keyless licensing by managing the server or cluster with a management server, such as Veritas Operations Manager (VOM). 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/sfnameless

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

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  
  See “Setting or changing the product level for keyless licensing” on page 213. 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 package 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 package enables product licensing. After the VRTSvlic is installed, the following commands and their manual pages are available on the system:

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

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

**To install a new license**

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

  ```
  # cd /opt/VRTS/bin
  # ./vxlicinst -k xxxx-xxxx-xxxx-xxxx-xxxx-xxx
  ```
Installing Veritas product license keys
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 35.

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>Enable communication between systems.</td>
<td>See “Setting up inter-system communication” on page 493.</td>
</tr>
</tbody>
</table>
### Table 5-1  Preinstallation tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up ssh on cluster systems.</td>
<td>See “Setting up ssh on cluster systems” on page 493.</td>
</tr>
<tr>
<td>Set up shared storage for I/O fencing (optional)</td>
<td>See “Setting up shared storage” on page 64.</td>
</tr>
<tr>
<td>Set the PATH and the MANPATH variables.</td>
<td>See “Setting the PATH variable” on page 68.</td>
</tr>
<tr>
<td></td>
<td>See “Setting the MANPATH variable” on page 68.</td>
</tr>
<tr>
<td>Disable the abort sequence on SPARC systems.</td>
<td>See “Disabling the abort sequence on SPARC systems” on page 69.</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 70.</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 70.</td>
</tr>
<tr>
<td>Install the patches that are required for Java Run Time environment from Oracle.</td>
<td>For instructions, see the Oracle documentation.</td>
</tr>
<tr>
<td>Prepare zone environments</td>
<td>See “Preparing zone environments” on page 70.</td>
</tr>
<tr>
<td>Mount the product disc</td>
<td>See “Mounting the product disc” on page 71.</td>
</tr>
<tr>
<td>Verify the systems before installation</td>
<td>See “Performing automated preinstallation check” on page 72.</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. However, Oracle systems assign the same MAC address to all interfaces by default. Thus, connecting two or more interfaces to a network switch can cause problems.

For example, consider the following case where:

- The IP address is configured on one interface and LLT on another
Both interfaces are connected to a switch (assume separate VLANs)

The duplicate MAC address on the two switch ports can cause the switch to incorrectly redirect IP traffic to the LLT interface and vice versa. To avoid this issue, configure the system to assign unique MAC addresses by setting the `eeprom(1M)` parameter `local-mac-address` to `true`.

The following products make extensive use of the private cluster interconnects for distributed locking:

- Veritas Storage Foundation Cluster File System (SFCFS)
- Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)

Symantec recommends network switches for the SFCFS and the SF Oracle RAC clusters due to their performance characteristics.

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.

**Figure 5-1** Private network setups: two-node and four-node clusters

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 Ethernet controllers 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.

4. Configure the Ethernet devices that are used for the private network such that the autonegotiation protocol is not used. You can achieve a more stable configuration with crossover cables if the autonegotiation protocol is not used.
To achieve this stable configuration, do one of the following:

- Edit the /etc/system file to disable autonegotiation on all Ethernet devices system-wide.
- Create a qfe.conf or bge.conf file in the /kernel/drv directory to disable autonegotiation for the individual devices that are used for private network.

Refer to the Oracle Ethernet driver product documentation for information on these methods.

5 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 223.

About using ssh or rsh with the Veritas installer

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

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 add new nodes to an existing cluster.
- When the nodes are in a subcluster during a phased upgrade.
- When you perform installer sessions using a response file.

See “Setting up inter-system communication” on page 493.
Setting up shared storage

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

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

See “About planning to configure I/O fencing” on page 89.

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

Setting up shared storage: SCSI disks

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

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

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

To set up shared storage

1. Install the required SCSI host adapters on each node that connects to the storage, and make cable connections to the storage.
   Refer to the documentation that is shipped with the host adapters, the storage, and the systems.

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

3. Power on one system, but do not allow it to boot. If necessary, halt the system so that you can use the `ok` prompt.
   Note that only one system must run at a time to avoid address conflicts.
4 Find the paths to the host adapters:

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

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

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

```
{0} ok nvedit
```

As you edit the script, note the following points:

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

In this example, edit the `nvramrc` script as follows:

```
0: probe-all
1: cd /sbus@6,0/QLGC,isp@2,10000
2: 5 " scsi-initiator-id" integer-property
3: device-end
4: install-console
5: banner
6: <CTRL-C>
```
6 Store the changes you make to the \texttt{nvramrc} script. The changes you make are temporary until you store them.

\texttt{ok nvstore}

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

\texttt{ok printenv nvramrc}

You can re-edit the file to make corrections:

\texttt{ok nedit}

Or, discard the changes if necessary by entering:

\texttt{ok nvquit}

7 Instruct the OpenBoot PROM Monitor to use the \texttt{nvramrc} script on the node.

\texttt{ok setenv use-nvramrc? true}

8 Reboot the node. If necessary, halt the system so that you can use the \texttt{ok} prompt.
9 Verify that the scsi-initiator-id has changed. Go to the ok prompt. Use the output of the show-disks command to find the paths for the host adapters. Then, display the properties for the paths. For example:

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

Permit the system to continue booting.

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

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

Permit the system to continue booting.

### Setting up shared storage: Fibre Channel

Perform the following steps to set up Fibre Channel.

#### To set up shared storage

1 Install the required FC-AL controllers.

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

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

3 Boot each system with the reconfigure devices option:

   ```
   ok boot -r
   ```

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

   If Volume Manager is used, the same number of external disk devices must appear, but device names (c#t#d#s#) may differ.
If Volume Manager is not used, then you must meet the following requirements:

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

**Setting the PATH variable**

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

If you have any custom scripts located in `/optVRTSvcs/bin` directory, make sure to add the `/optVRTSvcs/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=/optVRTS/bin:$PATH; export PATH
    ```
  
  - For the C Shell (csh) or enhanced C Shell (tcsh), type:
    
    ```
    $ setenv PATH :/optVRTS/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=/optVRTS/man:$MANPATH; export MANPATH
    ```
  
  - For the C Shell (csh) or enhanced C Shell (tcsh), type:
    
    ```
    $ setenv MANPATH /usr/share/man:/optVRTS/man
    ```
Disabling the abort sequence on SPARC systems

Most UNIX operating systems provide a method to perform a "break" or "console abort." The inherent problem when you abort a hung system is that it ceases to heartbeat in the cluster. When other cluster members believe that the aborted node is a failed node, these cluster members may begin corrective action.

Keep the following points in mind:

- The only action that you must perform following a system abort is to reset the system to achieve the following:
  - Preserve data integrity
  - Prevent the cluster from taking additional corrective actions
- Do not resume the processor as cluster membership may have changed and failover actions may already be in progress.
- To remove this potential problem on SPARC systems, you should alias the go function in the OpenBoot eeprom to display a message.

To alias the go function to display a message

1. At the ok prompt, enter:

   nvedit

2. Press Ctrl+L to display the current contents of the nvramrc buffer.

3. Press Ctrl+N until the editor displays the last line of the buffer.

4. Add the following lines exactly as shown. Press Enter after adding each line.

   " Aliasing the OpenBoot 'go' command! "
   : go ." It is inadvisable to use the 'go' command in a clustered environment. " cr
   ." Please use the 'power-off' or 'reset-all' commands instead. " cr
   ." Thank you, from your friendly neighborhood sysadmin. " ;

5. Press Ctrl+C to exit the nvramrc editor.

6. To verify that no errors exist, type the nvrun command. You should see only the following text:

   Aliasing the OpenBoot 'go' command!
7. Type the `nvstore` command to commit your changes to the non-volatile RAM (NVRAM) for use in subsequent reboots.

8. After you perform these commands, at reboot you see this output:

   **Aliasing the OpenBoot 'go' command! go isn't unique.**

**Optimizing LLT media speed settings on private NICs**

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

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

**Guidelines for setting the media speed of the LLT interconnects**

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

- Symantec recommends that you manually set the same media speed setting on each Ethernet card on each node. If you use different media speed for the private NICs, Symantec recommends that you configure the NICs with lesser speed as low-priority links to enhance LLT performance.

- If you have hubs or switches for LLT interconnects, then set the hub or switch port to the same setting as used on the cards on each node.

- If you use directly connected Ethernet links (using crossover cables), Symantec recommends that you set the media speed to the highest value common to both cards, typically 1000_Full_Duplex.

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

**Preparing zone environments**

You need to keep the following items in mind when you install or upgrade VCS in a zone environment.

- When you install or upgrade VCS using the `installer` program, all zones are upgraded (both global and non-global) unless they are detached and unmounted.
Make sure that all non-global zones are booted and in the running state before you install or upgrade the VCS packages in the global zone. If the non-global zones are not mounted and running at the time of upgrade, you must upgrade each package in each non-global zone manually.

If you install VCS on Solaris 10 systems that run non-global zones, you need to make sure that non-global zones do not inherit the /opt directory. Run the following command to make sure that the /opt directory is not in the inherit-pkg-dir clause:

```
# zonecfg -z zone_name info
zonepath: /export/home/zone1
autoboot: false
pool: yourpool
inherit-pkg-dir:
  dir: /lib
inherit-pkg-dir:
  dir: /platform
inherit-pkg-dir:
  dir: /sbin
inherit-pkg-dir:
  dir: /usr
```

If the /opt directory appears in the output, remove the /opt directory from the zone's configuration and reinstall the zone.

**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 into a DVD drive that is connected to your system.
If Solaris volume management software is running on your system, the software disc automatically mounts as /cdrom/cdrom0.

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

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

Where c0t6d0s2 is the default address for the disc drive.

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.

   ```bash
   # cd /cdrom/cdrom0/cluster_server
   ```

2. Start the preinstallation check:

   ```bash
   # ./installvcs -precheck galaxy nebula
   ```

   The program proceeds in a noninteractive mode to examine the systems for licenses, packages, 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.

   See “Command options for installvcs program” on page 419.

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 a 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 packages.

<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 Example: galaxy, nebula</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. See “About Veritas product licensing” on page 53. Depending on the type of installation, keys can include: A valid site license key A valid demo license key A valid license key for VCS global clusters See “Obtaining VCS license keys” on page 54.</td>
<td></td>
</tr>
<tr>
<td>Decide which packages to install</td>
<td>Minimum packages—provides basic VCS functionality. Recommended packages—provides full functionality of VCS without advanced features. All packages—provides advanced feature functionality of VCS. The default option is to install the recommended packages. See “Viewing the list of VCS packages” on page 210.</td>
<td></td>
</tr>
</tbody>
</table>

Table 5-3 lists the 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;. 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. 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>
<th>Your 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. You must manually enter details for options 1 and 2, whereas the installer detects the details for option 3. See &quot;Using the UDP layer for LLT&quot; on page 475.</td>
<td></td>
</tr>
</tbody>
</table>
| Decide which configuration mode you want to choose| Installer provides you with three options:  
  ■ 1. Configure heartbeat links using LLT over Ethernet  
  ■ 2. Configure heartbeat links using LLT over UDP  
  ■ 3. 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 hme0 for SPARC and bge0 for x64.  
  For example on a SPARC system: qfe0, qfe1  
  For example on an x64 system: e1000g1, e1000g2  
  ■ 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>
<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. Example: hme0</td>
<td></td>
</tr>
<tr>
<td>A virtual IP address of the NIC</td>
<td>You can enter either an IPv4 or an IPv6 address. This virtual IP address becomes a resource for use by the ClusterService group. The &quot;Cluster Virtual IP address&quot; can fail over to another cluster system. Example IPv4 address: 192.168.1.16 Example IPv6 address: 2001:454e:205a:110:203:baff:feee:10</td>
<td></td>
</tr>
<tr>
<td>The netmask for the virtual IPv4 address</td>
<td>The subnet that you use with the virtual IPv4 address. Example: 255.255.240.0</td>
<td></td>
</tr>
<tr>
<td>The prefix for the virtual IPv6 address</td>
<td>The prefix length for the virtual IPv6 address. Example: 64</td>
<td></td>
</tr>
</tbody>
</table>

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

## Table 5-6  Information you need to add VCS users

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

### 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: <strong>hme0</strong></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: <strong>smtp.symantecexample.com</strong></td>
<td></td>
</tr>
<tr>
<td>The email address of each SMTP recipient to be notified</td>
<td>Example: <strong><a href="mailto:john@symantecexample.com">john@symantecexample.com</a></strong></td>
<td></td>
</tr>
<tr>
<td>To decide the minimum severity of events for SMTP email notification</td>
<td>Events have four levels of severity, and the severity levels are cumulative:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCS sends notifications for important events that exhibit normal behavior.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Warning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCS sends notifications for events that exhibit any deviation from normal behavior. Notifications include both Warning and Information type of events.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCS sends notifications for faulty behavior. Notifications include both Error, Warning, and Information type of events.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SevereError</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: <strong>Error</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Table 5-8** lists the information you need to configure SNMP trap notification (optional).

### 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: <strong>hme0</strong></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: saturn</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.  
For example for SPARC systems: hme0  
For example for x64 systems: bge0 |            |
### 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>
</table>
| The virtual IP address of the NIC  | 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: **192.168.1.16**  
| The netmask for the virtual IPv4 address | 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: **255.255.240.0**                                                                                   |            |
| The prefix for the virtual IPv6 address | The prefix length for the virtual IPv6 address.  
Example: **64**                                                                                           |            |

Review the information you need to configure I/O fencing.

See “About planning to configure I/O fencing” on page 89.
Installation using the script-based installer

- Chapter 6. Installing VCS
- Chapter 7. Preparing to configure VCS
- 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 language packages using the installer

Installing VCS using the installer

Perform the following steps to install VCS.

To install VCS

1. Confirm that you are logged in as the superuser and you mounted the product disc.
   
   See “Mounting the product disc” on page 71.

2. Start the installation program. If you obtained VCS from an electronic download site, which does not include the Veritas product installer, use the installvcs program.

   Perform the following steps to start the product installer:

   1. Start the installer.

      # ./installer

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

   2. From the opening Selection Menu, choose 1 for "Install a Product."

   3. From the displayed list of products to install, choose: Veritas Cluster Server.
Perform the following steps to start the product installer:

1. Navigate to the folder that contains the installvcs program.
   
   ```
   # cd /cdrom/cdrom0/cluster_server
   ```

2. Start the installvcs program.
   
   ```
   # ./installvcs
   ```

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

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_Ux_6.0.pdf`
   file present on media? [y,n,q,?] `y`

4. Choose the VCS packages that you want to install.
   
   See “Veritas Cluster Server installation packages” on page 413.

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

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

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

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

   4. Displays the VCS packages for each option.

   Select the packages to be installed on all systems? [1-4,q,?] `y`
   (2) `3`

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

   Enter the system names separated by spaces:
   
   [q,?] (galaxy) `galaxy nebula`

   For a single-node VCS installation, enter one name for the system.
See “Creating a single-node cluster using the installer program” on page 472.

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.

- Makes sure the systems install from the global zone.

- 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.
  - See “About upgrading to VCS 6.0” on page 259.

- 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 packages already exists on a system.
  - If the current version of any package exists, the installer removes the package from the installation list for the system. If a previous version of any package exists, the installer replaces the package with the current version.

6 Review the list of packages and patches that the installer would install on each node.

The installer installs the VCS packages and patches on the systems galaxy and nebula.

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,?]
   
   XXXX-XXXX-XXXX-XXXX-XXXX

   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 galaxy nebula [y,n,q] (n) n

   See “Overview of tasks to configure VCS using the script-based installer” on page 113.

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 packages 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 179.

## Installing language packages using the installer

Before you install the language packages, do the following:

- Make sure `install_lp` command uses the `ssh` or `rsh` commands as root on all systems in the cluster.

- Make sure that permissions are granted for the system on which `install_lp` is run.

### To install the language packages

1. Insert the language disc into the drive.
   
   The Solaris volume-management software automatically mounts the disc as `/cdrom/cdrom0`.

2. Change to the `/cdrom/cdrom0` directory.
   
   ```
   # cd /cdrom/cdrom0
   ```

3. Install the language packages:
   
   ```
   # ./install_lp
   ```
Installing language packages using the installer
Preparing to configure VCS

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 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 91.
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

1. **Install and configure VCS**
2. **Configure disk-based fencing (scsi3 mode)**
   - **Three disks**
   - **Preparatory tasks**
     - Initialize disks as VxVM disks
     - Check disks for I/O fencing compliance
   - **Configuration tasks**
     - Use one of the following methods
       - Run the installvcs -fencing, choose option 2, and follow the prompts
       - Edit the values in the response file you created and use them with installvcs -responsefile command
       - Manually configure disk-based I/O fencing
       - Choose to configure disk-based fencing using the Web-based installer

3. **Coordinate points for I/O fencing?**
4. **At least one CP server**
5. **Configure server-based fencing (customized mode)**
   - **Identify an existing CP server**
   - **Establish TCP/IP connection between CP server and VCS cluster**
   - **Install and configure VCS or SFHA on CP server systems**
   - **Establish TCP/IP connection between CP server and VCS cluster**
   - **If the CP server is clustered, set up shared storage for the CP server**
   - **Run the configure_cps utility and follow the prompts (OR) Manually configure CP server**
     - Initialize disks as VxVM disks and Check disks for I/O fencing compliance

For the disks that will serve as coordination points:

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

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

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

1. Run the `installvcs -fencing`, choose option 1, enter n to confirm that storage is not SCSI3-compliant, and follow the prompts
2. Edit the values in the response file you created and use them with `installvcs -responsefile` command
3. Manually configure non-SCSI3 server-based I/O fencing
Using the `installvcs` program

See “Setting up disk-based I/O fencing using `installvcs` program” on page 137.
See “Setting up server-based I/O fencing using `installvcs` program” on page 145.
See “Setting up non-SCSI-3 server-based I/O fencing in virtual environments using `installvcs` program” on page 154.

Using the Web-based installer

See “Configuring VCS for data integrity using the Web-based installer” on page 172.

Using response files

See “Response file variables to configure disk-based I/O fencing” on page 198.
See “Response file variables to configure server-based I/O fencing” on page 200.
See “Response file variables to configure non-SCSI-3 server-based I/O fencing” on page 202.
See “Configuring I/O fencing using response files” on page 197.

Manually editing configuration files

See “Setting up disk-based I/O fencing manually” on page 233.
See “Setting up server-based I/O fencing manually” on page 238.
See “Setting up non-SCSI-3 fencing in virtual environments manually” on page 250.

You can also migrate from one I/O fencing configuration to another.
See the *Veritas Cluster Server 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.

*Figure 7-3* Typical VCS cluster configuration with disk-based 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 94.

- Multiple application clusters use a single CP server and multiple pairs of coordinator disks (two) as their coordination points
  See Figure 7-6 on page 95.

- 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 95.
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 CP servers 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

(application 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

See “Configuration diagrams for setting up server-based I/O fencing” on page 505.
# Setting up the CP server

Table 7-1 lists the tasks to set up the 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 96.</td>
</tr>
<tr>
<td>Install the CP server</td>
<td>See “Installing the CP server using the installer” on page 97.</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 98.</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 98.</td>
</tr>
</tbody>
</table>
| Configure the CP server             | See “Configuring the CP server using the configuration utility” on page 99.  
                                           See “Configuring the CP server manually” on page 109. |
| Verify the CP server configuration  | See “Verifying the CP server configuration” on page 111.                 |

## Planning your CP server setup

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

### To plan your CP server setup

1. Decide whether you want to host the CP server on a single-node VCS cluster, or on an SFHA cluster.
   - Symantec recommends hosting the CP server on an SFHA cluster 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 configure disk-based fencing during the SFHA configuration.
   - You must set up shared storage for the CP server database during your CP server setup.
• Decide whether you want to configure server-based fencing for the 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.
  See “CP server requirements” on page 38.

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 packages for installation. The VRTScps package is installed only if you select to install all packages.
  Proceed to configure the CP server.
  See “Configuring the CP server using the configuration utility” on page 99.

See “Configuring the CP server manually” on page 109.
CP server setup uses multiple systems

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

Meet the following requirements for CP server:

■ During installation, make sure to select all packages for installation. The VRTScps package is installed only if you select to install all packages.
■ During configuration, configure disk-based fencing (scsi3 mode).

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

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

Configuring the CP server cluster in secure mode

You must configure security on the CP server only if you want to secure the communication between the CP server and the 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:

```bash
# installvcs -security
```

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

```bash
# installsfha -security
```

Setting up shared storage for the CP server database

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

Symantec recommends that you create a mirrored volume for the CP server database and that you use the vxfs file system type.
To set up shared storage for the CP server database

1. Create a disk group containing the disks. You require two disks to create a mirrored volume.
   For example:
   ```
   # vxdg init cps_dg  disk1 disk2
   ```

2. Import the disk group if it is not already imported.
   For example:
   ```
   # vxdg import cps_dg
   ```

3. Create a mirrored volume over the disk group.
   For example:
   ```
   # vxassist -g cps_dg make cps_vol volume_size layout=mirror
   ```

4. Create a file system over the volume.
   The CP server configuration utility only supports vxfs file system type. If you use an alternate file system, then you must configure CP server manually.
   Depending on the operating system that your CP server runs, enter the following command:
   ```
   AIX         # mkfs -V vxfs /dev/vx/rdsk/cps_dg/cps_volume
   HP-UX       # mkfs -F vxfs /dev/vx/rdsk/cps_dg/cps_volume
   Linux       # mkfs -t vxfs /dev/vx/rdsk/cps_dg/cps_volume
   Solaris     # mkfs -F vxfs /dev/vx/rdsk/cps_dg/cps_volume
   ```

Configuring the CP server using the configuration utility

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

Perform one of the following procedures:
For CP servers on single-node VCS cluster: See “To configure the CP server on a single-node VCS cluster” on page 100.

For CP servers on an SFHA cluster: See “To configure the CP server on an SFHA cluster” on page 104.

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

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

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

   # /opt/VRTScps/bin/configure_cps.pl

3 Enter 1 at the prompt to configure CP server on a single-node VCS cluster. The configuration utility then runs the following preconfiguration checks:

   ■ Checks to see if a single-node VCS cluster is running with the supported platform.
     The CP server requires VCS to be installed and configured before its configuration.

   ■ Checks to see if the CP server is already configured on the system.
     If the CP server is already configured, then the configuration utility informs the user and requests that the user unconfigure the CP server before trying to configure it.

4 Enter the name of the CP server.

   Enter the name of the CP Server: mycps1

5 Enter valid virtual IP addresses on which the CP server process should depend on:

   ■ Enter the number of virtual IP addresses you want to configure:

     Enter the number of virtual IP(s) to configure : 2

   ■ Enter valid virtual IP addresses:

     Enter a valid IP address for Virtual IP - 1 which the CP Server process should depend on : 10.209.83.85
     Enter a valid IP address for Virtual IP - 2 which the CP Server process should depend on : 10.209.83.87
You can also use IPv6 address.

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

Enter a port number for virtual IP 10.209.83.85 in range [49152, 65535], or press enter for default port (14250) :

Using default port: 14250

Enter a port number for virtual IP 10.209.83.87 in range [49152, 65535], or press enter for default port (14250) :

Using default port: 14250

7 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.

Veritas recommends secure communication between the CP server and application clusters. Enabling security requires Symantec Product Authentication Service to be installed and configured on the cluster.

Do you want to enable Security for the communications? (y/n) (Default:y) :

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

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

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

Enter absolute path of the database (Default:/etc/VRTScps/db):
Verify and confirm the CP server configuration information.

Following is the CP Server configuration information:
-------------------------------------------------
(a) CP Server Name: mycps1
(b) CP Server Virtual IP(s): 10.209.83.85 10.209.83.87
(c) CP Server Port(s): 14250 14250
(d) CP Server Security : 1
(e) CP Server Database Dir: /etc/VRTScps/db
-------------------------------------------------

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

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

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

Configuring CP Server Service Group (CPSSG) for this cluster

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.

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

Enter a valid network interface for virtual IP 10.209.83.85 on mycps1.symantecexample.com: hme0
Enter a valid network interface for virtual IP 10.209.83.87 on mycps1.symantecexample.com: hme0

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 10.209.83.85 [1 to 2] : 1
Enter the NIC resource you want to associate with the virtual IP 10.209.83.87 [1 to 2] : 2
14 Enter networkhosts information for each NIC resource.

Symantec recommends configuring NetworkHosts attribute to ensure NIC resource to be online always.
Do you want to add NetworkHosts attribute for the NIC device hme0 on system mycps1? [y/n] : y
Enter a valid IP address to configure NetworkHosts for NIC hme0 on system mycps1: 10.209.83.86
Do you want to add another Network Host? [y/n] : n

15 Enter the netmask for each virtual IP address. For example:

Enter the netmask for virtual IP 10.209.83.85: 255.255.252.0
Enter the netmask for virtual IP 10.209.83.87: 255.255.252.0

If you entered an IPv6 address, enter the prefix details at the prompt.
After the configuration process has completed, a success message appears. For example:

Successfully added the Quorum Agent Type to VCS configuration.
Successfully added the CPSSG service group to VCS configuration. Bringing the CPSSG service group online. Please wait...

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

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

For example:

```
# hagrp -state CPSSG
```

<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>mycps1.symantecexample.com</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>

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

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

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

See “Sample configuration files for CP server” on page 464.

To configure the CP server on an SFHA cluster

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

2. Make sure that you have configured passwordless ssh or rsh on the CP server cluster nodes.

3. Run the CP server configuration script on any node in the cluster:

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

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

4. Enter 2 at the prompt to configure CP server on an SFHA cluster. The configuration utility then runs the following preconfiguration checks:
Checks to see if an SFHA cluster is running with the supported platform. The CP server requires SFHA to be installed and configured before its configuration.

Checks to see if the CP server is already configured on the system. If the CP server is already configured, then the configuration utility informs the user and requests that the user unconfigure the CP server before trying to configure it.

5 Enter the name of the CP server.

Enter the name of the CP Server: mycps1

6 Enter valid virtual IP addresses on which the CP server process should depend on:

   Enter the number of virtual IP addresses you want to configure:

   Enter the number of virtual IP(s) to configure: 2

   Enter valid virtual IP addresses:

   Enter a valid IP address for Virtual IP - 1 which the CP Server process should depend on: 10.209.83.85
   Enter a valid IP address for Virtual IP - 2 which the CP Server process should depend on: 10.209.83.87

   You can also use IPv6 address.

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

   Enter a port number for virtual IP 10.209.83.85 in range [49152, 65535], or press enter for default port (14250): 

   Using default port: 14250

   Enter a port number for virtual IP 10.209.83.87 in range [49152, 65535], or press enter for default port (14250):

   Using default port: 14250
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.

Veritas recommends secure communication between the CP server and application clusters. Enabling security requires Symantec Product Authentication Service to be installed and configured on the cluster.

Do you want to enable Security for the communications? (y/n) (Default:y) :

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

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

Note: As the CP Server is being configured on SFHA cluster, the database should reside on shared storage with vxfs file system.

Please refer to documentation for information on setting up of shared storage for CP server database.

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

Verify and confirm the CP server configuration information.

Following is the CP Server configuration information:

| (a) CP Server Name: mycps1 |
| (b) CP Server Virtual IP(s): 10.209.83.85 10.209.83.87 |
| (c) CP Server Port(s): 14250 14250 |
| (d) CP Server Security : 1 |
| (e) CP Server Database Dir: /etc/VRTScps/db |

Press b if you want to change the configuration, <enter> to continue:
The configuration utility proceeds with the configuration process, and creates a vxcps.conf configuration file on each node.

The following output is for one node:

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

Configuring CP Server Service Group (CPSSG) for this cluster

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.

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

Is the name of network interfaces for NIC resource - 1 same on all the systems?[y/n] : y

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

Enter a valid interface for virtual IP 10.209.83.85 on all the systems : hme0

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 10.209.83.85 [1 to 2] : 1
Enter the NIC resource you want to associate with the virtual IP 10.209.83.87 [1 to 2] : 2
16 Enter networkhosts information for each NIC resource.

Symantec recommends configuring NetworkHosts attribute to ensure NIC resource to be online always.
Do you want to add NetworkHosts attribute for the NIC device hme0 on system mycps1? [y/n] : y
Enter a valid IP address to configure NetworkHosts for NIC hme0 on system mycps1 : 10.209.83.86
Do you want to add another Network Host? [y/n] : n

17 Enter the netmask for each virtual IP address.

Enter the netmask for virtual IP 10.209.83.85 :
255.255.252.0

If you entered an IPv6 address, enter the prefix details at the prompt.

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

Enter the name of diskgroup for cps database :
cps_dg

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

Enter the name of volume created on diskgroup cps_dg :
cps_volume
After the configuration process has completed, a success message appears. For example:

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

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

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

```
# hagrp -state CPSSG
```

<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>mycps1</td>
<td>ONLINE</td>
</tr>
<tr>
<td>CPSSG</td>
<td>State</td>
<td>mycps2</td>
<td>OFFLINE</td>
</tr>
</tbody>
</table>

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

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

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

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

See “Sample configuration files for CP server” on page 464.

**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:
   
   ```bash
   # hastop -local
   ```

2. Edit the `main.cf` file to add the CPSSG service group on any node. Use the CPSSG service group in the main.cf as an example:

   See “Sample configuration files for CP server” on page 464.

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

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

   ```bash
   # 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.

   ```bash
   # hastart
   ```

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

   ```bash
   # hagrp -state CPSSG
   ```

   Output similar to the following appears:

   ```
   Group Attribute System Value
   CPSSG State mycps1.symantecexample.com ONLINE
   ```
Verifying the CP server configuration

Perform the following steps to verify the CP server configuration.

To verify the CP server configuration

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

   ```bash
   # 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

Setting up the CP server
Configuring VCS

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 the cluster in secure mode
- Configuring a secure cluster node by node
- Adding VCS users
- Configuring SMTP email notification
- Configuring SNMP trap notification
- Configuring global clusters
- Completing the 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 114.</td>
</tr>
<tr>
<td>Specify the systems where you want to configure VCS</td>
<td>See “Specifying systems for configuration” on page 115.</td>
</tr>
<tr>
<td>Configure the basic cluster</td>
<td>See “Configuring the cluster name” on page 116.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring private heartbeat links” on page 116.</td>
</tr>
<tr>
<td>Configure virtual IP address of the cluster (optional)</td>
<td>See “Configuring the virtual IP of the cluster” on page 119.</td>
</tr>
<tr>
<td>Configure the cluster in secure mode (optional)</td>
<td>See “Configuring the cluster in secure mode” on page 121.</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 126.</td>
</tr>
<tr>
<td>Configure SMTP email notification (optional)</td>
<td>See “Configuring SMTP email notification” on page 127.</td>
</tr>
<tr>
<td>Configure SNMP email notification (optional)</td>
<td>See “Configuring SNMP trap notification” on page 129.</td>
</tr>
<tr>
<td>Configure global clusters (optional)</td>
<td>See “Configuring global clusters” on page 131.</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 132.</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.

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

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

## Specifying systems for configuration

The installer prompts for the system names on which you want to configure 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,?] (galaxy) galaxy nebula
   ```

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

   The installer does the following tasks:
   - Checks that the local node running the installer can communicate with remote nodes
     - If the installer finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases.
- Makes sure that the systems are running with the supported operating system
- Makes sure the installer started from the global zone
- Checks whether VCS is installed
- Exits if VCS 6.0 is not installed

3. Review the installer output about the I/O fencing configuration and confirm whether you want to configure fencing in enabled mode.

Do you want to configure I/O Fencing in enabled mode? [y,n,q,?] (y)

See “About planning to configure I/O fencing” on page 89.

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

See “Using the UDP layer for LLT” on page 475.

The following procedure helps you configure LLT over Ethernet.

To configure private heartbeat links

1. Choose one of the following options at the installer prompt based on whether you want to configure LLT over Ethernet or UDP.
   - Option 1: LLT over Ethernet (answer installer questions)
     Enter the heartbeat link details at the installer prompt to configure LLT over Ethernet.
     Skip to step 2.
Option 2: LLT over UDP (answer installer questions)
Make sure that each NIC you want to use as heartbeat link has an IP address configured. Enter the heartbeat link details at the installer prompt to configure LLT over UDP. If you had not already configured IP addresses to the NICs, the installer provides you an option to detect the IP address for a given NIC.
Skip to step 3.

Option 3: Automatically detect configuration for LLT over Ethernet
Allow the installer to automatically detect the heartbeat link details to configure LLT over Ethernet. The installer tries to detect all connected links between all systems.
Skip to step 5.

2 If you chose option 1, enter the network interface card details for the private heartbeat links.
The installer discovers and lists the network interface cards.
Answer the installer prompts. The following example shows different NICs based on architecture:

For Solaris SPARC:
You must not enter the network interface card that is used for the public network (typically hme0.)

Enter the NIC for the first private heartbeat link on galaxy: [b,q,?] qfe0
Would you like to configure a second private heartbeat link? [y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat link on galaxy: [b,q,?] qfe1
Would you like to configure a third private heartbeat link? [y,n,q,b,?] (n)
Do you want to configure an additional low priority heartbeat link? [y,n,q,b,?] (n)

For Solaris x64:
You must not enter the network interface card that is used for the public network (typically bge0.)

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

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

Enter the NIC for the first private heartbeat link on galaxy: [b,q,?] **private_NIC1**
Do you want to use address 192.168.0.1 for the first private heartbeat link on galaxy: [y,n,q,b,?] (y)
Enter the UDP port for the first private heartbeat link on galaxy: [b,q,?] (50000) ?
Would you like to configure a second private heartbeat link? [y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat link on galaxy: [b,q,?] **private_NIC2**
Do you want to use address 192.168.1.1 for the second private heartbeat link on galaxy: [y,n,q,b,?] (y)
Enter the UDP port for the second private heartbeat link on galaxy: [b,q,?] (50001) ?
Do you want to configure an additional low priority heartbeat link? [y,n,q,b,?] (n) y
Enter the NIC for the low priority heartbeat link on galaxy: [b,q,?] **private_NIC0**
Do you want to use address 192.168.3.1 for the low priority heartbeat link on galaxy: [y,n,q,b,?] (y)
Enter the UDP port for the low priority heartbeat link on galaxy: [b,q,?] (50004)
4 Choose whether to use the same NIC details to configure private heartbeat links on other systems.

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

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

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

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

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

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

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

6 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 galaxy: `hme0`
   Enter the NIC for Virtual IP of the Cluster to use on galaxy: `[b,q,?] (hme0)`

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 `hme0` 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,?] \texttt{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:

  \begin{center}
  \begin{tabular}{l}
  NIC: \texttt{hme0} \\
  IP: 192.168.1.16 \\
  Netmask: 255.255.240.0 \\
  \end{tabular}
  \end{center}

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

For IPv6

- Enter the virtual IP address.

  Enter the Virtual IP address for the Cluster:  

- 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,?] \texttt{64}

- Verify and confirm the Cluster Virtual IP information.

  Cluster Virtual IP verification:

  \begin{center}
  \begin{tabular}{l}
  NIC: \texttt{hme0} \\
  Prefix: 64 \\
  \end{tabular}
  \end{center}

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

---

**Configuring the cluster in secure mode**

The installer prompts whether you want to configure a secure cluster.
Would you like to configure the VCS cluster in secure mode?
[y,n,q,?] (n)

To configure a secure cluster, enter y.

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 -securitytrust

   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 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.

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

<table>
<thead>
<tr>
<th>Table 8-2</th>
<th>Configuring a secure cluster node by node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Reference</td>
</tr>
<tr>
<td>Configure security on one node</td>
<td>See “Configuring the first node” on page 123.</td>
</tr>
<tr>
<td>Configure security on the remaining nodes</td>
<td>See “Configuring the remaining nodes” on page 124.</td>
</tr>
<tr>
<td>Complete the manual configuration steps</td>
<td>See “Completing the secure cluster configuration” on page 125.</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 -securityonenode`

   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 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 `/var/VRTSvcs/vcsauth/bkup` directory 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 -securityonenuode
```

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/CmdServer/hastop -all -force
```
3  On all nodes, stop the CmdServer.
    
    # /opt/VRTSvcs/bin/CmdServer -stop

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

    cluster clus1 (
        SecureClus = 1
    )

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

6  On the first node, start VCS. Then start VCS on the remaining nodes.
    
    # /opt/VRTSvcs/bin/hastart

7  On all nodes, start CmdServer.
    
    # /opt/VRTSvcs/bin/CmdServer

8  On the first node, unfreeze the service groups.
    
    # /opt/VRTSvcs/bin/haconf -makerw
    
    # /opt/VRTSvcs/bin/hagrp -list Frozen=1
    
    # /opt/VRTSvcs/bin/hagrp -unfreeze groupname -persistent
    
    # /opt/VRTSvcs/bin/haconf -dump -makero

Adding VCS users

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

1. Review the required information to add VCS users.

2. Reset the password for the Admin user, if necessary.
   - Do you wish to accept the default cluster credentials of 'admin/password'? [y,n,q] (y) n
   - Enter the user name: [b,q,?] (admin)
   - Enter the password:
   - Enter again:

3. To add a user, enter y at the prompt.
   - Do you want to add another user to the cluster? [y,n,q] (y)

4. Enter the user's name, password, and level of privileges.
   - Enter the user name: [b,q,?] smith
   - Enter New Password:******
     Enter Again:******
   - Enter the privilege for user smith (A=Administrator, O=Operator, G=Guest): [b,q,?] a

5. Enter n at the prompt if you have finished adding users.
   - Would you like to add another user? [y,n,q] (n)

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

Configuring SMTP email notification

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

Refer to the *Veritas Cluster Server Administrator’s Guide* for more information.
To configure SMTP email notification

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

2  Specify whether you want to configure the SMTP notification.

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

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

   See “Configuring SNMP trap notification” on page 129.

3  Provide information to configure SMTP notification.

   Provide the following information:

   ■ Enter the NIC information.

      Active NIC devices discovered on galaxy: hme0
      Enter the NIC for the VCS Notifier to use on galaxy: [b,q,?] (hme0)
      Is hme0 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
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: hme0
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 131.
3 Provide information to configure SNMP trap notification. Provide the following information:

■ Enter the NIC information.

Active NIC devices discovered on galaxy: hme0
Enter the NIC for the VCS Notifier to use on galaxy: [b,q,?] (hme0)
Is hme0 to be the public NIC used by all systems? [y,n,q,b,?] (y)

■ Enter the SNMP trap daemon port.

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

■ Enter the SNMP console system name.

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

■ Enter the minimum security level of messages to be sent to each console.

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

4 Add more SNMP consoles, if necessary.

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

Would you like to add another SNMP console? [y,n,q,b] (n) y
Enter the SNMP console system name: [b,q,?] jupiter
Enter the minimum severity of events for which SNMP traps should be sent to jupiter [I=Information, W=Warning, E=Error, S=SevereError]: [b,q,?] S

■ If you do not want to add, answer n.
Would you like to add another SNMP console? [y,n,q,b] (n)

5 Verify and confirm the SNMP notification information.

NIC: hme0
SNMP Port: 162
Console: saturn receives SNMP traps for Error or higher events
Console: jupiter receives SNMP traps for SevereError or higher events

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

Configuring global clusters

If you had installed a valid HA/DR license, the installer provides you an option to configure this cluster as global cluster. If not, the installer proceeds to configure 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: hme0
IP: 192.168.1.16
Netmask: 255.255.240.0

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

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

For IPv6:

Global Cluster Option configuration verification:

NIC: hme0
Prefix: 64

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

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

**Completing the VCS configuration**

After you enter the 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 185.

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 133.

See “Updating product licenses using vxlicinst” on page 134.

Checking licensing information on the system

You can use the vxlicrep program to display information about the licenses on a system.
To check licensing information

1. Navigate to the folder containing the `vxlicrep` program and enter:

   ```
   # vxlicrep
   ```

2. Review the following output to determine the following information:
   - The license key
   - The type of license
   - The product for which it applies
   - Its expiration date, if any. Demo keys have expiration dates. Permanent keys and site keys do not have expiration dates.

   ```
   License Key = xxx-xxx-xxx-xxx-xxx
   Product Name = Veritas Cluster Server
   Serial Number = xxxxx
   License Type = PERMANENT
   OEM ID = xxxxx
   
   Features :=
   Platform = Solaris
   Version = 6.0
   Tier = 0
   Reserved = 0
   Mode = VCS
   ```

Updating product licenses using `vxlicinst`

You can use the `vxlicinst` command 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 135.

To update product licenses

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

  ```
  # vxlicinst -k XXXX-XXXX-XXXX-XXXX-XXXX-XXX
  ```
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 XXXX-XXXX-XXXX-XXXX-XXXX-XXX
   ```
4. Make sure demo licenses are replaced on all cluster nodes before starting VCS.
   ```
   # vxlicrep
   ```
5. Start VCS on each node:
   ```
   # hastart
   ```
Verifying and updating licenses on the system
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:

   
   # devfsadm

2. To initialize the disks as VxVM disks, use one of the following methods:

   - Use the interactive vxdiskadm utility to initialize the disks as VxVM disks.
For more information see the Veritas Storage Foundation Administrator’s Guide.

- Use the `vxdisksetup` command to initialize a disk as a VxVM disk.

  ```
  # vxdisksetup -i device_name
  ```

  The example specifies the CDS format:

  ```
  # vxdisksetup -i c2t13d0
  ```

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

### 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 -fencing
   ```

   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 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 140.

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.
   ■ 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 to monitor the coordinator disks.
   See “Configuring CoordPoint agent to monitor coordination points” on page 248.

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 -1 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 141.

- Verifying that nodes have access to the same disk
  See “Verifying that the nodes have access to the same disk” on page 142.

- Testing the shared disks for SCSI-3
  See “Testing the disks using vxfentsthdw utility” on page 143.

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>libvx3par.so</td>
<td>3PARdata</td>
<td>VV</td>
</tr>
<tr>
<td>libvxCLARion.so</td>
<td>DGC</td>
<td>All</td>
</tr>
<tr>
<td>libvxFJTSye6k.so</td>
<td>FUJITSU</td>
<td>E6000</td>
</tr>
<tr>
<td>libvxFJTSye8k.so</td>
<td>FUJITSU</td>
<td>All</td>
</tr>
<tr>
<td>libvxap.so</td>
<td>SUN</td>
<td>All</td>
</tr>
<tr>
<td>libvxatf.so</td>
<td>VERITAS</td>
<td>ATFNODES</td>
</tr>
<tr>
<td>libvxcompellent.so</td>
<td>COMPELNT</td>
<td>Compellent Vol</td>
</tr>
<tr>
<td>libvxcopan.so</td>
<td>COPANSYS</td>
<td>8814, 8818</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.
# vxenadm -i diskpath

Refer to the vxenadm (1M) manual page.

For example, an EMC disk is accessible by the /dev/rdsk/c1t1d0s2 path on node A and the /dev/rdsk/c2t1d0s2 path on node B.

From node A, enter:

```
# vxenadm -i /dev/rdsk/c1t1d0s2
```

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

The same serial number information should appear when you enter the equivalent command on node B using the /dev/rdsk/c2t1d0s2 path.

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

```
# vxenadm -i /dev/rdsk/c3t1d2s2
```

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

---

**Testing the disks using vxfentsthdw utility**

This procedure uses the /dev/rdsk/c1t1d0s2 disk in the steps.

If the utility does not show a message that states a disk is ready, the verification has failed. Failure of verification can be the result of an improperly configured disk array. The failure can also be due to a bad disk.

If the failure is due to a bad disk, remove and replace it. The vxfentsthdw utility indicates a disk can be used for I/O fencing with a message resembling:

```
The disk /dev/rdsk/c1t1d0s2 is ready to be configured for I/O Fencing on node galaxy
```

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 493.

2. From one node, start the utility.
   Run the utility with the -n option if you use `rsh` for communication.
   ```
   # vxfentsthdw [-n]
   ```

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

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

   ************ WARNING!************
   THIS UTILITY WILL DESTROY THE DATA ON THE DISK!!
   Do you still want to continue : [y/n] (default: n) y
   Enter the first node of the cluster: galaxy
   Enter the second node of the cluster: nebula
4 Enter the names of the disks that you want to check. Each node may know
the same disk by a different name:

Enter the disk name to be checked for SCSI-3 PGR on node
IP_adrs_of_galaxy in the format:
for dmp: /dev/vx/rdmp/cxtxdxsx
for raw: /dev/rdsk/cxtxdxsx
Make sure it’s the same disk as seen by nodes
IP_adrs_of_galaxy and IP_adrs_of_nebula
/dev/rdsk/c2t13d0s2

Enter the disk name to be checked for SCSI-3 PGR on node
IP_adrs_of_nebula in the format:
for dmp: /dev/vx/rdmp/cxtxdxsx
for raw: /dev/rdsk/cxtxdxsx
Make sure it’s the same disk as seen by nodes
IP_adrs_of_galaxy and IP_adrs_of_nebula
/dev/rdsk/c2t13d0s2

If the serial numbers of the disks are not identical, then the test terminates.

5 Review the output as the utility performs the checks and reports its activities.

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

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

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

Setting up 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 “About planning to configure I/O fencing” on page 89.

See “Recommended CP server configurations” on page 93.

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 146.

Single CP server See “To configure server-based fencing for the VCS cluster (single CP server)” on page 151.

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.
  See “Setting up the CP server” on page 96.

- The coordination disks are verified for SCSI3-PR compliance.
  See “Checking shared disks for I/O fencing” on page 140.

2 Start the installvcs program with the -fencing option.

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

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 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 SCSI 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) c1t1d0s2
2) c2t1d0s2
3) c3t1d0s2

Please enter a valid disk which is available from all the cluster nodes for co-ordination point [1-3,q] 1

- If you have not already checked the disks for SCSI-3 PR compliance in step 1, check the disks now.

The installer displays a message that recommends you to verify the disks in another window and then return to this configuration procedure. Press Enter to continue, and confirm your disk selection at the installer prompt.

- Enter a disk group name for the coordinator disks or accept the default.

Enter the disk group name for coordinating disk(s):
[b] (vxfencoorddg)
9 Verify and confirm the coordination points information for the fencing configuration.

For example:

Total number of coordination points being used: 3
Coordination Point Server ([VIP or FQHN]:Port):
  1. 10.109.80.197 ([10.109.80.197]:14250)
SCSI-3 disks:
  1. c1t1d0s2
  2. c2t1d0s2
Disk Group name for the disks in customized fencing: vxfencoorddg
Disk policy used for customized fencing: raw

The installer initializes the disks and the disk group and deports the disk group on the 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 galaxy 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 nebula 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 galaxy .................................. Done
Updating /etc/vxfenmode file on nebula ........... ......................... Done

See “About I/O fencing configuration files” on page 462.

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] (vxefen)

Adding Coordination Point Agent via galaxy .... Done

15 Note the location of the configuration log files, summary files, and response files that the installer displays for later use.
To configure server-based fencing for the 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.
   
   See “Setting up the CP server” on page 96.

2. Start the installvcs program with `-fencing` option.
   
   ```
   # /opt/VRTS/install/installvcs -fencing
   ```
   
   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 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. 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.

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 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)

8 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)

9 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.

10 Verify and confirm the I/O fencing configuration information.

CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: clus1
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
11 Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the /etc/vxfenmode file with the appropriate details in each of the application cluster nodes.

The installer also populates the /etc/vxfenmode file with the entry single_cp=1 for such single CP server fencing configuration.

 Updating client cluster information on Coordination Point Server 10.210.80.197
 Adding the client cluster to the Coordination Point Server 10.210.80.197 ............ Done

 Registering client node galaxy 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 nebula 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 galaxy ................................ Done
 Updating /etc/vxfenmode file on nebula ................................. Done

 See “About I/O fencing configuration files” on page 462.

12 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.

13 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 galaxy ... Done

14 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.
   
   ```
   # /opt/VRTS/install/installvcs -fencing
   ```

   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 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/llttab 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 33.
To enable preferred fencing for the I/O fencing configuration

1. Make sure that the cluster is running with I/O fencing set up.
   
   # vxfenadm -d

2. Make sure that the cluster-level attribute UseFence has the value set to SCSI3.
   
   # haclus -value UseFence

3. To enable system-based race policy, perform the following steps:
   - Make the VCS configuration writable.
     
     # haconf -makerw
   - Set the value of the cluster-level attribute PreferredFencingPolicy as System.
     
     # haclus -modify PreferredFencingPolicy System
   - Set the value of the system-level attribute FencingWeight for each node in the cluster.
     For example, in a two-node cluster, where you want to assign galaxy five times more weight compared to nebula, run the following commands:
     
     # hasys -modify galaxy FencingWeight 50
     # hasys -modify nebula FencingWeight 10
   - Save the VCS configuration.
     
     # haconf -dump -makero

4. To enable group-based race policy, perform the following steps:
   - Make the VCS configuration writable.
     
     # haconf -makerw
   - Set the value of the cluster-level attribute PreferredFencingPolicy as Group.
     
     # haclus -modify PreferredFencingPolicy Group
   - Set the value of the group-level attribute Priority for each service group.
     For example, run the following command:
# hagrp -modify service_group Priority 1

Make sure that you assign a parent service group an equal or lower priority than its child service group. In case the parent and the child service groups are hosted in different subclusters, then the subcluster that hosts the child service group gets higher preference.

■ Save the VCS configuration.

  # haconf -dump -makero

5 To view the fencing node weights that are currently set in the fencing driver, run the following command:

  # vxfenconfig -a

To disable preferred fencing for the I/O fencing configuration

1 Make sure that the cluster is running with I/O fencing set up.

  # vxfenadm -d

2 Make sure that the cluster-level attribute UseFence has the value set to SCSI3.

  # haclus -value UseFence

3 To disable preferred fencing and use the default race policy, set the value of the cluster-level attribute PreferredFencingPolicy as Disabled.

  # haconf -makerw
  # haclus -modify PreferredFencingPolicy Disabled
  # haconf -dump -makero
Configuring VCS clusters for data integrity

Enabling or disabling the preferred fencing policy
Installation using the Web-based installer

- Chapter 10. Installing VCS
- Chapter 11. Configuring VCS
Installing VCS

This chapter includes the following topics:

- Before using the Veritas Web-based installer
- Starting the Veritas Web-based installer
- Obtaining a security exception on Mozilla Firefox
- Performing a pre-installation check with the Veritas Web-based installer
- Installing VCS with the Web-based installer

Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

<table>
<thead>
<tr>
<th>Table 10-1 Web-based installer requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
</tr>
<tr>
<td>Target system</td>
</tr>
<tr>
<td>Installation server</td>
</tr>
</tbody>
</table>
Table 10-1  Web-based installer requirements (continued)

<table>
<thead>
<tr>
<th>System</th>
<th>Function</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative system</td>
<td>The system where you run the Web browser to perform the installation.</td>
<td>Must have a Web browser. Supported browsers: Internet Explorer 6, 7, and 8 Firefox 3.x and later</td>
</tr>
</tbody>
</table>

Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

To start the Web-based installer

1. Start the Veritas XPortal Server process `xprt1wid`, on the installation server:

   ```
   # ./webinstaller start
   ```

   The webinstaller script displays a URL. Note this URL.

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

   The default listening port is 14172. If you have a firewall that blocks port 14172, use the `-port` option to use a free port instead.

2. On the administrative server, start the Web browser.

3. Navigate to the URL that the script displayed.

4. Certain browsers may display the following message:

   Secure Connection Failed

   Obtain a security exception for your browser.

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

5. Log in as superuser.

Obtaining a security exception on Mozilla Firefox

You may need to get a security exception on Mozilla Firefox.
The following instructions are general. They may change because of the rapid release cycle of Mozilla browsers.

To obtain a security exception

1. Click **Or you can add an exception** link.
2. Click **Add Exception** button.
3. Click **Get Certificate** button.
4. Uncheck **Permanently Store this exception checkbox (recommended)**.
5. Click **Confirm Security Exception** button.
6. Enter root in User Name field and root password of the web server in the Password field.

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

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

To perform a pre-installation check

1. Start the Web-based installer.
   
   See “Starting the Veritas Web-based installer” on page 162.

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

3. Select the Veritas Cluster Server from the **Product** drop-down list, and click **Next**.

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

5. The installer performs the precheck and displays the results.

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

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

Installing VCS with the Web-based installer

This section describes installing VCS with the Veritas Web-based installer.
To install VCS using the Web-based installer

1. Perform preliminary steps.
   See “Performing a pre-installation check with the Veritas Web-based installer” on page 163.

2. Start the Web-based installer.
   See “Starting the Veritas Web-based installer” on page 162.

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

4. Select **Veritas Cluster Server (VCS)** from the Product drop-down list, and click **Next**.

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

6. Choose minimal, recommended, or all packages. Click **Next**.

7. Indicate the systems where you want to install. Separate multiple system names with spaces. Click **Next**.

8. If you have not yet configured a communication mode among systems, you have the option to let the installer configure ssh or rsh. If you choose to allow this configuration, select the communication mode and provide the superuser passwords for the systems.

9. After the validation completes successfully, click **Next** to install VCS on the selected system.

10. After the installation completes, you must choose your licensing method. On the license page, select one of the following tabs:

    - **Keyless licensing**

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

    For more information, go to the following website:

    [http://go.symantec.com/sfhakeyless](http://go.symantec.com/sfhakeyless)

    Complete the following information:

    - Choose whether you want to enable Global Cluster option.
      Click **Register**.

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

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

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

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

12 If prompted, select the checkbox to specify whether you want to send your installation information to Symantec.

Would you like to send the information about this installation to Symantec to help improve installation in the future?

Click **Finish**. The installer prompts you for another task.
Installing VCS

Installing VCS with the Web-based installer
Configuring VCS

This chapter includes the following topics:

■ Configuring VCS using the Web-based installer

Configuring VCS using the Web-based installer

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

See “Getting your VCS installation and configuration information ready” on page 73.

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

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

To configure VCS on a cluster

1. Start the Web-based installer.
   See “Starting the Veritas Web-based installer” on page 162.

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

   Task               Configure a Product
   Product            Veritas Cluster Server

   Click Next.
3 On the Select Systems page, enter the system names where you want to configure VCS, and click Next.

Example: galaxy nebula

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

Click Next after the installer completes the system verification successfully.

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

To configure I/O fencing, click Yes.

To configure I/O fencing later, click No. You can configure I/O fencing later using the Web-based installer.

See “Configuring VCS for data integrity using the Web-based installer” on page 172.

You can also configure I/O fencing later using the installvcs -fencing command, the response files, or manually configure.
5 On the Set Cluster Name/ID page, specify the following information for the cluster.

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

Click **Next**.

6 On the Set Cluster Heartbeat page, select the heartbeat link details for the LLT type you chose on the Set Cluster Name/ID page.
For **LLT over Ethernet**: Do the following:

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

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

Click **Next**.

7 On the Optional Configuration page, decide the optional VCS features that you want to configure. Click the corresponding tab to specify the details for each option:

**Virtual IP**

- Select the **Configure Virtual IP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- Select the interface on which you want to configure the virtual IP.
- Enter a virtual IP address and value for the netmask. You can use an IPv4 or an IPv6 address.

**VCS Users**

- Reset the password for the Admin user, if necessary.
- Select the **Configure VCS users** option.
- Click **Add** to add a new user.
  
  Specify the user name, password, and user privileges for this user.

**SMTP**

- Select the **Configure SMTP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- If all the systems use the same NIC, select the NIC for the VCS Notifier to be used on all systems. If not, select the NIC to be used by each system.
- In the **SMTP Server** box, enter the domain-based hostname of the SMTP server. Example: smtp.yourcompany.com
- In the **Recipient** box, enter the full email address of the SMTP recipient. Example: user@yourcompany.com.
- In the **Event** list box, select the minimum security level of messages to be sent to each recipient.
- Click **Add** to add more SMTP recipients, if necessary.
SNMP
- Select the **Configure SNMP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- If all the systems use the same NIC, select the NIC for the VCS Notifier to be used on all systems. If not, select the NIC to be used by each system.
- In the **SNMP Port** box, enter the SNMP trap daemon port: (162).
- In the **Console System Name** box, enter the SNMP console system name.
- In the **Event** list box, select the minimum security level of messages to be sent to each console.
- Click **Add** to add more SNMP consoles, if necessary.

GCO
If you installed a valid HA/DR license, you can now enter the wide-area heartbeat link details for the global cluster that you would set up later.

See the *Veritas Cluster Server Administrator’s Guide* for instructions to set up VCS global clusters.

- Select the **Configure GCO** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- Select a NIC.
- Enter a virtual IP address and value for the netmask.
  You can use an IPv4 or an IPv6 address.

Security
To configure a secure VCS cluster, select the **Configure secure cluster** check box.

If you want to perform this task later, do not select the **Configure secure cluster** check box. You can use the `-security` option of the `installvcs` program.

Click **Next**.

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

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

If you did not choose to configure I/O fencing in step 4, then skip to step 11. Go to step 10 to configure fencing.
10 On the Select Fencing Type page, choose the type of fencing configuration:

- **Configure Coordination Point client based fencing**
  - Choose this option to configure server-based I/O fencing.

- **Configure disk based fencing**
  - Choose this option to configure disk-based I/O fencing.

Based on the fencing type you choose to configure, follow the installer prompts.

See “Configuring VCS for data integrity using the Web-based installer” on page 172.

11 Click **Next** to complete the process of configuring VCS.

On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

12 Select the checkbox to specify whether you want to send your installation information to Symantec.

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

### Configuring VCS for data integrity using the Web-based installer

After you configure VCS, you must configure the cluster for data integrity. Review the configuration requirements.

See “Configuring VCS using the Web-based installer” on page 167.

See “About planning to configure I/O fencing” on page 89.

**To configure VCS for data integrity**

1 Start the Web-based installer.

   See “Starting the Veritas Web-based installer” on page 162.

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

   - **Task**: I/O fencing configuration
   - **Product**: Veritas Cluster Server

   Click **Next**.

3 Verify the cluster information that the installer presents and confirm whether you want to configure I/O fencing on the cluster.
4 On the Select Cluster page, click **Next** if the installer completes the cluster verification successfully.

The installer performs the initial system verification. It checks for the system communication. It also checks for release compatibility, installed product version, platform version, and performs product prechecks.

5 On the Select Fencing Type page, choose whether to configure disk-based fencing or server-based fencing.

If you chose to configure disk-based fencing, go to step 7.

If you chose to configure server-based fencing, go to step 10.

6 In the Confirmation dialog box that appears, confirm whether your storage environment supports SCSI-3 PR.

You can configure non-SCSI-3 server-based fencing in a virtual environment that is not SCSI-3 PR compliant.

7 On the Configure Fencing page, the installer prompts for details based on the fencing type you chose to configure. Specify the coordination points details.

Click **Next**.

8 On the Configure Fencing page, specify the following information:

   **Select a Disk Group**

   Select the **Create a new disk group** option or select one of the disk groups from the list.

   - If you selected one of the disk groups that is listed, choose the fencing disk policy for the disk group. Go to step 16.
   - If you selected the **Create a new disk group** option, make sure you have SCSI-3 PR enabled disks, and click **Yes** in the confirmation dialog box. Click **Next**. Go to step 9.
9 On the Create New DG page, specify the following information:

**New Disk Group Name**  Enter a name for the new coordinator disk group you want to create.

**Select Disks**  Select at least three disks to create the coordinator disk group.

If you want to select more than three disks, make sure to select an odd number of disks.

**Fencing Disk Policy**  Choose the fencing disk policy for the disk group.

Go to step 16.

10 On the Configure Fencing page, the installer prompts for details based on the fencing type you chose to configure. Specify the coordination points details. Click Next.

11 Provide the following details for each of the CP servers:

- Enter the virtual IP addresses or host names of the virtual IP address. The installer assumes these values to be identical as viewed from all the application cluster nodes.
- Enter the port that the CP server must listen on.
- Click Next.

12 If your server-based fencing configuration also uses disks as coordination points, perform the following steps:

- If you have not already checked the disks for SCSI-3 PR compliance, check the disks now, and click OK in the dialog box.
- If you do not want to use the default coordinator disk group name, enter a name for the new coordinator disk group you want to create.
- Select the disks to create the coordinator disk group.
- Choose the fencing disk policy for the disk group.

13 In the Confirmation dialog box that appears, confirm whether the coordination points information you provided is correct, and click Yes.

14 Verify and confirm the I/O fencing configuration information.

The installer stops and restarts the VCS and the fencing processes on each application cluster node, and completes the I/O fencing configuration.

15 Configure the CP agent on the VCS (application cluster), and click Next.
16 Click **Next** to complete the process of configuring I/O fencing.

   On the Completion page, view the summary file, log file, or response file, if needed, to confirm the configuration.

17 Select the checkbox to specify whether you want to send your installation information to Symantec.

   Click **Finish**. The installer prompts you for another task.
Installation using response files

- Chapter 12. Performing automated VCS installation
- Chapter 13. Performing automated VCS configuration
- Chapter 14. Performing automated I/O fencing configuration for VCS
Performing 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 35.

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.
   
   See “Sample response file for installing VCS” on page 182.

4. Edit the values of the response file variables as necessary.
   
   See “Response file variables to install VCS” on page 180.
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:

```bash
# ./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 12-1** 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 packages. (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 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>
<tr>
<td>Variable</td>
<td>List or Scalar</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| CFG{opt}{installallpkgs} or CFG{opt}{installrecpkgs} or CFG{opt}{installminpkgs} | Scalar | Instructs the installer to install VCS packages based on the variable that has the value set to 1:  
- `installallpkgs`: Installs all packages  
- `installrecpkgs`: Installs recommended packages  
- `installminpkgs`: Installs minimum packages  
**Note**: The installer requires only one of these variable values to be set to 1.  
*(Required)* |
| CFG{opt}{rsh} | Scalar | Defines that `rsh` must be used instead of `ssh` as the communication method between systems.  
*(Optional)* |
| CFG{opt}{gco} | Scalar | 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)* |
| CFG{opt}{keyfile} | Scalar | Defines the location of an `ssh` keyfile that is used to communicate with all remote systems.  
*(Optional)* |
| CFG{opt}{patchpath} | Scalar | 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)* |
### Table 12-1  
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][pkgpath]</td>
<td>Scalar</td>
<td>Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems. <em>(Optional)</em></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 packages that are needed during the install. The default location is /var/tmp. <em>(Optional)</em></td>
</tr>
</tbody>
</table>
| CFG[opt][logpath]             | Scalar         | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.  
**Note:** The installer copies the response files and summary files also to the specified logpath location. *(Optional)* |
| CFG[opt][vxkeyless]           | Scalar         | Installs the product with keyless license if the value is set to 1. If the value is set to 0, you must define the CFG[keys][system] variable with the license keys. *(Optional)* |
| CFG[keys]                     |                | List of keys to be registered on the system if the variable $CFG[opt][vxkeyless]$ is set to 0. *(Optional)* |

---

**Sample response file for installing VCS**

Review the response file variables and their definitions.
See “Response file variables to install VCS” on page 180.

# Configuration Values:
#
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installrecpkgs}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw(galaxy nebula) ];
1;
Performing automated VCS installation

Sample response file for installing VCS
Performing 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 packages 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 195.
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 186.

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

```
# /opt/VRTS/install/installvcs -responsefile /tmp/response_file
```

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

Response file variables to configure Veritas Cluster Server

Table 13-1 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[opt][configure]</td>
<td>Scalar</td>
<td>Performs the configuration if the packages are already installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Required)</td>
</tr>
<tr>
<td>CFG[systems]</td>
<td>List</td>
<td>List of systems on which the product is to be configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Required)</td>
</tr>
<tr>
<td>CFG[prod]</td>
<td>Scalar</td>
<td>Defines the product to be configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value is VCS60 for VCS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
</tbody>
</table>
### Table 13-1  
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{opt}{rsh}</td>
<td>Scalar</td>
<td>Defines that <code>rsh</code> must be used instead of <code>ssh</code> as the communication method between systems.</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 <code>/opt/VRTS/install/logs</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The installer copies the response files and summary files also to the specified <code>logpath</code> location.</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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value 0 indicates that the installation logs are not uploaded to the Symantec Web site.</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 13-2 lists the response file variables that specify the required information to configure a basic VCS cluster.
### Table 13-2  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 13-3 lists the response file variables that specify the required information to configure LLT over Ethernet.

### Table 13-3  Response file variables specific to configuring private LLT over Ethernet

<table>
<thead>
<tr>
<th>Variable</th>
<th>List or Scalar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG{vcs_lltlink#}</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>
<tr>
<td>{&quot;system&quot;}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 13-3  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_ltlkowpri#} {&quot;system&quot;}</td>
<td>Scalar</td>
<td>Defines a low priority heartbeat link. Typically, ltlkowpri is used on a public network link to provide an additional layer of communication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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, ltlkowpri1, ltlkowpri2, and so on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must enclose the system name within double quotes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
</tbody>
</table>

Table 13-4 lists the response file variables that specify the required information to configure LLT over UDP.

Table 13-4  Response file variables specific to configuring LLT over UDP

<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} {&lt;system1&gt;}</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>

Performing automated VCS configuration
Response file variables to configure Veritas Cluster Server
<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;_address} {&lt;system1&gt;}</td>
<td>Scalar</td>
<td>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 &lt;n&gt; for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required)</td>
</tr>
<tr>
<td>CFG{vcs_udplink&lt;n&gt;_port} {&lt;system1&gt;}</td>
<td>Scalar</td>
<td>Stores the UDP port (16-bit integer value) 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>
<tr>
<td>CFG{vcs_udplinklowpri&lt;n&gt;_port} {&lt;system1&gt;}</td>
<td>Scalar</td>
<td>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 &lt;n&gt; for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required)</td>
</tr>
<tr>
<td>CFG{vcs_udplink&lt;n&gt;_netmask} {&lt;system1&gt;}</td>
<td>Scalar</td>
<td>Stores the netmask (prefix for 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>
### Table 13-4
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{vcs_udplinklowpri&lt;n&gt;_netmask}</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 13-5 lists the response file variables that specify the required information to configure virtual IP for VCS cluster.

### Table 13-5
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}</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 13-6 lists the response file variables that specify the required information to configure the VCS cluster in secure mode.
### Table 13-6
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>
</tbody>
</table>

### Table 13-7
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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Administrators Operators Guests&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The order of the values for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the vcs_userenpw list must match the order of the values in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vcs_username list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
<tr>
<td>CFG[vcs_username]</td>
<td>List</td>
<td>List of names of VCS users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
</tbody>
</table>
Table 13-7  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_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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
</tbody>
</table>

Table 13-8 lists the response file variables that specify the required information to configure VCS notifications using SMTP.

Table 13-8  Response file variables specific to configuring VCS notifications using SMTP

<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
<tr>
<td>CFG{vcs_smtprsev}</td>
<td>List</td>
<td>Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SMTP recipients are to receive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that the ordering of severity levels must match that of the addresses of SMTP recipients.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
</tbody>
</table>

Table 13-9 lists the response file variables that specify the required information to configure VCS notifications using SNMP.
Table 13-9  Response file variables specific to configuring VCS notifications using SNMP

<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).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
<tr>
<td>CFG[vcs_snmpcons]</td>
<td>List</td>
<td>List of SNMP console system names</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
</tbody>
</table>

Table 13-10 lists the response file variables that specify the required information to configure VCS global clusters.

Table 13-10  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]</td>
<td>Scalar</td>
<td>Defines the NIC for the Virtual IP that the Global Cluster Option uses.</td>
</tr>
<tr>
<td>[system]</td>
<td></td>
<td>You can enter 'all' as a system value if the same NIC is used on all systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional)</td>
</tr>
<tr>
<td>CFG[vcs_gconetmask]</td>
<td>Scalar</td>
<td>Defines the Netmask of the virtual IP address that the Global Cluster Option uses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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 186.

Note: For Solaris x64 Platform Edition, read the values of NICs as e1000g0, e1000g2, and e1000g3 instead of hme0, qfe0, qfe1 in the sample response file.

# Configuration Values:
#
our %CFG;

$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=13221;
$CFG{vcs_clustername}="clus1";
$CFG{vcs_csgnetmask}="255.255.255.0";
$CFG{vcs_csgnic}{all}="hme0";
$CFG{vcs_csgvip}="10.10.12.1";
$CFG{vcs_gconetmask}="255.255.255.0";
$CFG{vcs_gcovip}="10.10.12.1";
$CFG{vcs_lltlink1}{galaxy}="qfe0";
$CFG{vcs_lltlink1}{nebula}="qfe0";
$CFG{vcs_lltlink2}{galaxy}="qfe1";
$CFG{vcs_lltlink2}{nebula}="qfe1";

$CFG{vcs_smtprecp}=[ qw(earnie@symantecexample.com) ];
$CFG{vcs_smtpserver}=[ qw(SevereError) ];
$CFG{vcs_smtpserver}="smtp.symantecexample.com";
$CFG{vcs_snmpccons}=[ qw(neptune) ];
$CFG{vcs_snmpcsev}=[ qw(SevereError) ];
$CFG{vcs_snmpport}=162;
1;
Performing automated VCS configuration

Sample response file for configuring VCS
Performing automated I/O fencing configuration for VCS

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.

See “About planning to configure I/O fencing” on page 89.
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 199.
See “Sample response file for configuring server-based I/O fencing” on page 202.

4 Edit the values of the response file variables as necessary.
See “Response file variables to configure disk-based I/O fencing” on page 198.
See “Response file variables to configure server-based I/O fencing” on page 200.

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

```
# /opt/VRTS/install/installvcs -responsefile /tmp/response_file
```
Where /tmp/response_file is the response file’s full path name.

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

*Table 14-1* lists the response file variables that specify the required information to configure disk-based I/O fencing for VCS.

<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>
<tr>
<td>CFG[fencing_option]</td>
<td>Scalar</td>
<td>Specifies the I/O fencing configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 1—Coordination Point Server-based I/O fencing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 2—Coordinator disk-based I/O fencing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 3—Disabled mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 4—Fencing migration when the cluster is online (Required)</td>
</tr>
</tbody>
</table>
Table 14-1  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_scsi3_disk_policy]</td>
<td>Scalar</td>
<td>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)</td>
</tr>
<tr>
<td>CFG[fencing_dgname]</td>
<td>Scalar</td>
<td>Specifies the disk group for I/O fencing. (Optional) <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>CFG[fencing_newdg_disks]</td>
<td>List</td>
<td>Specifies the disks to use to create a new disk group for I/O fencing. (Optional) <strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>

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 198.

```
# Configuration Values:
```
Response file variables to configure server-based I/O fencing

You can use a coordination point server-based fencing response file to configure server-based customized I/O fencing.

Table 14-2 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>
</tbody>
</table>
### Table 14-2  
Coordination point server (CP server) based fencing response file definitions (continued)

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

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

```bash
$CFG{fencing_config_cpagent}=0;
$CFG{fencing_cps}=[ qw(10.200.117.145) ];
$CFG{fencing_cps_vips}{"10.200.117.145"}=[ qw(10.200.117.145) ];
$CFG{fencing_dgname}="vxfencoordg";
$CFG{fencing_disks}=[ qw(emc_clariion0_37 emc_clariion0_13) ];
$CFG{fencing_scsi3_disk_policy}="raw";
$CFG{fencing_ncp}=3;
$CFG{fencing_ndisks}=2;
$CFG{fencing_ports}{"10.200.117.145"}=14250;
$CFG{fencing_reusedg}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{fencing_option}=1;
```

Response file variables to configure non-SCSI-3 server-based I/O fencing

Table 14-3 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 31.

<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.</td>
</tr>
<tr>
<td></td>
<td>Valid values are 1 or 0. Enter 1 to configure non-SCSI-3 server-based I/O fencing.</td>
</tr>
</tbody>
</table>
Table 14-3 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_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 &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>
<tr>
<td>CFG {fencing_cpagentgrp}</td>
<td>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'.</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:

```plaintext
$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;
```
Performing automated I/O fencing configuration for VCS

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

```
$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(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{fencing_option}=1;
```
Manual installation

- Chapter 15. Performing preinstallation tasks
- Chapter 16. Manually installing VCS
- Chapter 17. Manually configuring VCS
- Chapter 18. 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.
   
   See “Mounting the product disc” on page 71.
3. Copy the files to a temporary location on the system.

   # cp -r packages/* /tmp/install

Requirements for installing VCS

Review requirements before you install.

See “Important preinstallation information for VCS” on page 35.
Performing preinstallation tasks

Requirements for installing VCS
Manually installing VCS

This chapter includes the following topics:

■ About VCS manual installation
■ Installing VCS software manually
■ Installing using JumpStart

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

If you manually install VCS software to upgrade your cluster, make sure to back up the previous VCS configuration files before you start the installation. These files follow:

■ /etc/VRTSvcs/conf/config
■ /etc/ltttab
■ /etc/gabtab
■ /etc/lthosts
■ /etc/default/vcs
■ /opt/VRTSvcs/bin/vcsenv
Table 16-1 lists the tasks that you must perform when you manually install and configure VCS 6.0.

<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 “Installing VCS packages for a manual installation” on page 211.</td>
</tr>
<tr>
<td>Install VCS language pack software manually on each node in the cluster.</td>
<td>See “Installing language packages in a manual installation” on page 212.</td>
</tr>
<tr>
<td>Add a license key.</td>
<td>See “Adding a license key for a manual installation” on page 213.</td>
</tr>
<tr>
<td>Copy the installation guide to each node.</td>
<td>See “Copying the installation guide to each node” on page 215.</td>
</tr>
<tr>
<td>Configure LLT and GAB.</td>
<td>■ See “Configuring LLT manually” on page 223.</td>
</tr>
<tr>
<td>■ See “Configuring GAB manually” on page 227.</td>
<td></td>
</tr>
<tr>
<td>Configure VCS.</td>
<td>See “Configuring VCS manually” on page 228.</td>
</tr>
<tr>
<td>Start LLT, GAB, and VCS services.</td>
<td>See “Starting LLT, GAB, and VCS after manual configuration” on page 230.</td>
</tr>
<tr>
<td>Modify the VCS configuration.</td>
<td>See “Modifying the VCS configuration” on page 232.</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 215.</td>
</tr>
</tbody>
</table>

Viewing the list of VCS packages

During the VCS installation, the installer prompts you with an option to choose the VCS packages to install. You can view the list of packages 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 packages in a specified order. For example, you must install some packages before other packages because of various product dependencies. The following installer command options list the packages in the order in which you must install these packages.

Table 16-2 describes the VCS package installation options and the corresponding command to view the list of packages.
Table 16-2  Installer command options to view VCS packages

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

To view the list of VCS packages

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 packages. Based on what packages you want to install, enter the appropriate command option:
   
   ```
   # ./installvcs -minpkgs
   
   Or
   
   # ./installvcs -recpkgs
   
   Or
   
   # ./installvcs -allpkgs
   ```

Installing VCS packages for a manual installation

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

You can create lists of the packages to install.

See “Viewing the list of VCS packages” on page 210.

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

- Install the following required packages in the order shown:

  # pkgadd -d VRTSvlic.pkg
  # pkgadd -d VRTSperl.pkg
  # pkgadd -d VRTSspt.pkg
  # pkgadd -d VRTSllt.pkg
  # pkgadd -d VRTSgab.pkg
  # pkgadd -d VRTSvxfen.pkg
  # pkgadd -d VRTSsamf.pkg
  # pkgadd -d VRTSvcs.pkg
  # pkgadd -d VRTScps.pkg
  # pkgadd -d VRTSvcsag.pkg
  # pkgadd -d VRTSvcesa.pkg
  # pkgadd -d VRTSsfmh.pkg
  # pkgadd -d VRTSvbs.pkg
  # pkgadd -d VRTSsfcp60.pkg

---

**Note:** To configure an Oracle VM Server logical domain for disaster recovery, install the following required package inside the logical domain:

# pkgadd -d VRTSvcsnr.pkg

See “Veritas Cluster Server installation packages” on page 413.

Installing language packages in a manual installation

Install the language packages that VCS requires after you install the base VCS packages.

See “Veritas Cluster Server installation packages” on page 413.

Before you install, make sure that you are logged on as superuser and that you have mounted the language disc.

See “Mounting the product disc” on page 71.

Perform the steps on each node in the cluster to install the language packages.
To install the language packages on a node

1. Copy the package files from the software disc to the temporary directory.

   ```
cp -r pkgs/* /tmp
   ```

2. Install the following required and optional VCS packages from the compressed files:

   - Install the following required packages in the order shown for Chinese language support:
     ```
     # pkgadd -d VRTSmulic.pkg
     # pkgadd -d VRTSzhvm.pkg
     ```

   - Install the following required packages in the order shown for Japanese language support:
     ```
     # pkgadd -d VRTSmulic.pkg
     # pkgadd -dVRTSjacav.pkg
     # pkgadd -d VRTSjacse.pkg
     # pkgadd -d VRTSjacs.pkg
     # pkgadd -d VRTSjacsu.pkg
     # pkgadd -d VRTSjadba.pkg
     # pkgadd -d VRTSjadbe.pkg
     # pkgadd -d VRTSjafs.pkg
     # pkgadd -d VRTSjaodm.pkg
     # pkgadd -d VRTSjavm.pkg
     ```

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 213.

After you have installed all packages 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. In order to use keyless licensing, you must set up a Management Server to manage your systems.
For more information and to download the management server, see the following URL:

http://go.symantec.com/vom

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

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

**To set or change the product level**

1. Show your current working directory:

   ```
   # pwd
   
   Output resembles:
   
   /opt/VRTSvlic/bin
   ```

2. View the current setting for the product level.

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

3. View the possible settings for the product level.

   ```
   # ./vxkeyless displayall
   ```

4. Set the desired product level.

   ```
   # ./vxkeyless set prod_levels
   
   where `prod_levels` is a comma-separated list of keywords. The keywords are the product levels as shown by the output of step 3.
   ```

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

---

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

1. View the current setting for the product license level.
   
   ```
   # ./vxkeyless [-v] display
   ```

2. If there are keyless licenses installed, remove all keyless licenses:
   
   ```
   # ./vxkeyless [-q] set NONE
   ```

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

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 133.

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 `/opt/VRTS/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.

Installing using JumpStart

These JumpStart instructions assume a working knowledge of JumpStart. See the JumpStart documentation that came with your operating system for details on using JumpStart.

Upgrading is not supported. The following procedure assumes a stand-alone configuration.

For the language pack, you can use JumpStart to install packages. You add the language packages in the script, and put those files in the JumpStart server directory.

You can use a Flash archive to install VCS and the operating system in conjunction with JumpStart.

See “Using a Flash archive to install VCS and the operating system” on page 219.

Overview of JumpStart installation tasks

Review the summary of tasks before you perform the JumpStart installation.

Summary of tasks

1  Add a client (register to the JumpStart server). See the JumpStart documentation that came with your operating system for details.

2  Read the JumpStart installation instructions.

3  Generate the finish scripts.

   See “Generating the finish scripts” on page 217.

4  Prepare shared storage installation resources.

   See “Preparing installation resources” on page 217.

5  Modify the rules file for JumpStart.

   See the JumpStart documentation that came with your operating system for details.

6  Install the operating system using the JumpStart server.

7  When the system is up and running, run the installer command from the installation media to configure the Veritas software.

   # /opt/VRTS/install/installer -configure
Generating the finish scripts

Perform these steps to generate the finish scripts to install VCS.

To generate the script

1. Run the product installer program to generate the scripts for all products.
   
   ```
   ./installer -jumpstart directory_to_generate_scripts
   
   Or
   
   ./installprod -jumpstart directory_to_generate_script
   ```
   
   Where `prod` is the product's installation command, and `directory_to_generate_scripts` is where you want to put the product's script.
   
   For example:
   
   ```
   # ./installvcs -jumpstart /js_scripts
   ```

2. Modify the JumpStart script according to your requirements. You must modify the BUILDSRC and ENCAPSRC values. Keep the values aligned with the resource location values.

   ```
   BUILDSRC="hostname_or_ip:/path_to_pkgs"
   
   // If you don't want to encapsulate the root disk automatically
   // comment out the following line.
   
   ENCAPSRC="hostname_or_ip:/path_to_encap_script"
   ```

Preparing installation resources

Prepare resources for the JumpStart installation.
To prepare the resources

1. Copy the pkgs directory of the installation media to the shared storage.

```bash
# cd /path_to_installation_media
# cp -r pkgs BUILDSRC
```

2. Generate the response file with the list of packages.

```bash
# cd BUILDSRC/pkgs/
# pkgask -r package_name.response -d /BUILDSRC/pkgs/packages_name.pkg
```

3. Create the adminfile file under BUILDSRC/pkgs/ directory.

```plaintext
m@mail= instance=overwrite partial=nocheck runlevel=quit
idepend=quit rdepend=nocheck space=quit setuid=nocheck
conflict=nocheck action=nocheck
basedir=default
```

Adding language pack information to the finish file

To add the language pack information to the finish file, perform the following procedure.
To add the language pack information to the finish file

1  For the language pack, copy the language packages from the language pack installation disc to the shared storage.

```bash
# cd /cdrom/cdrom0/pkgs
# cp -r * BUILDSRC/pkgs
```

If you downloaded the language pack:

```bash
# cd /path_to_language_pack_installation_media/pkgs
# cp -r * BUILDSRC/pkgs
```

2  In the finish script, copy the product package information and replace the product packages with language packages.

3  The finish script resembles:

```bash
... for PKG in product_packages
do ...
done ...
for PKG in language_packages
do ...
done ...
```

Using a Flash archive to install VCS and the operating system

You can only use Flash archive on the Solaris 10 operating system. In the following outline, refer to Solaris documentation for Solars-specific tasks.

---

**Note:** Symantec does not support Flash Archive installation if the root disk of the master system is encapsulated.

---

The following is an overview of the creation and installation of a Flash archive with Veritas software.

- If you plan to start flar (flash archive) creation from bare metal, perform step 1 through step 10.

- If you plan to start flar creation from a system where you have installed but not configured the product, perform step 1 through step 4. Skip step 5 and finish step 6 through step 10.
If you plan to start flar creation from a system where you have installed and configured the product, perform step 5 through step 10.

**Flash archive creation overview**

1. Ensure that you have installed Solaris 10 on the master system.
2. Use JumpStart to create a clone of a system.
3. Reboot the cloned system.
4. Install the Veritas products on the master system.
   Perform one of the installation procedures from this guide.
5. If you have configured the product on the master system, create the vrts_deployment.sh file and the vrts_deployment.cf file and copy them to the master system.
   See “Creating the Veritas post-deployment scripts” on page 220.
6. Use the `flarcreate` command to create the Flash archive on the master system.
7. Copy the archive back to the JumpStart server.
8. Use JumpStart to install the Flash archive to the selected systems.
9. Configure the Veritas product on all nodes in the cluster. Start configuration with the following command:

**Creating the Veritas post-deployment scripts**

The generated files vrts_deployment.sh and vrts_post-deployment.cf are customized Flash archive post-deployment scripts. These files clean up Veritas product settings on a cloned system before you reboot it for the first time. Include these files in your Flash archives.

**To create the post-deployment scripts**

1. Mount the product disc.
2. From the prompt, run the `-flash_archive` option for the installer. Specify a directory where you want to create the files.
   
   ```
   # ./installer -flash_archive /tmp
   ```
3. Copy the `vrts_postedeployment.sh` file and the `vrts_postedeployment.cf` file to the golden system.
4 On the golden system perform the following:
   ■ Put the vrts_postdeployment.sh file in the /etc/flash/postdeployment directory.
   ■ Put the vrts_postdeployment.cf file in the /etc/vx directory.

5 Make sure that the two files have the following ownership and permissions:

   # chown root:root /etc/flash/postdeployment/vrts_postdeployment.sh
   # chmod 755 /etc/flash/postdeployment/vrts_postdeployment.sh
   # chown root:root /etc/vx/vrts_postdeployment.cf
   # chmod 644 /etc/vx/vrts_postdeployment.cf

   Note that you only need these files in a Flash archive where you have installed Veritas products.
Manually installing VCS

Installing using JumpStart
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 224.
- Set up the file `/etc/llttab`. 
  See “Setting up /etc/llttab for a manual installation” on page 224.
- 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/default/llt`

You can also configure LLT over UDP.

See “Using the UDP layer for LLT” on page 475.

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 galaxy
1 nebula
```

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 225.

Run the `dladm show-dev` command to query all NICs.

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

- For SPARC:
  
  ```
  set-node galaxy
  set-cluster 2
  ```
For x64:

```
set-node galaxy
set-cluster 2
link e1000g0 /dev/e1000g:0 - ether - -
link e1000g1 /dev/e1000g:1 - ether - -
link-lowpri e1000g2 /dev/e1000g:2 - ether - -
```

The first line must identify the system where the file exists. In the example, the value for `set-node` can be: `galaxy`, `0`, or the file name `/etc/nodename`. The file needs to contain the name of the system (galaxy in this example). 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 the following:

For SPARC:

```
set-node galaxy
set-cluster 2
link qfe0 qfe:0 - ether - -
link qfe1 qfe:1 - ether - -
link-lowpri qfe2 qfe:2 - ether - -
```

For x64:

```
set-node galaxy
set-cluster 2
link e1000g0 /dev/e1000g:0 - ether - -
link e1000g1 /dev/e1000g:1 - ether - -
link-lowpri e1000g2 /dev/e1000g:2 - ether - -
```

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

*Table 17-1* 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>set-node</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 0-31. The symbolic name corresponds to the system ID, which is in /etc/llthosts file. Note that LLT fails to operate if any systems share the same ID.</td>
</tr>
<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 is the device name of the network interface. Its format is device_name:device_instance_number. 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.

By default, Oracle systems assign the same MAC address to all interfaces. Thus, connecting two or more interfaces to a network switch can cause problems. Consider the following example. You configure an IP on one public interface and LLT on another. Both interfaces are connected to a switch. The duplicate MAC address on the two switch ports can cause the switch to incorrectly redirect IP traffic to the LLT interface and vice versa. To avoid this issue, configure the system to assign unique MAC addresses by setting the `eeprom(1M)` parameter `local-mac-address?` to true.

**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 -n

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 for /sbin/gabconfig. Using -c -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/default/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 resources.
- 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 resources. 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 galaxy ( )
   system nebula ( )
   ```

   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/default/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 228.

To configure VCS in single node mode

1. Copy the SMF service manifest file `vcs-onenode.xml` from `/etc/VRTSvcs/conf` to `/var/svc/manifest/system`.
   
   ```
   # cp /etc/VRTSvcs/conf/vcs-onenode.xml /var/svc/manifest/system
   ```

2. Disable the VCS SMF service imported by VRTSvcs package.
   
   ```
   # svcadm disable -s system/vcs:default
   ```

3. Delete the VCS SMF service configuration.
   
   ```
   # svccfg delete -f system/vcs:default
   ```

4. Edit the following file to change the value of the ONENODE environment variable to `yes`.
   
   `/etc/default/vcs`

5. Import the SMF service for vcs-onenode.
   
   ```
   # svccfg import /var/svc/manifest/system/vcs-onenode.xml
   ```

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:

   # svcadm enable llt

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

   Sep 1 19:12:57 galaxy kernel: LLT INFO V-14-1-10009
   LLT 5.1.100.00 Protocol available

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:

   # svcadm enable gab

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

   Sep 1 19:13:35 galaxy kernel: GAB INFO V-15-1-20021
   GAB 5.1.100.00 available

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:

   # svcadm enable vcs

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

   Apr 5 14:52:02 galaxy gab: GAB:20036: Port h gen 3972a201
   membership 01

See “Verifying the cluster” on page 351.
To start VCS as single node

- Run the following command:

  `# svcadm enable vcs-onenode`

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 459.
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 18-1 lists the tasks that are involved in setting up I/O fencing.

**Table 18-1** 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 137.</td>
</tr>
<tr>
<td>Identifying disks to use as coordinator disks</td>
<td>See “Identifying disks to use as coordinator disks” on page 234.</td>
</tr>
<tr>
<td>Checking shared disks for I/O fencing</td>
<td>See “Checking shared disks for I/O fencing” on page 140.</td>
</tr>
<tr>
<td>Setting up coordinator disk groups</td>
<td>See “Setting up coordinator disk groups” on page 234.</td>
</tr>
<tr>
<td>Creating I/O fencing configuration files</td>
<td>See “Creating I/O fencing configuration files” on page 235.</td>
</tr>
</tbody>
</table>
### Table 18-1 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 236.</td>
</tr>
<tr>
<td>Configuring CoordPoint agent to monitor coordination points</td>
<td>See “Configuring CoordPoint agent to monitor coordination points” on page 248.</td>
</tr>
<tr>
<td>Verifying I/O fencing configuration</td>
<td>See “Verifying I/O fencing configuration” on page 238.</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 137.

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 140.

## Setting up coordinator disk groups

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

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

Refer to the *Veritas Storage Foundation Administrator’s Guide* for details on how to create disk groups.

The following example procedure assumes that the disks have the device names c1t1d0s2, c2t1d0s2, and c3t1d0s2.
To create the vxfencoorddg disk group

1. On any node, create the disk group by specifying the device names:
   
   ```bash
   # vxdg init vxfencoorddg c1t1d0s2 c2t1d0s2 c3t1d0s2
   ```

2. Set the coordinator attribute value as "on" for the coordinator disk group:
   
   ```bash
   # vxdg -g vxfencoorddg set coordinator=on
   ```

3. Deport the coordinator disk group:
   
   ```bash
   # vxdg deport vxfencoorddg
   ```

4. Import the disk group with the \(-t\) option to avoid automatically importing it when the nodes restart:
   
   ```bash
   # vxdg -t import vxfencoorddg
   ```

5. Deport the disk group. Deporting the disk group prevents the coordinator disks from serving other purposes:
   
   ```bash
   # vxdg deport vxfencoorddg
   ```

Creating I/O fencing configuration files

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

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

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

1. On each nodes, type:
   
   ```bash
   # 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. If the I/O fencing driver vxfen is already running, stop the I/O fencing driver.
   ```
   # svcadm disable -t vxfen
   ```

4. Make a backup copy of the main.cf file:
   ```
   # cd /etc/VRTSvcs/conf/config
   # cp main.cf main.orig
   ```
5 On one node, use vi or another text editor to edit the main.cf file. To modify the list of cluster attributes, add the UseFence attribute and assign its value as SCSI3.

```sh
cluster clus1{
  UserNames = { admin = "cDRpdxPmHpzS." }
  Administrators = { admin }
  HacliUserLevel = COMMANDROOT
  CounterInterval = 5
  UseFence = SCSI3
}
```

Regardless of whether the fencing configuration is disk-based or server-based, the value of the cluster-level attribute UseFence is set to SCSI3.

6 Save and close the file.

7 Verify the syntax of the file /etc/VRTSvcs/conf/config/main.cf:

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

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

For example, on each remaining node, enter:

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

9 Start the I/O fencing driver and VCS. Perform the following steps on each node:

- Start the I/O fencing driver.
  The vxfen startup script also invokes the vxfenconfig command, which configures the vxfen driver to start and use the coordination points that are listed in /etc/vxfentab.

```sh
# svcadm enable vxfen
```

- Start VCS.

```sh
# /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:

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

RFSM State Information:
   node 0 in state 8 (running)
   node 1 in state 8 (running)
```

2 Verify that the disk-based I/O fencing is using the specified disks.

```bash
# 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 18-2  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 239.</td>
</tr>
</tbody>
</table>
Table 18-2  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 242.</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 236.</td>
</tr>
<tr>
<td>Configuring Coordination Point agent to monitor coordination points</td>
<td>See “Configuring CoordPoint agent to monitor coordination points” on page 248.</td>
</tr>
<tr>
<td>Verifying the server-based I/O fencing configuration</td>
<td>See “Verifying server-based I/O fencing configuration” on page 249.</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 18-3 displays the sample values used in this procedure.

Table 18-3  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>mycps1</td>
</tr>
<tr>
<td>Node #1 - VCS cluster</td>
<td>galaxy</td>
</tr>
<tr>
<td>Node #2 - VCS cluster</td>
<td>nebula</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 (galaxy):

   
   ```
   # 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 mycps1.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>galaxy(0)</td>
<td>0</td>
</tr>
<tr>
<td>clus1</td>
<td>{f0735332-1dd1-11b2-bb31-00306eea460a}</td>
<td>nebula(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 (mycps1.symantecexample.com) to add the cluster:

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

Cluster clus1 added successfully

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

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

Node 0 (galaxy) successfully added

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

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

Node 1 (nebula) successfully added

4. If security is to be enabled, check whether the 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 mycps1.symantecexample.com -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>CPSADM@VCS_SERVICES@f0735332-1dd1-11b2/vx clus1/{f0735332-1dd1-11b2}</td>
<td></td>
<td>Operator</td>
<td></td>
</tr>
</tbody>
</table>

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@galaxy).

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

Issue the following commands on the CP server (mycps1.symantecexample.com):

```
# cpsadm -s mycps1.symantecexample.com -a add_user -e
  CPSADM@VCS_SERVICES@cluster_uuid
  -f cps_operator -g vx
```

User CPSADM@VCS_SERVICES@cluster_uuid successfully added

6 Authorize the CP server user to administer the 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 (mycps1.symantecexample.com) for VCS cluster clus1 with two nodes galaxy and nebula:

```
# cpsadm -s mycps1.symantecexample.com -a
  add_clus_to_user -c clus1
  -u {f0735332-1dd1-11b2}
  -e CPSADM@VCS_SERVICES@cluster_uuid
  -f cps_operator -g vx
```

Cluster successfully added to user
CPSADM@VCS_SERVICES@cluster_uuid privileges.

Configuring server-based fencing on the 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 234.

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/default/vxfen

   You must change the values of the VXFEN_START and the VXFEN_STOP environment variables to 1.

2 Use a text editor to edit the /etc/vxfenmode file values to meet your configuration specifications.

   If your server-based fencing configuration uses a single highly available CP server as its only coordination point, make sure to add the single_cp=1 entry in the /etc/vxfenmode file.

   The following sample file output displays what the /etc/vxfenmode file contains:

   See “Sample vxfenmode file output for server-based fencing” on page 243.

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

   For example:

   # svcadm enable vxfen

4 For CP servers in secure mode, make sure that the security is enabled on the cluster and the credentials for the CPSADM are present in the /var/VRTSvcs/vcsauth/data/CPSADM directory.

Sample vxfenmode file output for server-based fencing

The following is a sample vxfenmode file for server-based fencing:

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

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

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

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

# Specify 3 or more odd number of coordination points in this file,
# one in its own line. They can be all-CP servers, all-SCSI-3
# compliant coordinator disks, or a combination of CP servers and
# SCSI-3 compliant coordinator disks. Please ensure that the CP
# server coordination points are numbered sequentially and in the
# same order on all the cluster nodes.
#
# Coordination Point Server (CPS) is specified as:
#
# cps<number>=[<vip/vhn>]:<port>
#
# If a CPS supports multiple virtual IPs or virtual hostnames over # different subnets, all of the IPs/names can be specified in a # comma separated list as follows:
#
# cps<number>=[<vip_1/vhn_1>]:<port_1>,[<vip_2/vhn_2>]:<port_2>,..., # [<vip_n/vhn_n>]:<port_n>
#
# Where,
# <number>
# is the serial number of the CPS as a coordination point; must # start with 1.
# <vip>
# is the virtual IP address of the CPS, must be specified in # square brackets ("[]").
# <vhn>
# is the virtual hostname of the CPS, must be specified in square # brackets ("[]").
# <port>
# is the port number bound to a particular <vip/vhn> of the CPS. # It is optional to specify a <port>. However, if specified, it # must follow a colon (":") after <vip/vhn>. If not specified, the # colon (":") must not exist after <vip/vhn>. #
# For all the <vip/vhn>s which do not have a specified <port>, a # default port can be specified as follows:
#
# port=<default_port>
#
# Where <default_port> is applicable to all the <vip/vhn>s for # which a <port> is not specified. In other words, specifying <port> # with a <vip/vhn> overrides the <default_port> for that <vip/vhn>. # If the <default_port> is not specified, and there are <vip/vhn>s for # which <port> is not specified, then port number 14250 will be used # for such <vip/vhn>s.
#
# Example of specifying CP Servers to be used as coordination points:
# port=57777
# cps1=[192.168.0.23],[192.168.0.24]:58888,[mycps1.company.com]
# cps2=[192.168.0.25]
# cps3=[mycps2.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 [mycps2.company.com], and
# - default port 57777 will be used for all remaining <vip/vhn>s:
#   [192.168.0.23]
#   [mycps1.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]
#   [mycps1.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 this case should have three disks
#

Table 18-4 defines the vxfenmode parameters that must be edited.
<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;. Note: 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>
</tbody>
</table>
| cps1, cps2, or vxfendg   | Coordination point parameters. Enter either the virtual IP address or the FQHN (whichever is accessible) of the CP server. 

cps<number>=[virtual_ip_address/virtual_host_name]: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:

cps1=[192.168.0.23],[192.168.0.24]:58888, [mycps1.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 18-4  vxfenmode file parameters (continued)

<table>
<thead>
<tr>
<th>vxfenmode File Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</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>single_cp</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:

```bash
# haconf -makerw
# hagrp -add vxfen
# hagrp -modify vxfen SystemList galaxy 0 nebula 1
# hagrp -modify vxfen AutoFailOver 0
# hagrp -modify vxfen Parallel 1
# hagrp -modify vxfen SourceFile "/main.cf"
# hares -add coordpoint CoordPoint vxfen
# hares -modify coordpoint FaultTolerance 1
# hares -modify coordpoint Enabled 1
# haconf -dump -makero
```
3 Verify the status of the agent on the 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>galaxy</td>
<td>ONLINE</td>
</tr>
<tr>
<td>coordpoint</td>
<td>State</td>
<td>nebula</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 all such information 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 238.

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 `/kernel/drv/vxfen.conf` file as follows:

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

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

Refer to the sample /etc/vxfenmode file.

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

- Run the following command:
  
  ```
  lltconfig -T sendhbcap:3000
  ```

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

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

- Make the VCS configuration file writable:
  
  ```
  # haconf -makerw
  ```

- For each resource of the type DiskGroup, set the value of the MonitorReservation attribute to 0 and the value of the Reservation attribute to NONE.
  
  ```
  # hares -modify <dg_resource> MonitorReservation 0
  # hares -modify <dg_resource> Reservation "NONE"
  ```

- Run the following command to verify the value:
  
  ```
  # hares -list Type=DiskGroup MonitorReservation!=0
  # hares -list Type=DiskGroup Reservation!="NONE"
  ```

  The command should not list any resources.

- Modify the default value of the Reservation attribute at type-level.
  
  ```
  # haattr -default DiskGroup Reservation "NONE"
  ```

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

10 To make these VxFEN changes take effect, stop and restart VxFEN and the dependent modules
   ■ On each node, run the following command to stop VCS:
     
     # svcadm disable -t vcs
   
   ■ After VCS takes all services offline, run the following command to stop VxFEN:
     
     # svcadm disable -t vxfen
    
   ■ On each node, run the following commands to restart VxFEN and VCS:
     
     # svcadm enable vxfen

Sample /etc/vxfenmode file for non-SCSI-3 fencing

#-------------------------------------------------------------------------------
# vxen_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
#
# vxen_mode=customized
#
# vxen_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
#
# vxen_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,[mycps1.company.com] 
# cps2=[192.168.0.25] 
# cps3=[mycps2.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 [mycps2.company.com], and 
# - default port 57777 will be used for all remaining <vip/vhn>s: 
#   [192.168.0.23]
# [mycps1.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]
# [mycps1.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=[mycps1.company.com]
cps2=[mycps2.company.com]
cps3=[mycps3.company.com]
port=14250
================================
Manually configuring the clusters for data integrity
Setting up non-SCSI-3 fencing in virtual environments manually
Upgrading VCS

- Chapter 19. Planning to upgrade VCS
- Chapter 20. Performing a typical VCS upgrade using the installer
- Chapter 21. Performing a phased upgrade
- Chapter 22. Performing an automated VCS upgrade using response files
- Chapter 23. Performing a rolling upgrade
- Chapter 24. Upgrading using Live Upgrade
- Chapter 25. Upgrading the Solaris operating system
Planning to upgrade VCS

This chapter includes the following topics:

- About upgrading to VCS 6.0
- VCS supported upgrade paths
- Upgrading VCS in secure enterprise environments

About upgrading to VCS 6.0

You can upgrade VCS using one of the following methods:

- Typical upgrade using Veritas product installer or the installvcs program
  See “VCS supported upgrade paths” on page 260.
  See “Upgrading VCS using the script-based installer” on page 265.

- Typical upgrade using Veritas Web installer
  See “VCS supported upgrade paths” on page 260.
  See “Upgrading Veritas Cluster Server using the Veritas Web-based installer” on page 267.

- Phased upgrade to reduce downtime
  See “Performing a phased upgrade” on page 272.

- Automated upgrade using response files
  See “VCS supported upgrade paths” on page 260.
  See “Upgrading VCS using response files” on page 291.

- Upgrade using supported native operating system utility
  Live Upgrade
  See “About Live Upgrade” on page 301.

- Rolling upgrade to minimize downtime
See “Performing a rolling upgrade of VCS using the Web-based installer” on page 299.

You can upgrade VCS 6.0 to Storage Foundation High Availability 6.0 using Veritas product installer or response files.

See the Veritas Storage Foundation and High Availability Installation Guide.

## VCS supported upgrade paths

**Table 19-1** lists the supported upgrade paths for Solaris SPARC.

<table>
<thead>
<tr>
<th>Current version of VCS</th>
<th>Solaris 8 or older</th>
<th>Solaris 9</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5</td>
<td>No upgrade path exists. Uninstall VCS.</td>
<td>No upgrade path exists. Uninstall VCS.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>3.5 MP4</td>
<td>Upgrade the operating system to at least Solaris 10.</td>
<td>Upgrade the operating system to at least Solaris 10.</td>
<td></td>
</tr>
<tr>
<td>4.0</td>
<td>Use the installer to perform a full installation of VCS 6.0.</td>
<td>Use the installer to perform a full installation of VCS 6.0.</td>
<td></td>
</tr>
<tr>
<td>4.0 MP1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.0 MP2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>No upgrade path exists. Uninstall VCS.</td>
<td>No upgrade path exists. Uninstall VCS.</td>
<td>No upgrade path exists.</td>
</tr>
<tr>
<td>4.1 MP1</td>
<td>Upgrade the operating system to at least Solaris 10.</td>
<td>Upgrade the operating system to at least Solaris 10.</td>
<td>Uninstall VCS and then use the installer to perform a full installation of VCS 6.0.</td>
</tr>
<tr>
<td>4.1 MP2</td>
<td>Use the installer to perform a full installation of VCS 6.0.</td>
<td>Use the installer to perform a full installation of VCS 6.0.</td>
<td></td>
</tr>
<tr>
<td>Current version of VCS</td>
<td>Solaris 8 or older</td>
<td>Solaris 9</td>
<td>Solaris 10</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>5.0</td>
<td>No upgrade path exists. Uninstall VCS. Upgrade the operating system to at least Solaris 10. Use the installer to perform a full installation of VCS 6.0.</td>
<td>No upgrade path exists. Uninstall VCS. Upgrade the operating system to at least Solaris 10. Use the installer to perform a full installation of VCS 6.0.</td>
<td>No upgrade path exists. Uninstall VCS and then use the installer to perform a full installation of VCS 6.0.</td>
</tr>
<tr>
<td>5.0 MP1</td>
<td>No upgrade path exists. Uninstall VCS. Upgrade the operating system to at least Solaris 10. Use the installer to perform a full installation of VCS 6.0.</td>
<td>Upgrade directly to VCS 6.0 using the installer script.</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Not applicable</td>
<td>No upgrade path exists. Uninstall VCS. Upgrade the operating system to at least Solaris 10. Use the installer to perform a full installation of VCS 6.0.</td>
<td>Upgrade directly to VCS 6.0 using the installer script.</td>
</tr>
</tbody>
</table>

Table 19-2 lists the supported upgrade paths for the Solaris x64 Platform Edition.

<table>
<thead>
<tr>
<th>Current version of VCS</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>No upgrade path exists. Uninstall VCS. Use the installer to perform a full installation of VCS 6.0.</td>
</tr>
<tr>
<td>4.1 Phase 2</td>
<td></td>
</tr>
</tbody>
</table>
### Table 19-2 Supported upgrade paths for Solaris x64 Platform Edition (continued)

<table>
<thead>
<tr>
<th>Current version of VCS</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0</td>
<td>No upgrade path exists. Uninstall VCS.</td>
</tr>
<tr>
<td>5.0 MP1</td>
<td>Use the installer to perform a full installation of VCS 6.0.</td>
</tr>
<tr>
<td>5.0 MP3</td>
<td>Use the installer to upgrade to VCS 6.0.</td>
</tr>
<tr>
<td>5.0 MP3RPs</td>
<td>Use the installer to upgrade to VCS 6.0.</td>
</tr>
<tr>
<td>5.1</td>
<td>Use the installer to upgrade to VCS 6.0.</td>
</tr>
<tr>
<td>5.1RPs</td>
<td>Use the installer to upgrade to VCS 6.0.</td>
</tr>
<tr>
<td>5.1SP1</td>
<td>Use the installer to upgrade to VCS 6.0.</td>
</tr>
<tr>
<td>5.1SP1RPs</td>
<td>Use the installer to upgrade to VCS 6.0.</td>
</tr>
</tbody>
</table>

## 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.
   
   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.

   ```
   # hastart
   ```

   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 346.
Planning to upgrade VCS

Upgrading VCS in secure enterprise environments
Performing a typical VCS upgrade using the installer

This chapter includes the following topics:
- Before upgrading using the script-based or Web-based installer
- Upgrading VCS using the script-based installer
- Upgrading Veritas Cluster Server using the Veritas Web-based installer

Before upgrading using the script-based or Web-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

- Make sure that all non-global zones are booted and in the running state before you install or upgrade the VCS packages in the global zone. If the non-global zones are not mounted and running at the time of upgrade, you must upgrade each package in each non-global zone manually.

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 packages 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 packages, installs or upgrades packages, 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, make sure that you first upgrade all application clusters to version VCS 6.0. 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 451.
Upgrading Veritas Cluster Server using the Veritas Web-based installer

This section describes upgrading VCS with the Veritas Web-based installer. The installer detects and upgrades the product that is currently installed on the specified system or systems.

To upgrade VCS

1. Perform the required steps to save any data that you wish to preserve. For example, make configuration file backups.

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

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

   For each service group listed, take it offline:

   ```
   # /opt/VRTSvcs/bin/hagrp -offline service_group -all
   ```

3. Start the Web-based installer. See “Starting the Veritas Web-based installer” on page 162.

4. On the Select a task and a product page, select Upgrade a Product from the Task drop-down menu.

   The installer detects the product that is installed on the specified system. Click Next.

5. Indicate the systems on which to upgrade. Enter one or more system names, separated by spaces. Click Next.

6. On the License agreement page, select whether you accept the terms of the End User License Agreement (EULA). To continue, select Yes I agree and click Next.

7. Click Next to complete the upgrade.

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

8. After the upgrade, if the product is not configured, the Web-based installer asks: "Do you want to configure this product?" If the product is already configured, it will not ask any questions.
9 Click **Finish**. The installer prompts you for another task.

10 If you want to upgrade VCS or SFHA 5.1 on the CP server systems to version VCS 6.0, make sure that you upgraded all application clusters to version VCS 6.0. Then, upgrade VCS or SFHA on the CP server systems. For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

If you are upgrading from 4.x, you may need to create new VCS accounts if you used native operating system accounts.

See “Creating new VCS accounts if you used native operating system accounts” on page 451.
Performing a phased upgrade

This chapter includes the following topics:

■ About phased upgrade
■ Performing a phased upgrade

About phased upgrade

Perform a phased upgrade to minimize the downtime for the cluster. Depending on the situation, you can calculate the approximate downtime as follows:

You can fail over all your service groups to the nodes that are up. Downtime equals the time that is taken to offline and online the service groups.

You have a service group that you cannot fail over to a node that runs during upgrade. Downtime for that service group equals the time that is taken to perform an upgrade and restart the node.

Prerequisites for a phased upgrade

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

Planning for a phased upgrade

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

■ Split the cluster into two sub-clusters of equal or near equal size.

■ Split the cluster so that your high priority service groups remain online during the upgrade of the first subcluster.

■ Before you start the upgrade, back up the VCS configuration files `main.cf` and `types.cf` which are in the directory `/etcVRTSvcs/conf/config/`.

Phased upgrade limitations

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

■ While you perform the upgrades, do not start any modules.

■ When you start the installer, only select VCS.

■ While you perform the upgrades, do not add or remove service groups to any of the nodes.

■ After you upgrade the first half of your cluster (the first subcluster), you need to set up password-less SSH. Create the connection between an upgraded node in the first subcluster and a node from the other subcluster. The node from the other subcluster is where you plan to run the installer and also plan to upgrade.

■ Depending on your configuration, you may find that you cannot upgrade multiple nodes at the same time. You may only be able to upgrade one node at a time.

■ For very large clusters, you might have to repeat these steps multiple times to upgrade your cluster.

Phased upgrade example

In this example, you have a secure cluster that you have configured to run on four nodes: node01, node02, node03, and node04. You also have five service groups: sg1, sg2, sg3, and sg4. For the purposes of this example, the cluster is split into two subclusters. The nodes node01 and node02 are in the first subcluster, which you first upgrade. The nodes node03 and node04 are in the second subcluster, which you upgrade last.
Each service group is running on the nodes as follows:

- sg1 and sg2 are parallel service groups and run on all the nodes.
- sg3 and sg4 are failover service groups. sg3 runs on node01 and sg4 runs on node02.

In your system list, you have each service group that fails over to other nodes as follows:

- sg1 and sg2 are running on all the nodes.
- sg3 and sg4 can fail over to any of the nodes in the cluster.

**Phased upgrade example overview**

This example's upgrade path follows:

- Move all the failover service groups from the first subcluster to the second subcluster.
- Take all the parallel service groups offline on the first subcluster.
- Upgrade the operating system on the first subcluster's nodes, if required.
- On the first subcluster, start the upgrade using the installation program.
- Get the second subcluster ready.
- Activate the first subcluster.
- Upgrade the operating system on the second subcluster's nodes, if required.
- On the second subcluster, start the upgrade using the installation program.
- Activate the second subcluster.

See “Performing a phased upgrade” on page 272.
Performing a phased upgrade

This section explains how to perform a phased upgrade of VCS on four nodes with four service groups. Note that in this scenario, VCS and the service groups cannot stay online on the second subcluster during the upgrade of the second subcluster. Do not add, remove, or change resources or service groups on any nodes during the upgrade. These changes are likely to get lost after the upgrade.

An example of a phased upgrade follows. It illustrates the steps to perform a phased upgrade. The example makes use of a secure VCS cluster.

You can perform a phased upgrade from VCS 5.1 or other supported previous versions to VCS 6.0.

See “About phased upgrade” on page 269.

See “Phased upgrade example” on page 270.

Moving the service groups to the second subcluster

Perform the following steps to establish the service group's status and to switch the service groups.
To move service groups to the second subcluster

1. On the first subcluster, determine where the service groups are online.

   \# hagrp -state

   The output resembles:

<table>
<thead>
<tr>
<th>Group</th>
<th>Attribute</th>
<th>System</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sg1</td>
<td>State</td>
<td>node01</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg1</td>
<td>State</td>
<td>node02</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg1</td>
<td>State</td>
<td>node03</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg1</td>
<td>State</td>
<td>node04</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg2</td>
<td>State</td>
<td>node01</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg2</td>
<td>State</td>
<td>node02</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg2</td>
<td>State</td>
<td>node03</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg2</td>
<td>State</td>
<td>node04</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg3</td>
<td>State</td>
<td>node01</td>
<td>ONLINE</td>
</tr>
<tr>
<td>sg3</td>
<td>State</td>
<td>node02</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>sg3</td>
<td>State</td>
<td>node03</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>sg3</td>
<td>State</td>
<td>node04</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>sg4</td>
<td>State</td>
<td>node01</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>sg4</td>
<td>State</td>
<td>node02</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>sg4</td>
<td>State</td>
<td>node03</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>sg4</td>
<td>State</td>
<td>node04</td>
<td>OFFLINE</td>
</tr>
</tbody>
</table>

2. Offline the parallel service groups (sg1 and sg2) from the first subcluster. Switch the failover service groups (sg3 and sg4) from the first subcluster (node01 and node02) to the nodes on the second subcluster (node03 and node04).

   \# hagrp -offline sg1 -sys node01
   \# hagrp -offline sg2 -sys node01
   \# hagrp -offline sg1 -sys node02
   \# hagrp -offline sg2 -sys node02
   \# hagrp -switch sg3 -to node03
   \# hagrp -switch sg4 -to node04
3 On the nodes in the first subcluster, unmount all the VxFS file systems that VCS does not manage, for example:

```bash
# df -k
```

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>kbytes</th>
<th>used</th>
<th>avail</th>
<th>capacity</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/dsk/c1t0d0s0</td>
<td>66440242</td>
<td>10114415</td>
<td>55661425</td>
<td>16%</td>
<td>/</td>
</tr>
<tr>
<td>/devices</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/devices</td>
</tr>
<tr>
<td>ctrfs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/system/contract</td>
</tr>
<tr>
<td>proc</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/proc</td>
</tr>
<tr>
<td>mnttab</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/etc/mnttab</td>
</tr>
<tr>
<td>swap</td>
<td>5287408</td>
<td>1400</td>
<td>5286008</td>
<td>1%</td>
<td>/etc/svc/volatile</td>
</tr>
<tr>
<td>objfs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/system/object</td>
</tr>
<tr>
<td>sharefs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/etc/dfs/sharetab</td>
</tr>
<tr>
<td>/platform/sun4u-us3/lib/libc_psr/libc_psr_hwcap1.so.1</td>
<td>66440242</td>
<td>10114415</td>
<td>55661425</td>
<td>16%</td>
<td>/platform/sun4u-us3/lib/libc_psr.so.1</td>
</tr>
<tr>
<td>/platform/sun4u-us3/lib/sparcv9/libc_psr/libc_psr_hwcap1.so.1</td>
<td>66440242</td>
<td>10114415</td>
<td>55661425</td>
<td>16%</td>
<td>/platform/sun4u-us3/lib/sparcv9/libc_psr.so.1</td>
</tr>
<tr>
<td>fd</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/dev/fd</td>
</tr>
<tr>
<td>swap</td>
<td>5286064</td>
<td>56</td>
<td>5286008</td>
<td>1%</td>
<td>/tmp</td>
</tr>
<tr>
<td>swap</td>
<td>5286056</td>
<td>48</td>
<td>5286008</td>
<td>1%</td>
<td>/var/run</td>
</tr>
<tr>
<td>swap</td>
<td>5286008</td>
<td>0</td>
<td>5286008</td>
<td>0%</td>
<td>/dev/vx/dmp</td>
</tr>
<tr>
<td>swap</td>
<td>5286008</td>
<td>0</td>
<td>5286008</td>
<td>0%</td>
<td>/dev/vx/rdmp</td>
</tr>
<tr>
<td>/platform/sun4u-us3/lib/sparcv9/libc_psr/libc_psr_hwcap1.so.1</td>
<td>3.0G</td>
<td>18M</td>
<td>2.8G</td>
<td>1%</td>
<td>/mnt/dg2/dg2vol1</td>
</tr>
<tr>
<td>/dev/vx/dsk/dg2/dg2vol12</td>
<td>1.0G</td>
<td>18M</td>
<td>944M</td>
<td>2%</td>
<td>/mnt/dg2/dg2vol2</td>
</tr>
<tr>
<td>/dev/vx/dsk/dg2/dg2vol13</td>
<td>10G</td>
<td>20M</td>
<td>9.4G</td>
<td>1%</td>
<td>/mnt/dg2/dg2vol3</td>
</tr>
</tbody>
</table>

```bash
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

4 On the nodes in the first subcluster, stop all VxVM volumes (for each disk group) that VCS does not manage.

5 Make the configuration writable on the first subcluster.

```bash
# haconf -makerw
```
6  Freeze the nodes in the first subcluster.

```bash
# hasys -freeze -persistent node01
# hasys -freeze -persistent node02
```

7  Dump the configuration and make it read-only.

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

8  Verify that the service groups are offline on the first subcluster that you want to upgrade.

```bash
# hagrp -state
```

Output resembles:

```
#Group Attribute System Value
sg1 State node01 |OFFLINE|
sg1 State node02 |OFFLINE|
sg1 State node03 |ONLINE|
sg1 State node04 |ONLINE|
sg2 State node01 |OFFLINE|
sg2 State node02 |OFFLINE|
sg2 State node03 |ONLINE|
sg2 State node04 |ONLINE|
sg3 State node01 |OFFLINE|
sg3 State node02 |OFFLINE|
sg3 State node03 |ONLINE|
sg3 State node04 |OFFLINE|
sg4 State node01 |OFFLINE|
sg4 State node02 |OFFLINE|
sg4 State node03 |OFFLINE|
sg4 State node04 |ONLINE|
```

9  Perform this step on the nodes (node01 and node02) in the first subcluster if the cluster uses I/O Fencing. Use an editor of your choice and change the following:

- In the `/etc/vxfenmode` file, change the value of the `vxfen_mode` variable from `scsi3` to `disabled`. Ensure that the line in the `vxfenmode` file resembles:

  ```bash
  vxfen_mode=disabled
  ```
In the `/etc/VRTSvcs/conf/config/main.cf` file, change the value of the UseFence attribute from SCSI3 to NONE. Ensure that the line in the `main.cf` file resembles:

```
UseFence = NONE
```

10 Back up the `llttab`, `llthosts`, `gabtab`, `types.cf`, `main.cf` and AT configuration files on the first subcluster.

```
# cp /etc/llttab /etc/llttab.bkp
# cp /etc/llthosts /etc/llthosts.bkp
# cp /etc/gabtab /etc/gabtab.bkp
# cp /etc/VRTSvcs/conf/config/main.cf \
    /etc/VRTSvcs/conf/config/main.cf.bkp
# cp /etc/VRTSvcs/conf/config/types.cf \
    /etc/VRTSvcs/conf/config/types.cf.bkp
# /opt/VRTSat/bin/vssat showbackuplist
B|/var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
B|/var/VRTSat/.VRTSat/profile/certstore
B|/var/VRTSat/ABAuthSource
B|/etc/vx/vss/VRTSat.conf
Quiescing ...
Snapshot Directory :/var/VRTSatSnapShot
```

Upgrading the operating system on the first subcluster

You can perform the operating system upgrade on the first subcluster, if required. Refer to the operating system's documentation for more information.

Upgrading the first subcluster

You now navigate to the installer program and start it.

To start the installer for the phased upgrade

1. Confirm that you are logged on as the superuser and you mounted the product disc.
2. Make sure that you can ssh or rsh from the node where you launched the installer to the nodes in the second subcluster without requests for a password.
3. Navigate to the folder that contains installvcs.

```
# cd cluster_server
```
4  Start the installvcs program, specify the nodes in the first subcluster (node1 and node2).

    # ./installvcs node1 node2

The program starts with a copyright message and specifies the directory where it creates the logs.

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

    Do you agree with the terms of the End User License Agreement as specified in the cluster_server/EULA/<lang>/EULA_VCS_Ux_6.0.pdf file present on media? [y,n,q,?]  y

6  Review the available installation options.

    See “Veritas Cluster Server installation packages” on page 413.

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

    2  Installs the recommended VCS packages that provide complete functionality of the product. This option does not install the optional VCS packages.

        Note that this option is the default.

    3  Installs all the VCS packages.

        You must choose this option to configure any optional VCS feature.

    4  Displays the VCS packages for each option.

        For this example, select 3 for all packages.

        Select the packages to be installed on all systems? [1-4,q,?] (2) 3

7  The installer performs a series of checks and tests to ensure communications, licensing, and compatibility.

8  When you are prompted, reply y to continue with the upgrade.

    Do you want to continue? [y,n,q] (y)
When you are prompted, reply \textbf{y} to stop appropriate processes. 

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

The installer ends for the first subcluster with the following output:

\begin{verbatim}
Configuring VCS: 100%

Estimated time remaining: 0:00

Performing VCS upgrade configuration .................... Done

Veritas Cluster Server Configure completed successfully
\end{verbatim}

You are performing phased upgrade (Phase 1) on the systems. Follow the steps in install guide to upgrade the remaining systems.

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

The upgrade is finished on the first subcluster. Do not reboot the nodes in the first subcluster until you complete the \underline{Preparing the second subcluster} procedure.

\textbf{Preparing the second subcluster}

Perform the following steps on the second subcluster before rebooting nodes in the first subcluster.
To prepare to upgrade the second subcluster

1. Get the summary of the status of your resources.

```
# hastatus -summ
-- SYSTEM STATE
   -- System State Frozen
   A node01 EXITED 1
   A node02 EXITED 1
   A node03 RUNNING 0
   A node04 RUNNING 0

-- GROUP STATE
   -- Group System Probed AutoDisabled State
   B SG1 node01 Y N OFFLINE
   B SG1 node02 Y N OFFLINE
   B SG1 node03 Y N ONLINE
   B SG1 node04 Y N ONLINE
   B SG2 node01 Y N OFFLINE
   B SG2 node02 Y N OFFLINE
   B SG2 node03 Y N ONLINE
   B SG2 node04 Y N ONLINE
   B SG3 node01 Y N OFFLINE
   B SG3 node02 Y N OFFLINE
   B SG3 node03 Y N ONLINE
   B SG3 node04 Y N OFFLINE
   B SG4 node01 Y N OFFLINE
   B SG4 node02 Y N OFFLINE
   B SG4 node03 Y N OFFLINE
   B SG4 node04 Y N ONLINE
```
2 Unmount all the VxFS file systems that VCS does not manage, for example:

```
# df -k
```

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>kbytes</th>
<th>used</th>
<th>avail</th>
<th>capacity</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/dsk/c1t0d0s0</td>
<td>66440242</td>
<td>10114415</td>
<td>55661425</td>
<td>16%</td>
<td>/</td>
</tr>
<tr>
<td>/devices</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/devices</td>
</tr>
<tr>
<td>/ctfs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/system/contract</td>
</tr>
<tr>
<td>/proc</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/proc</td>
</tr>
<tr>
<td>/mnttab</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/etc/mnttab</td>
</tr>
<tr>
<td>/swap</td>
<td>5287408</td>
<td>1400</td>
<td>5286008</td>
<td>1%</td>
<td>/etc/svc/volatile</td>
</tr>
<tr>
<td>/objfs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/system/object</td>
</tr>
<tr>
<td>/sharefs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/etc/dfs/sharetab</td>
</tr>
<tr>
<td>/platform/sun4u-us3/lib/libc_psr/libc_psr_hwcpl.so.1</td>
<td>66440242</td>
<td>10114415</td>
<td>55661425</td>
<td>16%</td>
<td>/platform/sun4u-us3/</td>
</tr>
<tr>
<td>/platform/sun4u-us3/lib/libc_psr.so.1</td>
<td>66440242</td>
<td>10114415</td>
<td>55661425</td>
<td>16%</td>
<td>/platform/sun4u-us3/</td>
</tr>
<tr>
<td>/platform/sun4u-us3/lib/sparcv9/libc_psr/libc_psr_hwcpl.so.1</td>
<td>66440242</td>
<td>10114415</td>
<td>55661425</td>
<td>16%</td>
<td>/platform/sun4u-us3/</td>
</tr>
<tr>
<td>fd</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>/dev/fd</td>
</tr>
<tr>
<td>/swap</td>
<td>5286064</td>
<td>56</td>
<td>5286008</td>
<td>1%</td>
<td>/tmp</td>
</tr>
<tr>
<td>/swap</td>
<td>5286056</td>
<td>48</td>
<td>5286008</td>
<td>1%</td>
<td>/var/run</td>
</tr>
<tr>
<td>/swap</td>
<td>5286008</td>
<td>0</td>
<td>5286008</td>
<td>0%</td>
<td>/dev/vx/dmp</td>
</tr>
<tr>
<td>/swap</td>
<td>5286008</td>
<td>0</td>
<td>5286008</td>
<td>0%</td>
<td>/dev/vx/rdmp</td>
</tr>
<tr>
<td>/dev/vx/dsk/dg2/dg2vol1</td>
<td>3.0G</td>
<td>18M</td>
<td>2.8G</td>
<td>1%</td>
<td>/mnt/dg2/dg2vol1</td>
</tr>
<tr>
<td>/dev/vx/dsk/dg2/dg2vol2</td>
<td>1.0G</td>
<td>18M</td>
<td>944M</td>
<td>2%</td>
<td>/mnt/dg2/dg2vol2</td>
</tr>
<tr>
<td>/dev/vx/dsk/dg2/dg2vol3</td>
<td>10G</td>
<td>20M</td>
<td>9.4G</td>
<td>1%</td>
<td>/mnt/dg2/dg2vol3</td>
</tr>
</tbody>
</table>

```
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

3 Stop all VxVM volumes (for each disk group) that VCS does not manage.

4 Make the configuration writable on the second subcluser.

```
# haconf -makerw
```
5 Unfreeze the service groups.

```
# hagrp -unfreeze sg1 -persistent
# hagrp -unfreeze sg2 -persistent
# hagrp -unfreeze sg3 -persistent
# hagrp -unfreeze sg4 -persistent
```

6 Dump the configuration and make it read-only.

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

7 Take the service groups offline on node03 and node04.

```
# hagrp -offline sg1 -sys node03
# hagrp -offline sg1 -sys node04
# hagrp -offline sg2 -sys node03
# hagrp -offline sg2 -sys node04
# hagrp -offline sg3 -sys node03
# hagrp -offline sg4 -sys node04
```

8 Verify the state of the service groups.

```
# hagrp -state

<table>
<thead>
<tr>
<th>Group</th>
<th>Attribute</th>
<th>System</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG1</td>
<td>State</td>
<td>node01</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG1</td>
<td>State</td>
<td>node02</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG1</td>
<td>State</td>
<td>node03</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG1</td>
<td>State</td>
<td>node04</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG2</td>
<td>State</td>
<td>node01</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG2</td>
<td>State</td>
<td>node02</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG2</td>
<td>State</td>
<td>node03</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG2</td>
<td>State</td>
<td>node04</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG3</td>
<td>State</td>
<td>node01</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG3</td>
<td>State</td>
<td>node02</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG3</td>
<td>State</td>
<td>node03</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>SG3</td>
<td>State</td>
<td>node04</td>
<td>OFFLINE</td>
</tr>
</tbody>
</table>
```

9 Perform this step on node03 and node04 if the cluster uses I/O Fencing. Use an editor of your choice and change the following:

- In the `/etc/vxfenmode` file, change the value of the `vxfen_mode` variable from `scsi3` to `disabled`. Ensure that the line in the `vxfenmode` file resembles:

```
vxfen_mode=disabled
```
In the `/etc/VRTSvcs/conf/config/main.cf` file, change the value of the UseFence attribute from SCSI3 to NONE. Ensure that the line in the main.cf file resembles:

```bash
UseFence = NONE
```

**10** Stop VCS, I/O Fencing, GAB, and LLT on node03 and node04.

- **Solaris 9:**
  ```bash
  # /opt/VRTSvcs/bin/hastop -local
  # /etc/init.d/vxfen stop
  # /etc/init.d/gab stop
  # /etc/init.d/llt stop
  ```

- **Solaris 10:**
  ```bash
  # /opt/VRTSvcs/bin/hastop -local
  # svcadm disable -t /system/vxfen
  # svcadm disable -t /system/gab
  # svcadm disable -t /system/llt
  ```

**11** Make sure that the VXFEN, GAB, and LLT modules on node03 and node04 are not loaded.

- **Solaris 9:**
  ```bash
  # /etc/init.d/vxfen status
  VXFEN module is not loaded
  
  # /etc/init.d/gab status
  GAB module is not loaded
  
  # /etc/init.d/llt status
  LLT module is not loaded
  ```

- **Solaris 10:**
  ```bash
  # /lib/svc/method/vxfen status
  VXFEN module is not loaded
  
  # /lib/svc/method/gab status
  GAB module is not loaded
  ```
Activating the first subcluster

Get the first subcluster ready for the service groups.

**Note:** These steps fulfill part of the installer’s output instructions, see Upgrading the first subcluster step 10.

To activate the first subcluster

1. Perform this step on node01 and node02 if the cluster uses I/O Fencing. Use an editor of your choice and revert the following to an enabled state before you reboot the first subcluster’s nodes:
   - In the /etc/VRTSvcs/conf/config/main.cf file, change the value of the UseFence attribute from NONE to SCSI3. Ensure that the line in the main.cf file resembles:
     ```
     UseFence = SCSI3
     ```
   - In the /etc/vxfenmode file, change the value of the vxfen_mode variable from disabled to scsi3. Ensure that the line in the vxfenmode file resembles:
     ```
     vxfen_mode=scsi3
     ```

2. Reboot the node01 and node02 in the first subcluster.
   ```
   # /usr/sbin/shutdown -y -i6 -g0
   ```

3. Seed node01 and node02 in the first subcluster.
   ```
   # gabconfig -xc
   ```

4. For nodes that use Solaris 10, start VCS in first half of the cluster:
   ```
   # svcadm enable system/vcs
   ```

5. Start VCS on node01 and node02. On each node run:
   ```
   # hastart
   ```
6  Make the configuration writable on the first subcluster.
   
   # haconf -makerw

7  Unfreeze the nodes in the first subcluster.
   
   # hasys -unfreeze -persistent node01
   # hasys -unfreeze -persistent node02

8  Dump the configuration and make it read-only.
   
   # haconf -dump -makero

9  Bring the service groups online on node01 and node02.
   
   # hagrp -online sg1 -sys node01
   # hagrp -online sg1 -sys node02
   # hagrp -online sg2 -sys node01
   # hagrp -online sg2 -sys node02
   # hagrp -online sg3 -sys node01
   # hagrp -online sg4 -sys node02

Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required. Refer to the operating system's documentation for more information.

Before you perform the operating system upgrade, make sure to disable VCS, VXFEN, GAB, and LLT.

To disable VCS, VXFEN, GAB, and LLT

1  On the second subcluster, disable VCS so that it does not start after reboot. Edit the vcs file in /etc/default. Open the vcs file in an editor, and change the line that reads VCS_START=1 to VCS_START=0. Save and close the file.

2  On the second subcluster, disable VXFEN so that it does not start after reboot. Edit the vxfen file in /etc/default. Open the vxfen file in an editor, and change the line that reads VXFEN_START=1 to VXFEN_START=0. Save and close the file.

3  On the second subcluster, disable GAB so that it does not start after reboot. Edit the gab file in /etc/default. Open the gab file in an editor, and change the line that reads GAB_START=1 to GAB_START=0. Save and close the file.
4 On the second subcluster, disable LLT so that it does not start after reboot. Edit the `llt` file in `/etc/default`. Open the `llt` file in an editor, and change the line that reads `LLT_START=1` to `LLT_START=0`. Save and close the file.

5 For a cluster that uses secure mode, create a password-less SSH connection. The connection is from the node where you plan to run the installer to one of the nodes that you have already upgraded.

Upgrading the second subcluster

Perform the following procedure to upgrade the second subcluster (node03 and node04).

To start the installer to upgrade the second subcluster

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

2 Navigate to the folder that contains `installvcs`.

   ```
   # cd cluster_server
   ``

3 Confirm that VCS is stopped on node03 and node04. Start the `installvcs` program, specify the nodes in the second subcluster (node3 and node4).

   ```
   # ./installvcs node3 node4
   ```

   The program starts with a copyright message and specifies the directory where it creates the logs.

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

   ```
   Do you agree with the terms of the End User License Agreement as specified in the cluster_server/EULA/<lang>/EULA_VCS_Ux_6.0.pdf file present on media? [y,n,q,?] y
   ```
5 Review the available installation options.

See “Veritas Cluster Server installation packages” on page 413.

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

2. Installs the recommended VCS packages that provide complete functionality of the product. This option does not install the optional VCS packages.

   Note that this option is the default.

3. Installs all the VCS packages.

   You must choose this option to configure any optional VCS feature.

4. Displays the VCS packages for each option.

   For this example, select 3 for all packages.

   Select the packages to be installed on all systems? [1-4,q,?] (2) 3

6 The installer performs a series of checks and tests to ensure communications, licensing, and compatibility.

7 When you are prompted, reply y to continue with the upgrade.

   Do you want to continue? [y,n,q] (y)

8 When you are prompted, reply y to stop VCS processes.

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

9 Monitor the installer program answering questions as appropriate until the upgrade completes.

Finishing the phased upgrade

   Complete the following procedure to complete the upgrade.
To finish the upgrade

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

   # /opt/VRTSvcs/bin/uuidconfig.pl
   -clus -display node1 [node2 ...]

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

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

2  Perform this step on node03 and node04 if the cluster uses I/O Fencing. Use an editor of your choice and revert the following to an enabled state before you reboot the second subcluster’s nodes:

   ■  In the /etc/vxfenmode file, change the value of the vxfen_mode variable from disabled to scsi3. Ensure that the line in the vxfenmode file resembles:

       vxfen_mode=scsi3

3  Reboot the node03 and node04 in the second subcluster.

   # /usr/sbin/shutdown -y -i6 -g0

   The nodes in the second subcluster join the nodes in the first subcluster.

4  For nodes that use Solaris 10, start VCS in first half of the cluster:

   # svcadm enable system/vcs

5  Check to see if VCS and its components are up.

   # gabconfig -a

   GAB Port Memberships
   ================================================================
   Port a gen nxxxxnn membership 0123
   Port b gen nxxxxnn membership 0123
   Port h gen nxxxxnn membership 0123
6 Run an `hastatus -sum` command to determine the status of the nodes, service groups, and cluster.

```
# hastatus -sum
```

```
-- SYSTEM STATE
-- System           State     Frozen
  A node01         RUNNING   0
  A node02         RUNNING   0
  A node03         RUNNING   0
  A node04         RUNNING   0

-- GROUP STATE
-- Group System Probed AutoDisabled State
  B sg1 node01 Y N ONLINE
  B sg1 node02 Y N ONLINE
  B sg1 node03 Y N ONLINE
  B sg1 node04 Y N ONLINE
  B sg2 node01 Y N ONLINE
  B sg2 node02 Y N ONLINE
  B sg2 node03 Y N ONLINE
  B sg2 node04 Y N ONLINE
  B sg3 node01 Y N ONLINE
  B sg3 node02 Y N OFFLINE
  B sg3 node03 Y N OFFLINE
  B sg3 node04 Y N OFFLINE
  B sg4 node01 Y N OFFLINE
  B sg4 node02 Y N ONLINE
  B sg4 node03 Y N OFFLINE
  B sg4 node04 Y N OFFLINE
```

7 After the upgrade is complete, start the VxVM volumes (for each disk group) and mount the VxFS file systems.

In this example, you have performed a phased upgrade of VCS. The service groups were down when you took them offline on node03 and node04, to the time VCS brought them online on node01 or node02.
Note: If you want to upgrade Coordination Point (CP) server systems that use Veritas Cluster Server (VCS) or Storage Foundation High Availability (SFHA) to 6.0, make sure that you upgraded all application clusters to version 6.0. Then, upgrade VCS or SFHA on the CP server systems. For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.
Performing 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 293.
4. Edit the values of the response file variables as necessary.
   
   See “Response file variables to upgrade VCS” on page 292.
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 -responsefile /tmp/response_file
```

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

### Response file variables to upgrade VCS

Table 22-1 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 packages. (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>
<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>
</tbody>
</table>
Table 22-1 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}[pkgpath]</td>
<td>Scalar</td>
<td>Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems. (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 packages 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. <strong>Note:</strong> The installer copies the response files and summary files also to the specified logpath location. (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>
</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 292.

```
# # Configuration Values: #
our %CFG;
```
Performing an automated VCS upgrade using response files

Sample response file for upgrading VCS

```
$CFG{accepteula}=1;
$CFG{vcs_allowcomms}=1;
$CFG{opt}{upgrade}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw( galaxy nebula) ];
1;
```
Performing a rolling upgrade

This chapter includes the following topics:

- About rolling upgrades
- Performing a rolling upgrade using the installer
- Performing a rolling upgrade of VCS using the Web-based installer

About rolling upgrades

The rolling upgrade minimizes downtime for highly available clusters to the amount of time that it takes to perform a service group failover. The rolling upgrade has two main phases where the installer upgrades kernel packages in phase 1 and VCS and VCS agent packages in phase 2.

**Note:** You need to perform a rolling upgrade on a completely configured cluster.

The following is an overview of the flow for a rolling upgrade:

1. The installer performs prechecks on the cluster.

2. The installer moves service groups to free nodes for the first phase of the upgrade as is needed. Application downtime occurs during the first phase as the installer moves service groups to free nodes for the upgrade. The only downtime that is incurred is the normal time required for the service group to fail over.

3. The installer performs the second phase of the upgrade on all of the nodes in the cluster. The second phase of the upgrade includes downtime of the Veritas Cluster Server (VCS) engine HAD, but does not include application downtime.
Figure 23-1 illustrates an example of the installer performing a rolling upgrade for three service groups on a two node cluster.

Figure 23-1 Example of the installer performing a rolling upgrade

The following limitations apply to rolling upgrades:
Rolling upgrades are not compatible with phased upgrades.
Do not mix rolling upgrades and phased upgrades.
You can perform a rolling upgrade from 5.1 and later versions.

Performing a rolling upgrade using the installer

Use a rolling upgrade to upgrade Veritas Cluster Server to the latest release with minimal application downtime.

Performing a rolling upgrade using the script-based installer

Before you start the rolling upgrade, make sure that Veritas Cluster Server (VCS) is running.

To perform a rolling upgrade

1. Complete the preparatory steps on the first sub-cluster.
2. Log in as superuser and mount the VCS VCS 6.0 installation media.
3. From root, start the installer.
   
   # ./installer

4. From the menu select Rolling Upgrade.
5. The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type y to continue.
6. The installer inventories the running service groups and determines the node or nodes to upgrade in phase 1 of the rolling upgrade. Type y to continue. If you choose to specify the nodes, type n and enter the names of the nodes.
7. The installer performs further prechecks on the nodes in the cluster and may present warnings. You can type y to continue or quit the installer and address the precheck's warnings.
8. Review the EULA, and type y if you agree to its terms.
9. The installer prompts you to stop the applicable processes. Type y to continue.

The installer fails over failover service groups to the node or nodes that are not upgraded at this time. The downtime is the time that it normally takes for the service group's failover. The installer stops parallel service groups on the nodes that are to be upgraded.
10 The installer stops relevant processes, uninstalls old kernel packages, and installs the new packages. It performs the configuration for the upgrade and re-starts processes.

   In case of failure in the startup of some of the processes, you may need to reboot the nodes and manually check the cluster's status.

11 Complete the preparatory steps on the nodes that you have not yet upgraded.

12 The installer begins phase 1 of the upgrade on the remaining node or nodes. Type `y` to continue the rolling upgrade.

   If the installer reboots nodes, restart the installer.

   The installer repeats step 6 through step 10.

   For clusters with larger number of nodes, this process may repeat several times. Service groups come down and are brought up to accommodate the upgrade.

13 When phase 1 of the rolling upgrade completes, begin phase 2 of the upgrade. Phase 2 of the upgrade includes downtime for the VCS engine (HAD), which does not include application downtime. Type `y` to continue.

   If the boot disk is encapsulated, you need to reboot nodes when phase 1 completes.

14 The installer determines the remaining packages to upgrade. Press `Enter` to continue.

15 The installer stops Veritas Cluster Server (VCS) processes. Type `y` to continue.

   The installer performs prechecks, uninstalls old packages, and installs the new packages. It performs post-installation tasks, and the configuration for the upgrade.

16 Type `y` or `n` to help Symantec improve the automated installation.

17 If you have network connection to the Internet, the installer checks for updates.

   If updates are discovered, you can apply them now.

18 Upgrade application.

19 To upgrade VCS or Storage Foundation High Availability (SFHA) on the Coordination Point (CP) server systems to version 6.0, upgrade all the application clusters to 6.0. You then upgrade VCS or SFHA on the CP server systems.

   For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.
Performing a rolling upgrade of VCS using the Web-based installer

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

See “About rolling upgrades” on page 295.

To start the rolling upgrade—phase 1

1. Complete the preparatory steps on the first sub-cluster.

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

3. Start the Web-based installer.
   See “Starting the Veritas Web-based installer” on page 162.

4. In the Task pull-down menu, select Rolling Upgrade.
   Click the Next button to proceed.

5. Review the systems that the installer has chosen to start the rolling upgrade. These systems are chosen to minimize downtime during the upgrade.
   Click Yes to proceed.
   The installer validates systems. If it throws an error, address the error and return to the installer.

6. Review the End User License Agreement (EULA). To continue, select Yes I agree and click Next.

7. The installer stops all processes. Click Next to proceed.

8. The installer removes old software and upgrades the software on the systems that you selected. Review the output and click the Next button when prompted. The installer starts all the relevant processes and brings all the service groups online.
   If the installer reboots nodes, restart the installer.

9. Complete the preparatory steps on the nodes that you have not yet upgraded.
When prompted, perform step 4 through step 8 on the nodes that you have not yet upgraded.

When prompted, start phase 2. Click Yes to continue with the rolling upgrade.

You may need to restart the Web-based installer to perform phase 2.

See “Starting the Veritas Web-based installer” on page 162.

**To upgrade the non-kernel components—phase 2**

1. In the Task pull-down menu, make sure that Rolling Upgrade is selected. Click the Next button to proceed.

2. The installer detects the information of cluster and the state of rolling upgrade.

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

3. Review the End User License Agreement (EULA). To continue, select Yes I agree and click Next.

4. The installer validates systems. If it throws an error, address the error and return to the installer. Click Next to proceed.

5. The installer stops all processes. Click Next to proceed.

6. The installer removes old software and upgrades the software on the systems that you selected. Review the output and click the Next button when prompted. The installer starts all the relevant processes and brings all the service groups online.

7. If you have network connection to the Internet, the installer checks for updates.

   If updates are discovered, you can apply them now.

8. Upgrade application.

   The upgrade is complete.
Upgrading using Live Upgrade

This chapter includes the following topics:

- About Live Upgrade
- Supported upgrade paths for Live Upgrade
- Before you upgrade VCS using Solaris Live Upgrade
- Upgrading VCS and Solaris using Live Upgrade
- Upgrading Solaris using Live Upgrade
- Upgrading VCS using Live Upgrade
- Administering boot environments

About Live Upgrade

You can use Live Upgrade to perform the following types of upgrade:

- Upgrade the operating system and VCS.
  See “Upgrading VCS and Solaris using Live Upgrade” on page 306.

- Upgrade the operating system.
  See “Upgrading Solaris using Live Upgrade” on page 313.

- Upgrade VCS.
  See “Upgrading VCS using Live Upgrade” on page 315.

Figure 24-1 illustrates an example of an upgrade of Veritas products from 5.1 SP1 to 6.0, and the operating system from Solaris 9 to Solaris 10.
**Live Upgrade process**

1. **Create the alternate boot environment from the primary boot environment while the server runs.**
   - **Solaris 9**
   - Veritas 5.1 SP1
   - Other packages
   - **Primary boot environment**
   - **Alternate boot environment**

2. **Upgrade the Veritas product in the alternate boot environment using the installer or manually.**
   - **Solaris 9**
   - Veritas 5.1 SP1
   - Other packages
   - **Primary boot environment**
   - **Alternate boot environment**

3. **The server now runs the new primary boot environment.**
   - **Solaris 10**
   - Veritas 5.1 SP1
   - Other packages
   - **Primary boot environment**
   - **Alternate boot environment**

**Restart the server**

Some service groups (failover and parallel) may be online in this cluster and they are not affected by the Live Upgrade process. The only downtime experienced is when the server is rebooted to boot into the alternate boot disk.

**Veritas Cluster Server exceptions for Live Upgrade**

If you have configured I/O Fencing or Veritas File System or Veritas Volume Manager, use the Live Upgrade instructions in the *Storage Foundation and High Availability Installation Guide*.

**Supported upgrade paths for Live Upgrade**

The systems where you plan to use Live Upgrade must run Solaris 9 or Solaris 10. You can upgrade from systems that run Solaris 9, but VCS 6.0 is not supported on Solaris 9.

For Solaris 10, make sure that all non-global zones are booted and in the running state before you use the Symantec product installer to upgrade the Storage Foundation products in the global zone. If the non-global zones are not mounted and running at the time of the upgrade, you must upgrade each package in each non-global zone manually.

For Live Upgrade, if the alternative root environment also has a zone, you cannot install VRTSodm. You must remove the VRTSodm package first then install the
Storage Foundation product. After you reboot the alternative root, you can install VRTSodm.

VCS version must be at least 5.0 MP3.

Symantec requires that both global and non-global zones run the same version of Veritas products.

**Note:** If you use Live Upgrade on a system where non-global zones are configured, make sure that all the zones are in the installed state before you start Live Upgrade.

You can use Live Upgrade in the following virtualized environments:

<table>
<thead>
<tr>
<th>Environment</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris native zones</td>
<td>Perform Live Upgrade to upgrade both global and local zones. See “Upgrading VCS and Solaris using Live Upgrade” on page 306.</td>
</tr>
<tr>
<td>Solaris branded zones (BrandZ)</td>
<td>Perform Live Upgrade to upgrade the global zone. See “Upgrading VCS and Solaris using Live Upgrade” on page 306.</td>
</tr>
<tr>
<td></td>
<td>VCS6.0 does not support Branded zones. You must migrate applications running on Solaris 8 or Solaris 9 branded zones to Solaris 10 non-global zones if the applications needed to be managed by VCS.</td>
</tr>
<tr>
<td>Oracle VM Server for SPARC</td>
<td>Perform Live Upgrade on the Control domain only. Perform Live Upgrade on the Guest domain only. Use the standard Live Upgrade procedure for both types of logical domains.</td>
</tr>
<tr>
<td></td>
<td>See “Upgrading VCS and Solaris using Live Upgrade” on page 306.</td>
</tr>
</tbody>
</table>

---

**Before you upgrade VCS using Solaris Live Upgrade**

Before you upgrade, perform the following procedure.
To prepare for the Live Upgrade

1. Make sure that the VCS installation media and the operating system installation images are available and on hand.

2. On the nodes to be upgraded, select an alternate boot disk that is at least the same size as the root partition of the primary boot disk.
   If the primary boot disk is mirrored, you need to break off the mirror for the alternate boot disk.

3. Before you perform the Live Upgrade, take offline any services that involve non-root file systems. This prevents file systems from being copied to the alternate boot environment that could potentially cause a root file system to run out of space.

4. On the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.

5. The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:
   - Remove the installed Live Upgrade packages for the current operating system version:
     All Solaris versions: SUNWluu, SUNWlur packages.
     Solaris 10 update 7 or later also requires: SUNWlucfg package.
     Solaris 10 zones or Branded zones also requires: SUNWluzone package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:
     All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.
     Solaris 10 zones or Branded zones also requires: SUNWluzone package.

   **Note:** While you can perform Live Upgrade in the presence of branded zones, they must be halted, and the branded zones themselves are not upgraded.

Solaris installation media comes with a script for this purpose named liveupgrade20. Find the script at
/cdrom/solaris_release/Tools/Installers/liveupgrade20. If scripting, you can use:

```
# /cdrom/solaris_release/Tools/Installers/liveupgrade20 -nodisplay -noconsole
```
Symantec provides the `vxlustart` script that runs a series of commands to create the alternate boot disk for the upgrade. To preview the commands, specify the `vxlustart` script with the `-V` option. Symantec recommends that you preview the commands to ensure there are no problems before beginning the Live Upgrade process.

The `vxlustart` script is located on the distribution media, in the `scripts` directory.

```
# cd /cdrom/scripts

# ./vxlustart -V -u targetos_version -s osimage_path -d diskname
```

- `-V` Lists the commands to be executed during the upgrade process. The `-V` option is a preview option without execution. The `-v` option displays the commands as the script executes them.

- `-u` Specifies the operating system version for the upgrade on the alternate boot disk. For example, use 5.9 for Solaris 9 and 5.10 for Solaris 10.

- `-s` Indicates the path to the operating system image to be installed on the alternate boot disk. If you are upgrading the operating system, specify the path to the new operating system version.

  If you are not upgrading the operating system, and you specify the `-s` option, the `vxlustart -V` command can compare the patches that are installed on the specified image with the patches installed on the primary boot disk.

  If you are not upgrading the operating system, you can omit the `-s` option; the operating system is cloned from the primary boot disk.

- `-d` Indicates the name of the alternate boot disk on which you intend to upgrade. If you do not specify this option with the script, you are prompted for the disk information.

- `-v` Indicates verbose, the executing commands display before they run.

- `-Y` Indicates a default yes with no questions asked.

- `-D` Prints with debug option on, and is for debugging.

- `-F` Specifies the rootdisk's file system, where the default is `ufs`.

- `-t` Specifies the number of CDs involved in upgrade.

- `-r` Specifies that if the machine crashes or reboots before remounting the alternate disk using this option.
For example, to preview the commands to upgrade the Veritas products only:

```
# ./vxlustart -V -u 5.10 -d disk_name
```

For example, to upgrade to Solaris 10 update 6:

```
# ./vxlustart -v -u 5.10 -s /mnt/Solaris_10u6
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6
```

If the specified image is missing patches that are installed on the primary boot disk, note the patch numbers. To ensure that the alternate boot disk is the same as the primary boot disk, you need to install any missing patches on the alternate boot disk.

In the procedure examples, the primary or current boot environment resides on Disk0 (c0t0d0) and the alternate or inactive boot environment resides on Disk1 (c0t1d0).

### Upgrading VCS and Solaris using Live Upgrade

Upgrading VCS and Solaris using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See “Before you upgrade VCS using Solaris Live Upgrade” on page 303.

- Create a new boot environment on the alternate boot disk.
  See “Creating a new boot environment on the alternate boot disk” on page 307.

- Upgrade to VCS 6.0 on the alternate boot environment manually or using the installer.
  To upgrade VCS manually, refer to the following procedure:
    - See “Upgrading VCS manually” on page 309.
  To upgrade VCS using the installer, refer to the following procedure:
    - See “Upgrading VCS using the installer for a Live Upgrade” on page 308.

- Switch the alternate boot environment to be the new primary.
  See “Completing the Live Upgrade” on page 311.

- Verify Live Upgrade of VCS.
  See “Verifying Live Upgrade of VCS” on page 312.
Creating a new boot environment on the alternate boot disk

Run the `vxllustart` command on each node in the cluster to create a new boot environment on the alternate boot disk.

**Note:** This step can take several hours to complete. Do not interrupt the session as it may leave the boot environment unstable.

At the end of the process:

- The Solaris operating system on the alternate boot disk is upgraded, if you have chosen to upgrade the operating system.
- A new boot environment is created on the alternate boot disk by cloning the primary boot environment.

**To create a new boot environment on the alternate boot disk**

Perform the steps in this procedure on each node in the cluster.

1. Navigate to the install media for the Symantec products:
   
   ```
   # cd /cdrom/scripts
   ```

2. View the list of VxVM disks on which you want to create the new boot environment.

   ```
   # vxdisk list
   ```
3 On each node, run one of the following commands:

To upgrade the operating system, by itself or together with upgrading the Veritas products:

```bash
#/vxlustart -v -u targetos_version \ -s osimage_path -d disk_name
```

To upgrade the Veritas products only:

```bash
#/vxlustart -v -u 5.10 -d disk_name
```

See “Before you upgrade VCS using Solaris Live Upgrade” on page 303. Refer to the step on command options.

For example, to upgrade to Solaris 10 update 6:

```bash
#/vxlustart -v -u 5.10 -s /mnt/Solaris_10u6
```

For example, to upgrade the Veritas products only:

```bash
#/vxlustart -v -u 5.10
```

4 Review the output and note the new mount points. If the system is rebooted before completion of the upgrade or if the mounts become unmounted, you may need to remount the disks.

If you need to remount, run the command:

```bash
#/vxlustart -r -u targetos_version -d disk_name
```

5 After the alternate boot disk is created and mounted on /altroot.5.10, install any operating system patches or packages on the alternate boot disk that are required for the Veritas product installation:

```bash
#/pkgadd -R /altroot.5.10 -d pkg_dir
```

---

**Upgrading VCS using the installer for a Live Upgrade**

You can use the Veritas product installer to upgrade VCS as part of the Live Upgrade.

On a node in the cluster, run the installer on the alternate boot disk to upgrade VCS on all the nodes in the cluster. The program uninstalls the existing version of VCS on the alternate boot disk during the process.

At the end of the process the following occurs:
VCS 6.0 is installed on the alternate boot disk.

To perform Live Upgrade of VCS using the installer

1. Insert the product disc with VCS 6.0 or access your copy of the software on the network.

2. Run the installer script specifying the root path as the alternate boot disk:

   ```
   # ./installer -upgrade -rootpath /altroot.5.10
   
   See “Removing and reinstalling VCS using the installer” on page 314.
   ```

3. Enter the names of the nodes that you want to upgrade to VCS 6.0.
   The installer displays the list of packages to be installed or upgraded on the nodes.

4. Press Return to continue with the installation.

   During Live Upgrade, if the OS of the alternate boot disk is upgraded, the installer will not update the VCS configurations for Oracle, Netlsnr, and Sybase resources. If cluster configurations include these resources, you will be prompted to run a list of commands to manually update the configurations after the cluster restarts from the alternate boot disks.

5. Verify that the version of the Veritas packages on the alternate boot disk is 6.0.

   ```
   # pkginfo -R /altroot.5.10 -l VRTSpkgname
   
   For example:
   ```

   ```
   # pkginfo -R /altroot.5.10 -l VRTSvcs
   ```

   Review the installation logs at /altroot.5.10/opt/VRTS/install/logs.

### Upgrading VCS manually

You can perform a manual upgrade of VCS using Live Upgrade. On each node, remove and install the appropriate VCS packages.

At the end of the process the following occurs:

- VCS 6.0 is installed on the alternate boot disk.

To perform Live Upgrade of VCS manually

1. Confirm that the vxlustart script has mounted the secondary (alternate) disk to /altroot.5.10.

   ```
   # mount
   ```
Or

# df -k

2 Remove VCS packages on the alternate boot disk in the following order:

# pkgrm -R /altroot.5.10 \
VRTScmcc VRTScmcs VRTScssim VRTScscm \
VRTSvcsmn VRTSacclib VRTSweb VRTScscw \
VRTSjre15 VRTSvcsag VRTSvcsmg VRTSvcs \
VRTSvxfen VRTSgab VRTSllt VRTSspt VRTSat \
VRTSpbx VRTSicsco VRTSvlic VRTSperl

The -R option removes the packages from the root path /altroot.5.10.

Package lists vary from release to release.

3 Install the VCS packages in the following order one at a time to the alternate boot disk using the pkgadd command. Note that this package list is an example. Full package lists vary from release to release and by product option.

VRTSvlic.pkg VRTSperl.pkg VRTSspt.pkg VRTSat.pkg
VRTSllt.pkg VRTSgab.pkg VRTSvxfen.pkg VRTSamf.pkg
VRTSvcs.pkg VRTScps.pkg VRTSvcsag.pkg VRTSvcsag.pkg

For example:

# pkgadd -R /altroot.5.10 -d package_name.pkg

where you replace package_name.pkg with a package's name, for example VRTSvcs.pkg.

# pkgadd -R /altroot.5.10 -d VRTSvcs.pkg

4 In the /media directory, list the patches for each platform. Enter the following:

# ./installer -listpatches

5 Unzip and extract the tar file for each patch.

# gunzip patch_name.tar.gz
# tar vxf patch_name.tar

where patch_name is the name of a patch listed in step 4.

For example:
Operating System and VCS Live Upgrade:

1. Install the patches on the alternative boot disk using the `patchadd` command.
   ```bash
   # patchadd -R /altroot.5.10 patch_name
   ```
   For example:
   ```bash
   # patchadd -R /altroot.5.10 143282-01
   ```

2. Verify that the version of the packages on the alternate boot disk is 6.0.
   ```bash
   # pkginfo -R /altroot.5.10 -l VRTSvcs
   ```

3. Run the following command to export the root path installation environment variable.
   ```bash
   # export INSTALL_ROOT_PATH=/altroot.5.10
   ```

4. Run the following command on the alternate root path of any one node in the cluster to configure a VCS cluster UUID:
   ```bash
   # /altroot.5.10/opt/VRTSvcs/bin/uuidconfig.pl -clus -configure -use_llthost
   ```
   The `-use_llthost` option indicates that the `/etc/llthost` file is used to determine the names of the nodes in the cluster. Alternatively, you can specify the node names instead of the file name.

5. Confirm that you have created the Universal Unique Identifier:
   ```bash
   # /altroot.5.10/opt/VRTSvcs/bin/uuidconfig.pl -clus -display -use_llthost
   ```

Completing the Live Upgrade:

At the end of the process:
- The alternate boot environment is activated.
- The system is booted from the alternate boot disk.
To complete the Live Upgrade

1. Complete the Live upgrade process. Enter the following command on all nodes in the cluster.

```
# ./vcslufinish -u target_os_version
Live Upgrade finish on the Solaris release <5.10>
```

2. If the system crashes or reboots before Live Upgrade completes successfully, you can remount the alternate disk using the following command:

```
# ./vxlustart -r -u target_os_version
```

Then, rerun the `vcslufinish` command from step 1

```
# ./vcslufinish -u target_os_version
```

3. **Note:** Do not use the `reboot`, `halt`, or `uadmin` commands to reboot the system. Use either the `init` or the `shutdown` commands to enable the system to boot using the alternate boot environment.

You can ignore the following error if it appears: ERROR: boot environment <dest.13445> already mounted on </altroot.5.10>.

```
# shutdown -g0 -y -i6
```

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

For instructions to upgrade VCS or SFHA on the CP server systems, see the VCS or SFHA Installation Guide.

**Verifying Live Upgrade of VCS**

To ensure that Live Upgrade has completed successfully, verify that all the nodes have booted from the alternate boot environment and joined the cluster.
To verify that Live Upgrade completed successfully

1 Verify that the alternate boot environment is active.

   # lustatus

   If the alternate boot environment is not active, you can revert to the primary boot environment.

   See “Reverting to the primary boot environment” on page 316.

2 Make sure that GAB ports a and h are up.

   # gabconfig -a
   Port a gen 39d901 membership 01
   Port h gen 39d909 membership 01

3 Perform other verification as required to ensure that the new boot environment is configured correctly. For example, verify the version in the /etc/release file and verify the VRTSdbac version.

4 In a zone environment, verify the zone configuration.

Upgrading Solaris using Live Upgrade

If you are upgrading Solaris only, you must remove and reinstall VCS from the alternate boot environment prior to completing the Live Upgrade even if VCS has version 6.0 on the primary. You must remove and reinstall because VCS has kernel components that are specific to Solaris operating system versions. The correct version of the VCS packages must be installed.

Upgrading Solaris using Live Upgrade involves the following steps:

- Preparing to upgrade using Solaris Live Upgrade.
  See “Before you upgrade VCS using Solaris Live Upgrade” on page 303.

- Creating a new boot environment on the alternate boot disk
  See “Creating a new boot environment on the alternate boot disk” on page 307.

- Removing and reinstalling VCS 6.0 on the alternate boot environment, in one of the following ways:
  Using manual steps:
  See “Upgrading VCS manually” on page 309.
  Using the installer:
  See “Removing and reinstalling VCS using the installer” on page 314.

Note: Do NOT configure the VCS 6.0
Switching the alternate boot environment to be the new primary
See “Completing the Live Upgrade” on page 311.

Verifying Live Upgrade of VCS.
See “Verifying Live Upgrade of VCS” on page 312.

Removing and reinstalling VCS using the installer

VCS has kernel components that are specific for Solaris operating system versions. When you use Solaris Live Upgrade to upgrade the Solaris operating system, you must complete these steps to ensure the correct version of VCS components are installed.

On a node in the cluster, run the installer on the alternate boot disk to remove and reinstall VCS 6.0 on all the nodes in the cluster.

At the end of the process the following occurs:

VCS 6.0 is installed on the alternate boot disk, with the correct binaries for the new operating system version

To remove and reinstall VCS using the installer

1. Uninstall using the installer script, specifying the alternate boot disk as the root path:

   ```
   # /opt/VRTS/install/uninstallvcs -rootpath altrootpath
   ```

   For example:

   ```
   # /opt/VRTS/install/uninstallvcs -rootpath /altroot.5.10
   ```

2. Enter the names of the nodes that you want to uninstall.
   The installer displays the list of packages that will be uninstalled.

3. Press Return to continue.

4. Insert the product disc and run the following commands:

   ```
   # ./installvcs -install -rootpath altrootpath
   ```

   For example:

   ```
   # cd /cdrom/cluster_server
   # ./installvcs -install -rootpath /altroot.5.10
   ```

   The installer displays the list of packages that will be installed.
5 Press **Return** to continue.

6 Verify that the version of the Veritas packages on the alternate boot disk is 6.0.

```bash
# pkginfo -R /altroot.5.10 -l VRTSpkgname
```

For example:

```bash
# pkginfo -R /altroot.5.10 -l VRTSvcs
```

Review the installation logs at `/altroot.5.10/opt/VRTS/install/log`.

---

**Upgrading VCS using Live Upgrade**

Perform the Live Upgrade manually or use the installer. The nodes will not form a cluster until all of the nodes are upgraded to VCS 6.0. At the end of the Live Upgrade of the last node, all the nodes must boot from the alternate boot environment and join the cluster.

Upgrading VCS using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See “Before you upgrade VCS using Solaris Live Upgrade” on page 303.

- Create a new boot environment on the alternate boot disk.
  See “Creating a new boot environment on the alternate boot disk” on page 307.

- Upgrade to VCS 6.0 on the alternate boot environment manually or using the installer. Refer to one of the following:
  To upgrade VCS manually:
    - See “Upgrading VCS manually” on page 309.
  To upgrade VCS using the installer:
    - See “Upgrading VCS using the installer for a Live Upgrade” on page 308.

- Switch the alternate boot environment to be the new primary.
  See “Completing the Live Upgrade” on page 311.

- Verify Live Upgrade of VCS.
  See “Verifying Live Upgrade of VCS” on page 312.

---

**Administering boot environments**

Use the following procedures to perform relevant administrative tasks for boot environments.
Reverting to the primary boot environment

If the alternate boot environment fails to start, you can revert to the primary boot environment.

On each node, start the system from the primary boot environment in the PROM monitor mode.

ok> setenv boot-device disk_0
ok> boot

Failure to perform this step can result in the operating system booting from the alternate boot environment after the reboot.

The vcslufinish script displays the way to revert to primary boot environment. Here is a sample output.

Notes:

******************************************************************************
In case of a failure while booting to the target BE, the following process needs to be followed to fallback to the currently working boot environment:
1. Enter the PROM monitor (ok prompt).
2. Change the boot device back to the original boot environment by typing:
   setenv boot-device /pci@1c,600000/scsi@2/disk@0,0:a
3. Boot to the original boot environment by typing:
   boot
******************************************************************************

Switching the boot environment for Solaris SPARC

You do not have to perform the following procedures to switch the boot environment when you use the vxlustart and vcslufinish scripts to process Live Upgrade. You must perform the following procedures when you perform a manual Live Upgrade.
To switch the boot environment

1. Display the status of Live Upgrade boot environments.

   ```
   # lustatus
   ```

<table>
<thead>
<tr>
<th>Boot Environment</th>
<th>Is Complete</th>
<th>Active</th>
<th>Can</th>
<th>Copy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Now on Reboot</td>
<td>Delete</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>source.2657</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>-</td>
</tr>
<tr>
<td>dest.2657</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

   In this example, the primary boot disk is currently (source.2657). You want to activate the alternate boot disk (dest.2657).

2. Unmount any file systems that are mounted on the alternate root disk (dest.2657).

   ```
   # lufslist dest.2657
   ```

   ```
   boot environment name: dest.2657
   ```

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>fstype</th>
<th>device</th>
<th>size</th>
<th>Mounted on</th>
<th>Mount Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/dsk/c0t0d0s1 swap</td>
<td>swap</td>
<td>4298342400</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s0 ufs</td>
<td>ufs</td>
<td>15729328128</td>
<td>/</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s5 ufs</td>
<td>ufs</td>
<td>8591474688</td>
<td>/var</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s3 ufs</td>
<td>ufs</td>
<td>5371625472</td>
<td>/vxfs</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

   ```
   # luumount dest.2657
   ```

3. Activate the Live Upgrade boot environment.

   ```
   # luactivate dest.2657
   ```

4. Reboot the system.

   ```
   # shutdown -g0 -i6 -y
   ```

   The system automatically selects the boot environment entry that was activated.

Switching the boot environment for Solaris x86-64

You do not have to perform the following procedures to switch the boot environment when you use the vxlustart and vcslnufinish scripts to process
Live Upgrade. You must perform the following procedures when you perform a manual Live Upgrade.

**To switch the boot environment**

1. Display the status of Live Upgrade boot environments.

   ```bash
   # lustatus
   ```

<table>
<thead>
<tr>
<th>Boot Environment Name</th>
<th>Complete</th>
<th>Active</th>
<th>Active</th>
<th>Can Copy</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>source.2657</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>-</td>
</tr>
<tr>
<td>dest.2657</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>-</td>
</tr>
</tbody>
</table>

   In this example, the primary boot disk is currently (source.2657). You want to activate the alternate boot disk (dest.2657).

2. Unmount any file systems that are mounted on the alternate root disk (dest.2657).

   ```bash
   # luflist dest.2657
   # luumount dest.2657
   ```
3 Activate the Live Upgrade boot environment.

   # luactivate dest.2657

4 Reboot the system.

   # shutdown -g0 -i6 -y

When the system boots up, the GRUB menu displays the following entries for the Live Upgrade boot environments:

source.2657
dest.2657

The system automatically selects the boot environment entry that was activated.
Upgrading the Solaris operating system

This chapter includes the following topics:

- Upgrading Solaris versions
- Upgrading Solaris on a node

Upgrading Solaris versions

An operating system upgrade can take hours to finish. When you upgrade, you typically upgrade one node at a time. Coordinate with your system administrator to plan for the down time of each system. Plan ahead to move service groups to running nodes, while the nodes that you upgrade are down. Planning ahead reduces downtime and ensures availability of services for your customers.

When you upgrade the operating system, you must remove the GAB, LLT, and fencing packages and patches before you upgrade the operating system. Reinstall fencing, GAB, and LLT after upgrading the operating system.

---

**Note:** Be sure that you have the Symantec software disc with the VCS software on hand before you begin.

---

You must upgrade the operating system on each node in the cluster to completely upgrade the Solaris versions in the cluster.

Upgrading Solaris on a node

The tasks that you need to perform when upgrading the Solaris operating system include the following:
Stopping VCS

Stopping fencing, GAB, LLT, and unloading the kernel modules

Removing packages and patches

Upgrading Solaris operating system

Reinstalling fencing, GAB, and LLT from the software disc

Restarting VCS

To stop VCS

1. Make the VCS configuration writable. On the first system, type:

    # haconf -makerw

2. Move all service groups from the node you are planning to upgrade to another system. Keep services from failing over to this server. On the system where you plan to upgrade, type:

    # hasys -freeze -persistent -evacuate upgrade_server

3. Check if all service groups and resources are offline on the system and online on the other system. Type:

    # hastatus -summary

4. Close the configuration and unload the VCS services on the system that you plan to upgrade. On the system that you plan to upgrade, type:

    # haconf -dump -makero
    # hastop -local

5. Confirm that VCS has stopped. On the upgrading system, type:

    # gabconfig -a

Output resembles:

```
GAB Port Memberships
=======================================
Port a gen 23dc0001 membership 01
```

Note that the output shows no membership for port h.
To stop fencing, GAB, LLT, and unload the kernel modules

1  Unconfigure fencing.
   
   # vxfenconfig -U

2  Unload the FENCING module from the kernel. Perform the following:
   ■ Determine the kernel module ID.
      
      # modinfo | grep vxfen
   ■ Unload the module from the kernel.
      
      # modunload -i vxfen_id

3  Unconfigure GAB.
   
   # gabconfig -U

4  Unload the GAB module from the kernel:
   ■ Determine the kernel module ID:
      
      # modinfo | grep gab
   ■ Unload the module from the kernel:
      
      # modunload -i gab_id

5  Unconfigure LLT. On each system, type:
   
   # lltconfig -U

   The following message is displayed on the console:

   lltconfig: this will attempt to stop and reset LLT. Confirm (y/n)?

   6  Type y on each system in response to the message.

   7  Unload the LLT module from the kernel:
   ■ Determine the kernel module ID:
      
      # modinfo | grep llt

      The module IDs are in the left-hand column of the output.
Unload the module from the kernel:

```
# modunload -i llt_id
```

To remove the fencing, GAB, and LLT packages and patches

- On each node, use the `pkgrm` command to remove the fencing, GAB, and LLT packages.

```
# pkgrm VRTSvxfen VRTSgab VRTSllt
```

To upgrade the operating system

1. Follow the Oracle installation guide to upgrade the operating system kernel to the new version of Solaris.
2. As the system comes up, enter single-user mode.

To reinstall fencing, GAB, and LLT from the software disc and restart

1. In single-user mode, log on as superuser on the system that you have upgraded.
2. Check whether the /tmp directory is mounted.

```
# mount
```

3. If the /tmp directory is not mounted, then enter:

```
# mount /tmp
```

4. Create a directory for installation:

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

5. Insert the software disc with the VCS software into a system drive where you have upgraded. The Solaris volume-management software automatically mounts the disc as /cdrom/cdrom0. Type the command:

```
# cd /cdrom/cdrom0
```

6. Copy the package files from the software disc to the temporary directory:

```
# cp -r pkgs/VRTSllt.pkg /tmp/install
# cp -r pkgs/VRTSgab.pkg /tmp/install
# cp -r pkgs/VRTSvxfen.pkg /tmp/install
```
7 Install the LLT, GAB, and fencing packages and patches. As you enter the command, be sure to install the packages and patches in the order shown:

- Install the packages.

```bash
# cd /tmp/install
# pkgadd -d VRTSllt.pkg
# pkgadd -d VRTSgab.pkg
# pkgadd -d VRTSvxfen.pkg
```

8 Bring up the system in multi-user mode:

```bash
# cd /
# init 3
```

To restart VCS

1 Verify that VCS services are running on the upgraded server. On the upgraded server, type:

```bash
# ps -ef | grep ha
root  576  1  0 16:54:12 ? 0:02 /opt/VRTSvcs/bin/had
root  578  1  0 16:54:13 ? 0:00 /opt/VRTSvcs/bin/hashadow
```

2 If the VCS services are not running, reload the VCS services. Type:

```bash
# hastart
```

3 Make the configuration writable.

```bash
# haconf -makerw
```

4 Unfreeze the upgraded server and save the configuration. On the upgraded server, type:

```bash
# hasys -unfreeze -persistent upgraded_server
# haconf -dump -makero
```
Upgrading the Solaris operating system

Upgrading Solaris on a node
Post-installation tasks

- Chapter 26. Performing post-installation tasks
- Chapter 27. Installing or upgrading VCS components
- Chapter 28. 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 Oracle Directory Server, Netscape, OpenLDAP, and Windows Active Directory.

For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain.

See “Enabling LDAP authentication for clusters that run in secure mode” on page 331.

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 26-1 depicts the VCS cluster communication with the LDAP servers when clusters run in secure mode.
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)
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

See the vssat.1m and the atldapconf.1m manual pages.
To enable OpenLDAP authentication for clusters that run in secure mode

1  Add the LDAP domain to the AT configuration using the `vssat` command.

   The following example adds the LDAP domain, MYENTERPRISE:

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat addldapdomain \
   --domainname "MYENTERPRISE.symantecdomain.com" \
   --server_url "ldap://my_openldap_host.symantecexample.com" \
   --user_base_dn "ou=people,dc=symantecdomain,dc=myenterprise,dc=com" \
   --user_attribute "cn" --user_object_class "account" \
   --user_gid_attribute "gidNumber" \
   --group_base_dn "ou=group,dc=symantecdomain,dc=myenterprise,dc=com" \
   --group_attribute "cn" --group_object_class "posixGroup" \
   --group_gid_attribute "member" \
   --admin_user "cn=manager,dc=symantecdomain,dc=myenterprise,dc=com" \
   --admin_user_password "password" --auth_type "FLAT"
   ```

2  Verify that you can successfully authenticate an LDAP user on the VCS nodes.

   You must have a valid LDAP user ID and password to run the command. In the following example, authentication is verified for the MYENTERPRISE domain for the LDAP user, vcsadmin1.

   ```
   galaxy# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat authenticate \
   --domain ldap:MYENTERPRISE.symantecdomain.com \
   --prplname vcsadmin1 --broker galaxy:14149
   
   Enter password for vcsadmin1: ##########
   
   authenticate
   ----------------------
   ----------------------
   Authenticated User vcsadmin1
   ----------------------
   ```
3 Add the LDAP user to the main.cf file.

```
# haconf makerw
# hauser -add "CN=vcsadmin1/CN=people/DC=symantecdomain/DC=myenterprise/DC=com@myenterprise.symantecdomain.com" -priv Administrator
# haconf -dump -makero
```

If you want to enable group-level authentication, you must run the following command:

```
# hauser -addpriv \
ldap_group@ldap_domain AdministratorGroup
```

4 Verify that the main.cf file has the following lines:

```
# cat /etc/VRTSvcs/conf/config/main.cf
...
...
cluster clus1 {
    SecureClus = 1
    Administrators = {
        "CN=vcsadmin1/CN=people/DC=symantecdomain/DC=myenterprise/DC=com@myenterprise.symantecdomain.com"
    }
    AdministratorGroups = {
        "CN=symantecusergroups/DC=symantecdomain/DC=myenterprise/DC=com@myenterprise.symantecdomain.com "
    }
}
...
...
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=myenterprise.symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh) or the Korn shell (ksh), run the following commands:

```
# export VCS_DOMAIN=myenterprise.symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```
6 Verify that you can log on to VCS. For example

```bash
# halogin vcsadmin1 password
# hasys -state
```

```
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System   Attribute   Value
  galaxy   Attribute   RUNNING
  nebula   Attribute   RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the VCS node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.
To enable Windows Active Directory authentication for clusters that run in secure mode

1. Run the LDAP configuration tool atldapconf using the -d option. The -d option discovers and retrieves an LDAP properties file which is a prioritized attribute list.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf -d \n-s domain_controller_name_or_ipaddress \n-u domain_user -g domain_group
```

For example:

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \n-d -s 192.168.20.32 -u Administrator -g "Domain Admins"
```

Search User provided is invalid or Authentication is required to proceed further. Please provide authentication information for LDAP server.

Username/Common Name: `symantecdomain\administrator`

Password: `*`

Attribute file created.

2. Run the LDAP configuration tool atldapconf using the -c option. The -c option creates a CLI file to add the LDAP domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \n-c -d windows_domain_name
```

For example:

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \n-c -d symantecdomain.com
```

Attribute list file not provided, using default AttributeList.txt. CLI file name not provided, using default CLI.txt.

CLI for addldapdomain generated.

3. Run the LDAP configuration tool atldapconf using the -x option. The -x option reads the CLI file and executes the commands to add a domain to the AT.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf -x
```
4 List the LDAP domains to verify that the Windows Active Directory server integration is complete.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat listldapdomains
```

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>symantecdomain.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server URL</td>
<td>ldap://192.168.20.32:389</td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>No</td>
</tr>
<tr>
<td>User Base DN</td>
<td>CN=people,DC=symantecdomain,DC=com</td>
</tr>
<tr>
<td>User Object Class</td>
<td>account</td>
</tr>
<tr>
<td>User Attribute</td>
<td>cn</td>
</tr>
<tr>
<td>User GID Attribute</td>
<td>gidNumber</td>
</tr>
<tr>
<td>Group Base DN</td>
<td>CN=group,DC=symantecdomain,DC=com</td>
</tr>
<tr>
<td>Group Object Class</td>
<td>group</td>
</tr>
<tr>
<td>Group Attribute</td>
<td>cn</td>
</tr>
<tr>
<td>Group GID Attribute</td>
<td>cn</td>
</tr>
<tr>
<td>Auth Type</td>
<td>FLAT</td>
</tr>
<tr>
<td>Admin User</td>
<td></td>
</tr>
<tr>
<td>Admin User Password</td>
<td></td>
</tr>
<tr>
<td>Search Scope</td>
<td>SUB</td>
</tr>
</tbody>
</table>

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh) or the Korn shell (ksh), run the following commands:

```
# export VCS_DOMAIN=symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```
6 Verify that you can log on to VCS. For example

```bash
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System     Attribute     Value
  galaxy     Attribute     RUNNING
  nebula     Attribute     RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the VCS node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.

**Accessing the VCS documentation**

The software disc contains the documentation for VCS in Portable Document Format (PDF) in the `cluster_server/docsdirectory`. 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.
Performing post-installation tasks

Removing permissions for communication
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

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 Solaris system with X-Windows. 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.

When you install the Java Console on the Solaris system, make sure a printer is configured to that system. If you print the online JavaHelp on a system that does not have a printer that is configured, the Java Console might hang.

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:
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.

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 Solaris

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 Solaris

1. Create a directory for installation of the Java Console:

   ```
   # mkdir /tmp/install
   ```
2 Download the Java GUI utility from http://go.symantec.com/vcsm_download to a temporary directory.

3 Go to the temporary directory and unzip the compressed package file using the gunzip utility:

```bash
# cd /tmp/install
# gunzip VRTScscm.tar.gz
```

The file VRTScscm.tar is now present in the temporary directory.

4 Extract the compressed file from the tar file:

```bash
# tar -xvf VRTScscm.tar
```

5 Install the software:

```bash
# pkgadd -d . VRTScscm
```

6 Answer Yes if prompted.

### 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 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 Solaris

1. Log in as superuser on the node where you intend to install the package.

2. Remove the GUI from the previous installation.

   \[ \texttt{# pkgrm VRTScsm} \]

3. Install the VCS Java console.

   See “Installing the Java Console on Solaris” on page 340.

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 \texttt{Add/Remove Programs}
   - Select \texttt{Veritas Cluster Manager}.
   - Click \texttt{Add/Remove}.
   - Follow the uninstall wizard instructions.

3. Install the new Cluster Manager.

   See “Installing the Java Console on a Windows system” on page 341.

Installing VCS Simulator

You can administer VCS Simulator from the Java Console or from the command line. For more information, see the \textit{Veritas Cluster Server Administrator's Guide}. Review the software requirements for VCS Simulator.

Software requirements for VCS Simulator

VCS Simulator is supported on:


\[ \textbf{Note:} \text{Make sure that you are using an operating system version that supports JRE 1.6 or later.} \]

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

1. Download VCS Simulator from the following location to a temporary directory.
2. Extract the compressed files to another directory.
3. Navigate to the path of the Simulator installer file:
   \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:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>attrpool</td>
<td>Information about attributes associated with VCS objects</td>
</tr>
<tr>
<td>bin</td>
<td>VCS Simulator binaries</td>
</tr>
<tr>
<td>default_clus</td>
<td>Files for the default cluster configuration</td>
</tr>
<tr>
<td>sample_clus</td>
<td>A sample cluster configuration, which serves as a template for each new cluster configuration</td>
</tr>
<tr>
<td>templates</td>
<td>Various templates that are used by the Java Console</td>
</tr>
<tr>
<td>types</td>
<td>The types.cf files for all supported platforms</td>
</tr>
<tr>
<td>conf</td>
<td>Contains another directory called types. This directory contains assorted resource type definitions that are useful for the Simulator. The type definition files are present in platform-specific sub directories.</td>
</tr>
</tbody>
</table>

Additionally, VCS Simulator installs directories for various cluster configurations.
VCS Simulator creates a directory for every new simulated cluster and copies the contents of the sample_clus directory. Simulator also creates a log directory within each cluster directory for logs that are associated with the cluster.

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 342.
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/.uuuids/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/lLttab
   - GAB
     /etc/gabtab
   - VCS
     /etc/VRTSvcs/conf/config/main.cf
2. Verify the content of the configuration files.
   See “About the LLT and GAB configuration files” on page 453.
   See “About the VCS configuration files” on page 457.

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 68.
3. Verify LLT operation.
   See “Verifying LLT” on page 347.
4. Verify GAB operation.
   See “Verifying GAB” on page 349.
5. Verify the cluster operation.
   See “Verifying the cluster” on page 351.
Verifying LLT

Use the `lltstat` command to verify that links are active for LLT. If LLT is configured correctly, this command shows all the nodes in the cluster. The command also returns information about the links for LLT for the node on which you typed the command.

Refer to the `lltstat(1M)` manual page for more information.

**To verify LLT**

1. Log in as superuser on the node galaxy.
2. Run the `lltstat` command on the node galaxy to view the status of LLT.

   ```
   lltstat -n
   
   The output on galaxy resembles:
   
   LLT node information:
   
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0</td>
<td>galaxy</td>
<td>OPEN</td>
</tr>
<tr>
<td>1</td>
<td>nebula</td>
<td>OPEN</td>
</tr>
</tbody>
</table>
   
   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:
   
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0</td>
<td>galaxy</td>
<td>OPEN</td>
</tr>
<tr>
<td>1</td>
<td>nebula</td>
<td>OPEN</td>
</tr>
<tr>
<td>2</td>
<td>saturn</td>
<td>OPEN</td>
</tr>
</tbody>
</table>
   
   3. Log in as superuser on the node nebula.
4. Run the `lltstat` command on the node nebula to view the status of LLT.

   ```
   lltstat -n
   ```

   The output on nebula resembles:

   LLT node information:
   
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>galaxy</td>
<td>OPEN</td>
</tr>
<tr>
<td>*1</td>
<td>nebula</td>
<td>OPEN</td>
</tr>
</tbody>
</table>
5 To view additional information about LLT, run the `lltstat -nvv` command on each node.

For example, run the following command on the node galaxy in a two-node cluster:

```
lltstat -nvv active
```

The output on galaxy resembles the following:

- For Solaris SPARC:

<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>Link</th>
<th>Status</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0 galaxy</td>
<td>OPEN</td>
<td>qfe:0</td>
<td>UP</td>
<td>08:00:20:93:0E:34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>qfe:1</td>
<td>UP</td>
<td>08:00:20:93:0E:38</td>
</tr>
<tr>
<td>1 nebula</td>
<td>OPEN</td>
<td>qfe:0</td>
<td>UP</td>
<td>08:00:20:8F:D1:F2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>qfe:1</td>
<td>DOWN</td>
<td></td>
</tr>
</tbody>
</table>

- For Solaris x64:

<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>Link</th>
<th>Status</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0 galaxy</td>
<td>OPEN</td>
<td>e1000g:1</td>
<td>UP</td>
<td>08:00:20:93:0E:34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e1000g:2</td>
<td>UP</td>
<td>08:00:20:93:0E:38</td>
</tr>
<tr>
<td>1 nebula</td>
<td>OPEN</td>
<td>e1000g:1</td>
<td>UP</td>
<td>08:00:20:8F:D1:F2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e1000g:2</td>
<td>DOWN</td>
<td></td>
</tr>
</tbody>
</table>

The command reports the status on the two active nodes in the cluster, galaxy and nebula.

For each correctly configured node, the information must show the following:
- A state of OPEN
- A status for each link of UP
- An address for each link

However, the output in the example shows different details for the node nebula. The private network connection is possibly broken or the information in the `/etc/llttab` file may be incorrect.

6 To obtain information about the ports open for LLT, type `lltstat -p` on any node.

For example, type `lltstat -p` on the node galaxy in a two-node cluster:
The output resembles:

<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: 0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63</td>
<td></td>
</tr>
<tr>
<td></td>
<td>connects: 0 1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>gab</td>
<td>0x7</td>
</tr>
<tr>
<td></td>
<td>opens: 0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63</td>
<td></td>
</tr>
<tr>
<td></td>
<td>connects: 0 1</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>gab</td>
<td>0x1F</td>
</tr>
<tr>
<td></td>
<td>opens: 0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63</td>
<td></td>
</tr>
<tr>
<td></td>
<td>connects: 0 1</td>
<td></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  galaxy     RUNNING  0
   A  nebula     RUNNING  0

   -- GROUP STATE
   -- Group               System  Probed AutoDisabled  State
   B  ClusterService     galaxy  Y   N           Y  ONLINE
   B  ClusterService     nebula  Y   N           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 galaxy and OFFLINE on nebula.

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.
**Note:** The example in the following procedure is for SPARC. x64 clusters have different command output.

To verify the cluster nodes

- On one of the nodes, type the `hasys -display` command:

```
# hasys -display
```

The example shows the output when the command is run on the node galaxy. The list continues with similar information for nebula (not shown) and any other nodes in the cluster.

<table>
<thead>
<tr>
<th>System</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>galaxy</td>
<td>AgentsStopped</td>
<td>0</td>
</tr>
<tr>
<td>galaxy</td>
<td>AvailableCapacity</td>
<td>100</td>
</tr>
<tr>
<td>galaxy</td>
<td>CPUBinding</td>
<td>BindTo None CPUNumber 0</td>
</tr>
<tr>
<td>galaxy</td>
<td>CPURuntimeLimit</td>
<td>Critical 90 Warning 80 Note 70 Info 60</td>
</tr>
<tr>
<td>galaxy</td>
<td>CPUUsageMonitoring</td>
<td>Enabled 0 ActionThreshold 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ActionTimeLimit 0 Action NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NotifyThreshold 0 NotifyTimeLimit 0</td>
</tr>
<tr>
<td>galaxy</td>
<td>Capacity</td>
<td>100</td>
</tr>
<tr>
<td>galaxy</td>
<td>ConfigBlockCount</td>
<td>130</td>
</tr>
<tr>
<td>galaxy</td>
<td>ConfigCheckSum</td>
<td>46688</td>
</tr>
<tr>
<td>galaxy</td>
<td>ConfigDiskState</td>
<td>CURRENT</td>
</tr>
<tr>
<td>galaxy</td>
<td>ConfigFile</td>
<td>/etc/VRTSvcs/conf/config</td>
</tr>
<tr>
<td>galaxy</td>
<td>ConfigInfoCnt</td>
<td>0</td>
</tr>
<tr>
<td>galaxy</td>
<td>ConfigModDate</td>
<td>Thu Sep 22 07:14:23 CDT 2011</td>
</tr>
<tr>
<td>galaxy</td>
<td>ConnectorState</td>
<td>Down</td>
</tr>
<tr>
<td>galaxy</td>
<td>CurrentLimits</td>
<td></td>
</tr>
<tr>
<td>galaxy</td>
<td>DiskHbStatus</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>DynamicLoad</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EngineRestarted</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EngineVersion</td>
<td>6.0.00.0</td>
<td></td>
</tr>
<tr>
<td>FencingWeight</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Frozen</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>GUIIPAddr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HostUtilization</td>
<td>CPU 7 Swap 0</td>
<td></td>
</tr>
<tr>
<td>LLTNodeId</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LicenseType</td>
<td>PERMANENT_SITE</td>
<td></td>
</tr>
<tr>
<td>Limits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LinkHbStatus</td>
<td>qfe:0 UP qfe:1 UP</td>
<td></td>
</tr>
<tr>
<td>LoadTimeCounter</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LoadTimeThreshold</td>
<td>600</td>
<td></td>
</tr>
<tr>
<td>LoadWarningLevel</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>NoAutoDisable</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>NodeId</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>OnGrpCnt</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>PhysicalServer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ShutdownTimeout</td>
<td>600</td>
<td></td>
</tr>
<tr>
<td>SourceFile</td>
<td>./main.cf</td>
<td></td>
</tr>
<tr>
<td>SwapThresholdLevel</td>
<td>Critical 90 Warning 80 Note 70 Info 60</td>
<td></td>
</tr>
<tr>
<td>SysInfo</td>
<td>Solaris:galaxy,Generic_118558-11,5.9,sun4u</td>
<td></td>
</tr>
<tr>
<td>SysName</td>
<td>galaxy</td>
<td></td>
</tr>
<tr>
<td>SysState</td>
<td>RUNNING</td>
<td></td>
</tr>
<tr>
<td>SystemLocation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 354.

To run the postcheck command on a node

1. Run the installer with the -postcheck option.

   ```
   # ./installer -postcheck system_name
   ```

2. Review the output for installation-related information.

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.
- 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.

See “Performing a postcheck on a node” on page 354.
Uninstalling VCS

- Chapter 29. Uninstalling VCS using the installer
- Chapter 30. Uninstalling VCS using response files
- Chapter 31. 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
- Uninstalling VCS with the Veritas Web-based installer
- Removing language packages using the uninstaller program
- Removing the CP server configuration using the removal script

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.
  
  See "About adding and removing nodes" on page 385.

- 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 72.
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 packages and VCS language packages.

The example demonstrates how to uninstall VCS using the uninstallvcs program. The uninstallvcs program uninstalls VCS on two nodes: galaxy nebula. The example procedure uninstalls VCS from all nodes in the cluster.

Removing VCS 6.0 packages

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
   ```

   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:
Verifies the communication between systems
Checks the installations on each system to determine the packages to be uninstalled.

6 Review the output as the uninstaller stops processes, unloads kernel modules, and removes the packages.

7 Note the location of summary, response, and log files that the uninstaller creates after removing all the packages.

Running uninstallvcs from the VCS 6.0 disc
You may need to use the uninstallvcs program on the VCS 6.0 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

Uninstalling VCS with the Veritas Web-based installer
This section describes how to uninstall using the Veritas Web-based installer.

Note: After you uninstall the product, you cannot access any file systems you created using the default disk layout Version in VCS 6.0 with a previous version of VCS.

To uninstall VCS

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

2 Start the Web-based installer.
See “Starting the Veritas Web-based installer” on page 162.

3 On the Select a task and a product page, select Uninstall a Product from the Task drop-down list.

4 Select Veritas Cluster Server from the Product drop-down list, and click Next.
5 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click Next.

6 After the validation completes successfully, click Next to uninstall VCS on the selected system.

7 If there are any processes running on the target system, the installer stops the processes. Click Next.

8 After the installer stops the processes, the installer removes the products from the specified system.

   Click Next.

9 After the uninstall completes, the installer displays the location of the summary, response, and log files. If required, view the files to confirm the status of the removal.

10 Click Finish.

   You see a prompt recommending that you reboot the system, and then return to the Web page to complete additional tasks.

Removing language packages using the uninstaller program

The uninstallvcs program removes all VCS packages and language packages.

Removing the CP server configuration using the removal script

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.

---

You can use the CP server configuration utility (`configure_cps.pl`) to remove the CP server configuration. This utility performs the following tasks when you choose to unconfigure the CP server:

- Removes all CP server configuration files
- Removes the VCS configuration for CP server

After you run this utility, you can uninstall VCS from the node or the cluster.
**Note:** You must run the configuration utility only once per CP server (which can be on a single-node VCS cluster or an SFHA cluster), when you want to remove the CP server configuration.

**To remove the CP server configuration**

1. To run the configuration removal script, enter the following command on the node where you want to remove the CP server configuration:

   ```bash
   root@mycps1.symantecexample.com # /opt/VRTScps/bin/configure_cps.pl
   ```

2. Select option 3 from the menu to unconfigure the CP server.

   **VERITAS COORDINATION POINT SERVER CONFIGURATION UTILITY**
   
   Select one of the following:

   [1] Configure Coordination Point Server on single node VCS system
   
   [2] Configure Coordination Point Server on SFHA cluster
   
   [3] Unconfigure Coordination Point Server

3. Review the warning message and confirm that you want to unconfigure the CP server.

   **WARNING:** Unconfiguring Coordination Point Server stops the vxcpserv process. VCS clusters using this server for coordination purpose will have one less coordination point.

   Are you sure you want to bring down the cp server? (y/n)
   (Default:n) : y

4. Review the screen output as the script performs the following steps to remove the CP server configuration:

   - Stops the CP server
   - Removes the CP server from VCS configuration
   - Removes resource dependencies
   - Takes the the CP server service group (CPSSG) offline, if it is online
   - Removes the CPSSG service group from the VCS configuration
5   Answer **y** to delete the CP server database.

   Do you want to delete the CP Server database? (y/n) (Default:n) :

6   Answer **y** at the prompt to confirm the deletion of the CP server database.

   Warning: This database won't be available if CP server is reconfigured on the cluster. Are you sure you want to proceed with the deletion of database? (y/n) (Default:n) :

7   Answer **y** to delete the CP server configuration file and log files.

   Do you want to delete the CP Server configuration file (/etc/vxcps.conf) and log files (in /var/VRTScps)? (y/n) (Default:n) : **y**

8   Run the **hagrp -state** command to ensure that the CPSSG service group has been removed from the node. For example:

   root@mycps1.symantecexample.com # hagrp -state CPSSG

   VCS WARNING V-16-1-40131 Group CPSSG does not exist in the local cluster
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 367.
3. Edit the values of the response file variables as necessary.
   
   See “Response file variables to uninstall VCS” on page 366.
4. Start the uninstallation from the system to which you copied the response file. For example:

   ```
   # /opt/VRTS/install/uninstallvcs -responsefile /tmp/response_file
   ```

   Where `/tmp/response_file` is the response file’s full path name.
Response file variables to uninstall VCS

Table 30-1 lists the response file variables that you can define to uninstall 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 packages. (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. The value is VCS51 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. (Optional)</td>
</tr>
</tbody>
</table>

Note: The installer copies the response files and summary files also to the specified logpath location.
Sample response file for uninstalling VCS

Review the response file variables and their definitions.
See “Response file variables to uninstall VCS” on page 366.

# Configuration Values:
our %CFG;

$CFG{opt}{uninstall}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw(galaxy nebula) ];
1;
Uninstalling VCS using response files

Sample response file for uninstalling VCS
Manually uninstalling VCS

This chapter includes the following topics:

■ Removing VCS packages manually
■ Manually remove the CP server fencing configuration
■ Manually deleting cluster details from a CP server

Removing VCS packages manually

You must remove the VCS packages from each node in the cluster to uninstall VCS.

To manually remove VCS packages on a node

1  Shut down VCS on the local system using the hastop command.

   # hastop -local

2  Unconfigure the fencing, GAB, LLT, and AMF modules.

   # /sbin/vxfenconfig -U
   # /sbin/gabconfig -U
   # /sbin/lltconfig -U
   # /opt/VRTSamf/bin/amfconfig -U

3  Determine the GAB kernel module ID:

   # modinfo | grep gab

   The module ID is in the left-hand column of the output.
4  Unload the GAB module from the kernel:
   # modunload -i gab_id

5  Determine the LLT kernel module ID:
   # modinfo | grep llt

   The module ID is in the left-hand column of the output.

6  Unload the LLT module from the kernel:
   # modunload -i llt_id

7  Determine the AMF kernel module ID:
   # modinfo | grep amf

8  Unload the AMF module from the kernel:
   # modunload -i amf_id
Remove the VCS 6.0 packages in the following order:

```bash
# pkgrm VRTSvbs
# pkgrm VRTSsfmh
# pkgrm VRTSvcsea
# pkgrm VRTSat (if it exists)
# pkgrm VRTSvcsdr
# pkgrm VRTSvcsag
# pkgrm VRTScps
# pkgrm VRTSvcs
# pkgrm VRTSat
# pkgrm VRTSvxfen
# pkgrm VRTSgab
# pkgrm VRTSllt
# pkgrm VRTSspt
# pkgrm VRTSsfcpi60
# pkgrm VRTSperl
# pkgrm VRTSvlic
```

**Note:** The VRTScps package should be removed after manually removing the CP server fencing configuration. See “Manually remove the CP server fencing configuration” on page 372.

Remove the following language packages:

- Remove the Chinese language support packages.

  ```bash
  # pkgrm VRTSzhvm
  # pkgrm VRTSmulic
  ```

- Remove the Japanese language support packages.

  ```bash
  # pkgrm VRTSjavm
  # pkgrm VRTSjaodm
  # pkgrm VRTSjafs
  # pkgrm VRTSjadbe
  # pkgrm VRTSjadba
  # pkgrm VRTSjacsc
  # pkgrm VRTSjacse
  # pkgrm VRTSjacav
  # pkgrm VRTSmulic
  ```
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 mycps1 -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-197f8305fff0}</td>
<td>node0(0)</td>
<td>1</td>
</tr>
</tbody>
</table>

2. List the CP server users:

   # cpsadm -s mycps1 -a list_users

<table>
<thead>
<tr>
<th>Username/Domain Type</th>
<th>Cluster Name/UUID</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpsclient@hostname/vx</td>
<td>cluster1/{3719a60a-1dd2-11b2-b8dc-197f8305fff0}</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 mycps1 -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 mycps1 -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 mycps1 -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 mycps1 -a rm_node -c cluster1 -n 0
   Node 0 (node0) successfully deleted
7  Remove the cluster.

    # cpsadm -s mycps1 -a rm_clus -c cluster1
    Cluster cluster1 deleted successfully

8  Verify that the cluster details are removed successfully.

    # cpsadm -s mycps1 -a list_nodes

    ClusterName          UUID          Hostname(Node ID)   Registered
    ==============    ===============   ================    ===========

    # cpsadm -s mycps1 -a list_users

    Username/Domain Type Cluster Name/UUID     Role
    ===============    ===============     =========
Adding and removing nodes

- Chapter 32. Adding a node to a single-node cluster
- Chapter 33. Adding and removing cluster nodes
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 32-1 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 378.</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 379.</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 380.</td>
</tr>
</tbody>
</table>
### Table 32-1  
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 “Bringing up the existing node” on page 380.</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 “Installing the VCS software manually when adding a node to a single node cluster” on page 381.</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 457.</td>
</tr>
<tr>
<td>Start LLT and GAB on Node B.</td>
<td>See “Starting LLT and GAB” on page 381.</td>
</tr>
<tr>
<td>■ Start LLT and GAB on Node A.</td>
<td>See “Reconfiguring VCS on the existing node” on page 381.</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 383.</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 packages and configuration files. See “Removing a node from a cluster” on page 401.

   ■ If the node you plan to add as Node B is also currently a single VCS node, uninstall VCS.

   ■ 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 379.

**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:

   # sync; sync; init 0

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 64.

Bringing up the existing node

Bring up the node.

To bring up the node

1 Start the operating system. On a SPARC node (Node A) enter the command:

   ok boot -r

2 Log in as superuser.

3 Make the VCS configuration writable.

   # haconf -makerw

4 Display the service groups currently configured.

   # hagrp -list

5 Freeze the service groups.

   # hagrp -freeze group -persistent

   Repeat this command for each service group in step 4.

6 Make the configuration read-only.

   # haconf -dump -makero

7 Stop VCS on Node A.

   # hastop -local -force

8 If you have configured I/O Fencing, GAB, and LLT on the node, stop them.

   # /usr/sbin/svcadm disable -t gab

   # /usr/sbin/svcadm disable -t llt
Installing the VCS software manually when adding a node to a single node cluster

Install the VCS 6.0 packages manually and install the license key.

Refer to the following sections:
- See “Preparing for a manual installation” on page 207.
- See “Adding a license key for a manual installation” on page 213.

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 224.
2. Create the file /etc/llthosts that list both the nodes.
   See “Setting up /etc/llthosts for a manual installation” on page 224.
3. Create the file /etc/gabtab.
   See “Configuring GAB manually” on page 227.

Starting LLT and GAB

On the new node, start LLT and GAB.

To start LLT and GAB
1. Start LLT on Node B.
   ■ On Solaris 10:
     ```bash
     # /usr/sbin/svcadm enable llt
     ```
2. Start GAB on Node B
   ■ On Solaris 10:
     ```bash
     # /usr/sbin/svcadm enable gab
     ```

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.
   - Solaris 10:
     ```
     # /usr/sbin/svcadm enable llt
     ```

3. Start GAB on Node A.
   - Solaris 10:
     ```
     # /usr/sbin/svcadm enable gab
     ```

4. Check the membership of the cluster.
   ```
   # gabconfig -a
   ```

5. Copy the cluster UUID from the existing node 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.

6. Start VCS on Node A.
   ```
   # hastart
   ```
   To start VCS using SMF service, use the following command:
   ```
   # svcadm enable vcs
   ```

7. Make the VCS configuration writable.
   ```
   # 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.
  
  ```bash
  # hagrp -list
  ```

- For each service group that is listed, add the node.
  
  ```bash
  # 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.
  
  ```bash
  # gabconfig -a
  ```

2. Start the VCS on Node B.
  
  ```bash
  # hastart
  ```

3. Verify that VCS is up on both nodes.
  
  ```bash
  # hastatus
  ```

4. List the service groups.
  
  ```bash
  # hagrp -list
  ```

5. Unfreeze the service groups.
  
  ```bash
  # hagrp -unfreeze group -persistent
  ```

6. Implement the new two-node configuration.
  
  ```bash
  # haconf -dump -makero
  ```
Adding a node to a single-node cluster

Adding a node to a single-node cluster
Adding and removing cluster nodes

This chapter includes the following topics:

■ About adding and removing nodes
■ Adding nodes using the VCS installer
■ Adding a node using the Web-based installer
■ Manually adding a node to a cluster
■ Removing a node from a cluster

About adding and removing nodes

After you install VCS and create a cluster, you can add and remove nodes from the cluster. You can create a cluster of up to 64 nodes.

See “Important preinstallation information for VCS” on page 35.

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 packages installed on the new node.
■ Discovers the network interfaces on the new node and checks the interface settings.
■ Creates the following files on the new node:
Updates the following configuration files and copies them on the new node:
/etc/llthosts
/etc/gabtab
/etc/VRTSvcs/conf/config/main.cf

Copies the following files from the existing cluster to the new node:
/etc/vxfenmode
/etc/vxfendg
/etc/vx/.uuids/clusuuid
/etc/default/llt
/etc/default/gab
/etc/default/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 -addnode
```

The installer displays the copyright message and the location where it stores the temporary installation logs.

3. Enter the name of a node in the existing 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 packages on the nodes and discovers the network interfaces.

6 Enter the name of the network interface that you want to configure as the first private heartbeat link.

**Note:** The 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 116.

Enter the NIC for the first private heartbeat link on **saturn**: [b,q,?] **qfe:0**

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,?] **qfe:1**

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: qfe:2

Adding a node using the Web-based installer

You can use the Web-based installer to add a node to a cluster.

To add a node to a cluster using the Web-based installer

1 From the Task pull-down menu, select Add a Cluster node. From the product pull-down menu, select the product. Click the Next button.

2 Click OK to confirm the prerequisites to add a node.

3 In the System Names field enter a name of a node in the cluster where you plan to add the node and click OK. The installer program checks inter-system communications and compatibility. If the node fails any of the checks, review the error and fix the issue. If prompted, review the cluster's name, ID, and its systems. Click the Yes button to proceed.

4 In the System Names field, enter the names of the systems that you want to add to the cluster as nodes. Separate system names with spaces. Click the Next button. The installer program checks inter-system communications and compatibility. If the system fails any of the checks, review the error and fix the issue. Click the Next button. If prompted, click the Yes button to add the system and to proceed.

5 From the heartbeat NIC pull-down menus, select the heartbeat NICs for the cluster. Click the Next button.

6 Once the addition is complete, review the log files. Optionally send installation information to Symantec. Click the Finish button to complete the node's addition to the cluster.
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 36.

Table 33-1 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 33-1  Tasks that are involved in adding a node to a cluster

<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 389.</td>
</tr>
<tr>
<td>Install the software manually.</td>
<td>See “Preparing for a manual installation” on page 207.</td>
</tr>
<tr>
<td></td>
<td>See “Installing VCS packages for a manual installation” on page 211.</td>
</tr>
<tr>
<td>Add a license key.</td>
<td>See “Adding a license key for a manual installation” on page 213.</td>
</tr>
<tr>
<td>Configure LLT and GAB.</td>
<td>See “Configuring LLT and GAB when adding a node to the cluster” on page 394.</td>
</tr>
<tr>
<td>Copy the UUID.</td>
<td>See “Reconfiguring VCS on the existing node” on page 381.</td>
</tr>
<tr>
<td>If the existing cluster is configured for I/O fencing, configure I/O fencing on the new node.</td>
<td>See “Configuring I/O fencing on the new node” on page 397.</td>
</tr>
<tr>
<td>Add the node to the existing cluster.</td>
<td>See “Adding the node to the existing cluster” on page 400.</td>
</tr>
<tr>
<td>Start VCS and verify the cluster.</td>
<td>See “Starting VCS and verifying the cluster” on page 401.</td>
</tr>
</tbody>
</table>

Setting up the hardware

Figure 33-1 shows that before you configure a new system on an existing cluster, you must physically add the system to the cluster.
Manually adding a node to a cluster

Figure 33-1  Adding a node to a two-node cluster using two switches

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 33-1 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 packages manually and add a license key.
For more information, see the following:
■ See “Installing VCS software manually” on page 209.
■ See “Adding a license key for a manual installation” on page 213.

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 394.

Table 33-2 uses the following information for the following command examples.

<table>
<thead>
<tr>
<th>Name</th>
<th>Fully-qualified host name (FQHN)</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>saturn</td>
<td>saturn.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 saturn

To configure the authentication broker on node saturn

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:

```bash
# cd /tmp/VxAT/version/bin/edition_number; \
./broker_setup.sh/tmp/eat_setup

/opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssregctl -s -f
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER/root/.VRTSat/profile \
/VRTSatlocal.conf -b 'Security\Authentication \\Authentication Broker' -k UpdatedDebugLogFileName \ 
-v /var/VRTSvcs/log/vcsauthserver.log -t string
```

4 Copy the broker credentials from one node in the cluster to saturn by copying the entire `bkup` directory.
The `bkup` directory content resembles the following example:

```bash
# cd /var/VRTSvcs/vcsauth/bkup/

# ls

CMDSERVER CPSADM CPSERVER HAD VCS_SERVICES WAC
```

5 Import the VCS_SERVICES domain.

```bash
# /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.

```bash
# /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 saturn.

```bash
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh
```
Perform the following tasks:

```bash
# 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:

```bash
# 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 `nebula`:
   - If the file on one of the existing nodes resembles:
     ```
     0 galaxy
     1 nebula
     ```
   - Update the file for all nodes, including the new one, resembling:
     ```
     0 galaxy
     1 nebula
     2 saturn
     ```

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:
   - For Solaris SPARC:
set-node saturn
set-cluster 2
link qfe0 qfe:0 - ether - -
link qfe1 qfe:1 - ether - -

For Solaris x64:

set-node saturn
set-cluster 2
link e1000g0 e1000g:0 - ether - -
link e1000g1 e1000g:1 - ether - -

3 Copy the following file from one of the nodes in the existing cluster to the
new node:
/etc/default/llt

4 On the new system, run the command:
# /sbin/lltconfig -c

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 -nN option, where N is the total number of cluster nodes.

■ If the /etc/gabtab file on the existing nodes resembles:
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/default/gab

3 On the new node, to configure GAB run the command:

`#/sbin/gabconfig -c`

**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 349.

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 397.

- 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 398.
  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 399.

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 400.

Preparin g 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:

   # 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 mycps1.symantecexample.com \\
   -a add_node -c clus1 -h saturn -n2
   ```

   Node 2 (saturn) successfully added

3. Verify that the new node is added to the CP server configuration:

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

   The new node must be listed in the command output.

4. Add the VCS user cpsclient@saturn to each CP server:

   ```
   # cpsadm -s mycps1.symantecexample.com \\
   -a add_user -e cpsclient@saturn \ 
   -f cps_operator -g vx
   ```

   User cpsclient@saturn successfully added
To configure server-based fencing with security on the new node

1. Log in to each CP server as the root user.

2. Update each CP server configuration with the new node information:
   
   ```
   # cpsadm -s mycps1.symantecexample.com -a add_node -c clus1 -h saturn -n2
   
   Node 2 (saturn) successfully added
   ```

3. Verify that the new node is added to the CP server configuration:

   ```
   # cpsadm -s mycps1.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 saturn to the existing vxfen group.
   
   ```
   # hagrp -modify vxfen SystemList -add saturn 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 and removing cluster nodes

Manually adding a node to a cluster

- /etc/vxfenmode
- /etc/vxfendg—This file is required only for disk-based fencing.
- /etc/default/vxfen

2  Start I/O fencing on the new node.
   # svcadm enable vxfen

3  Run the GAB configuration command on the new node to verify that the port b membership is formed.
   # gabconfig -a

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/default/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/
6  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/

7  If necessary, modify any new system attributes.
8  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

   To start VCS service using SMF, use the following command:

   # svcadm enable vcs

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 cluster

Table 33-3 specifies the tasks that are involved in removing a node from a cluster.
In the example procedure, the cluster consists of nodes galaxy, nebula, and saturn; node saturn is to leave the cluster.
Table 33-3  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 402.</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 403.</td>
</tr>
<tr>
<td>■ Delete the node from VCS configuration.</td>
<td></td>
</tr>
<tr>
<td>Modify the llthosts(4) and gabtab(4) files to reflect the change.</td>
<td>See “Modifying configuration files on each remaining node” on page 406.</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 407.</td>
</tr>
<tr>
<td>For a cluster that is running in a secure mode, remove the security credentials from the leaving node.</td>
<td>See “Removing security credentials from the leaving node” on page 408.</td>
</tr>
<tr>
<td>On the node departing the cluster:</td>
<td>See “Unloading LLT and GAB and removing VCS on the departing node” on page 408.</td>
</tr>
<tr>
<td>■ Modify startup scripts for LLT, GAB, and VCS to allow reboot of the node without affecting the cluster.</td>
<td></td>
</tr>
<tr>
<td>■ Unconfigure and unload the LLT and GAB utilities.</td>
<td></td>
</tr>
<tr>
<td>■ Remove the VCS packages.</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 galaxy or node nebula 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  galaxy   RUNNING  0
   A  nebula   RUNNING  0
   A  saturn   RUNNING  0
   
   -- GROUP STATE
   -- Group  System  Probed  AutoDisabled  State
   B  grp1    galaxy  Y      N      ONLINE
   B  grp1    nebula  Y      N      OFFLINE
   B  grp2    galaxy  Y      N      ONLINE
   B  grp3    nebula  Y      N      OFFLINE
   B  grp3    saturn  Y      N      ONLINE
   B  grp4    saturn  Y      N      ONLINE
   ```

The example output from the `hastatus` command shows that nodes galaxy, nebula, and saturn are the nodes in the cluster. Also, service group grp3 is configured to run on node nebula and node saturn, the departing node. Service group grp4 runs only on node saturn. Service groups grp1 and grp2 do not run on node saturn.

Deleting the departing node from 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 saturn to node nebula.

   # hagrp -switch grp3 -to nebula

2. Check for any dependencies involving any service groups that run on the departing node; for example, grp4 runs only on the departing node.

   # 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 saturn

   To stop VCS using SMF, run the following command:

   # svcadm disable vcs
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.

```bash
# hastatus -summary

-- SYSTEM STATE

-- System State Frozen
A  galaxy  RUNNING  0
A  nebula  RUNNING  0
A  saturn  EXITED  0

-- GROUP STATE

-- Group System Probed AutoDisabled State
B  grp1  galaxy  Y  N  ONLINE
B  grp1  nebula  Y  N  OFFLINE
B  grp2  galaxy  Y  N  ONLINE
B  grp3  nebula  Y  N  ONLINE
B  grp3  saturn  Y  Y  OFFLINE
B  grp4  saturn  Y  N  OFFLINE
```

6  Delete the departing node from the SystemList of service groups grp3 and grp4.

```bash
# hagrp -modify grp3 SystemList -delete saturn
# hagrp -modify grp4 SystemList -delete saturn
```

7  For the service groups that run only on the departing node, delete the resources from the group before you delete the group.

```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.

    # hastatus -summary
    -- SYSTEM STATE
    -- System  State  Frozen
    A  galaxy  RUNNING  0
    A   nebula  RUNNING  0
    A   saturn  EXITED  0

    -- GROUP STATE
    -- Group  System  Probed  AutoDisabled  State
    B   grp1  galaxy  Y  N  ONLINE
    B   grp1  nebula  Y  N  OFFLINE
    B   grp2  galaxy  Y  N  ONLINE
    B   grp3  nebula  Y  N  ONLINE

10  Delete the node from the cluster.

    # hasys -delete saturn

11  Save the configuration, making it read only.

    # haconf -dump -makero

Modifying configuration files on each remaining node

Perform the following tasks on each of the remaining nodes of the cluster.
To modify the configuration files on a remaining node

1. If necessary, modify the `/etc/gabtab` file.

   No change is required to this file if the `/sbin/gabconfig` command has only the argument `-c`. Symantec recommends using the `-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 galaxy
   1 nebula
   2 saturn
   ```

   To:

   ```
   0 galaxy
   1 nebula
   ```

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:

   ```
   # cpsadm -s cp_server -a list_users
   ```

   Where `cp_server` is the virtual IP/ virtual hostname of the CP server.
3  Remove the VCS user associated with the node you previously removed from
the cluster.

For CP server in non-secure mode:

```
# cpsadm -s cp_server -a rm_user \
-e cpsclient@saturn -f cps_operator -g vx
```

4  Remove the node entry from the CP server:

```
# cpsadm -s cp_server -a rm_node -h saturn -c clus1 -n 2
```

5  View the list of nodes on the CP server to ensure that the node entry was
removed:

```
# cpsadm -s cp_server -a list_nodes
```

Removing security credentials from the leaving node

If the leaving node is part of a cluster that is running in a secure mode, you must
remove the security credentials from node saturn. Perform the following steps.

To remove the security credentials

1  Stop the AT process.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh \ 
stop
```

2  Remove the credentials.

```
# rm -rf /var/VRTSvcs/vauth/data/
```

Unloading LLT and GAB and removing VCS on the departing node

Perform the tasks on the node that is departing the cluster.

If you have configured VCS as part of the Storage Foundation and High Availability
products, you may have to delete other dependent packages before you can delete
all of the following ones.
To unconfigure and unload LLT and GAB and remove VCS

1. If you had configured I/O fencing in enabled mode, then stop I/O fencing.
   
   ```bash
   # svcadm disable -t vxfen
   ```

2. Unconfigure GAB and LLT:
   
   ```bash
   # /sbin/gabconfig -U
   # /sbin/lltconfig -U
   ```

3. Unload the GAB and LLT modules from the kernel.
   ■ Determine the kernel module IDs:
   
   ```bash
   # modinfo | grep gab
   # modinfo | grep llt
   ```
   
   The module IDs are in the left-hand column of the output.
   ■ Unload the module from the kernel:
   
   ```bash
   # modunload -i gab_id
   # modunload -i llt_id
   ```

4. Disable the startup files to prevent LLT, GAB, or VCS from starting up:
   
   ```bash
   # /usr/sbin/svcadm disable -t llt
   # /usr/sbin/svcadm disable -t gab
   # /usr/sbin/svcadm disable -t vcs
   ```

5. To determine the packages to remove, enter:
   
   ```bash
   # pkginfo | grep VRTS
   ```
To permanently remove the VCS packages from the system, use the `pkgrm` command. Start by removing the following packages, which may have been optionally installed, in the order shown:

```
# pkgrm VRTSvcsea
# pkgrm VRTSat
# pkgrm VRTSvcsag
# pkgrm VRTScps
# pkgrm VRTSvcs
# pkgrm VRTSamf
# pkgrm VRTSvxfen
# pkgrm VRTSgab
# pkgrm VRTSl1t
# pkgrm VRTSspt
# rpm -e VRTSsfcpi60
# pkgrm VRTSperl
# pkgrm VRTSvlic
```

Remove the LLT and GAB configuration files.

```
# rm /etc/l1ttab
# rm /etc/gabtab
# rm /etc/l1thosts
```

Remove the language packages and patches.

See “Removing VCS packages manually” on page 369.
Installation reference

- Appendix A. VCS installation packages
- Appendix B. Installation command options
- Appendix C. Changes to bundled agents in VCS 6.0
- Appendix D. Configuration files
- Appendix E. Installing VCS on a single node
- Appendix F. Configuring LLT over UDP
- Appendix G. Configuring the secure shell or the remote shell for communications
- Appendix H. Troubleshooting VCS installation
- Appendix I. Sample VCS cluster setup diagrams for CP server-based I/O fencing
- Appendix J. Reconciling major/minor numbers for NFS shared disks
- Appendix K. Compatibility issues when installing Veritas Cluster Server with other products
VCS installation packages

This appendix includes the following topics:

- Veritas Cluster Server installation packages

### Veritas Cluster Server installation packages

Table A-1 shows the package name and contents for each Veritas Cluster Server package.

<table>
<thead>
<tr>
<th>Package</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>Package</td>
<td>Contents</td>
<td>Required/Optional</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>VRTSsfcpi60</td>
<td>Veritas Storage Foundation Common Product Installer</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>The Storage Foundation Common Product installer package contains the scripts that perform the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ upgrade</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ uninstallation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ adding nodes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ removing nodes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can use this script to simplify the native operating system installations, configurations, and upgrades.</td>
<td></td>
</tr>
<tr>
<td>VRTSspt</td>
<td>Contains the binaries for Veritas Software Support Tools.</td>
<td>Recommended package, optional</td>
</tr>
<tr>
<td>VRTSvcs</td>
<td>VRTSvcs contains the following components:</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>■ Contains the binaries for Veritas Cluster Server.</td>
<td>Depends on VRTSperl and VRTSvlic.</td>
</tr>
<tr>
<td></td>
<td>■ Contains the binaries for Veritas Cluster Server manual pages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Contains the binaries for Veritas Cluster Server English message catalogs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Contains the binaries for Veritas Cluster Server utilities.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>These utilities include security services.</td>
<td></td>
</tr>
<tr>
<td>VRTSvcsag</td>
<td>Contains the binaries for Veritas Cluster Server bundled agents.</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Depends on VRTSvcs.</td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Contents</td>
<td>Required/Optional</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VRTSvcsea</td>
<td>VRTSvcsea 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. 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must download the database separately at:</td>
<td></td>
</tr>
<tr>
<td>VRTSvbs</td>
<td>Enables the VBS command line interface on a Veritas Operations Manager managed host in a Virtual Business Service configuration.</td>
<td>Recommended Depends on VRTSsfmh. VRTSsfmh version must be 4.1 or later for VRTSvbs to get installed.</td>
</tr>
<tr>
<td>VRTSvcsnr</td>
<td>Network reconfiguration service for Oracle VM Server logical domains</td>
<td>Optional You must install VRTSvcsnr manually inside a Oracle VM Server logical domain if the domain is to be configured for disaster recovery.</td>
</tr>
</tbody>
</table>

*Table A-2* shows the package name, contents, and type for each Veritas Cluster Server language package.
### Table A-2  Veritas Cluster Server language packages

<table>
<thead>
<tr>
<th>Package</th>
<th>Contents</th>
<th>Package type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRTSmulic</td>
<td>Contains the multi-language Symantec license utilities.</td>
<td>Common L10N package</td>
</tr>
<tr>
<td>VRTSatJA</td>
<td></td>
<td>Japanese language package</td>
</tr>
<tr>
<td>VRTSjacsc</td>
<td>Contains the binaries for Veritas Cluster Server Japanese Message Catalogs by Symantec.</td>
<td>Japanese language package</td>
</tr>
<tr>
<td>VRTSjacsu</td>
<td>Contains the binaries for Japanese Veritas Cluster Utility Language Pack by Symantec.</td>
<td>Japanese language package</td>
</tr>
<tr>
<td>VRTSjadba</td>
<td>Contains the binaries for Japanese RAC support package by Symantec.</td>
<td>Japanese language package</td>
</tr>
<tr>
<td>VRTSjadbe</td>
<td>Contains the Japanese Storage Management Software for Databases - Message Catalog.</td>
<td>Japanese language package</td>
</tr>
<tr>
<td>VRTSjaodm</td>
<td>Contains the binaries for Japanese Message Catalog and Man Pages for ODM.</td>
<td>Japanese language package</td>
</tr>
</tbody>
</table>
Table A-2  Veritas Cluster Server language packages (continued)

<table>
<thead>
<tr>
<th>Package</th>
<th>Contents</th>
<th>Package type</th>
</tr>
</thead>
</table>
VCS installation packages

Veritas Cluster Server installation packages
Installation command options

This appendix includes the following topics:

- Command options for installvcs program
- Command options for uninstallvcs program

Command options for installvcs program

The `installvcs` command usage takes the following form:

```
installvcs [ system1 system2... ]
  [ -install | -configure | -uninstall | -license
    | -upgrade | -precheck | -requirements | -start | -stop
    | -postcheck ]
  [ -responsefile response_file ]
  [ -logpath log_path ]
  [ -tmppath tmp_path ]
  [ -tunablesfile tunables_file ]
  [ -timeout timeout_value ]
  [ -keyfile ssh_key_file ]
  [ -hostfile hostfile_path ]
  [ -pkgpath pkg_path ]
  [ -rootpath root_path ]
  [ -jumpstart jumpstart_path ]
  [ -flash_archive flash_archive_path ]
  [ -serial | -rsh | -redirect | -installminpkgs
    | -installrecpkgs | -installallpkgs | -minpkgs
    | -recpkgs | -allpkgs | -pkgset | -pkgtable | -pkginfo
    | -makeresponsefile | -comcleanup | -version | -nolic
```
<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-addnode</td>
<td>Add the nodes that you specify to a cluster. The cluster must be online to use this command option to add nodes.</td>
</tr>
<tr>
<td>-allpkgs</td>
<td>View a list of all VCS packages. The installvcs program lists the packages in the correct installation order. You can use the output to create scripts for command-line installation, or for installations over a network. See the -minpkgs and the -recpkgs options.</td>
</tr>
<tr>
<td>-comcleanup</td>
<td>Remove the ssh or ssh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated.</td>
</tr>
<tr>
<td>-configure</td>
<td>Configure VCS after using <code>--install</code> option to install VCS.</td>
</tr>
</tbody>
</table>
Table B-1  installvcs and uninstallvcs options (continued)

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| -copyinstallscripts | Use this option when you manually install products and want to use the installation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the -rootpath option. The following examples demonstrate the usage for this option:  
  ■ . /installer -copyinstallscripts  
  Copies the installation and uninstallation scripts for all products in the release to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/release_name .  
  ■ . /installproduct_name -copyinstallscripts  
  Copies the installation and uninstallation scripts for the specified product and any subset products for the product to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/release_name .  
  ■ . /installer-rootpath alt_root_path -copyinstallscripts  
  The path alt_root_path can be a directory like /rdisk2. In that case, this command copies installation and uninstallation scripts for all the products in the release to /rdisk2/opt/VRTS/install. CPI perl libraries are copied at /rdisk2/opt/VRTSperl/lib/site_perl/release_name. For example, for the 6.0 release, the release_name is UXRT60. |
| -fencing | Configure I/O fencing after you configure VCS. The script provides an option to configure disk-based I/O fencing or server-based I/O fencing. |
| -flash_archive | Generate Flash archive scripts which can be used by Solaris Jumpstart Server for automated Flash archive installation of all packages and patches for every product, an available location to store the post deployment scripts should be specified as a complete path. |
| -hostfile | Specify the location of a file that contains the system names for the installer. |
| -install | Install product packages on systems without configuring VCS. |
| -installallpkgs | Select all the packages for installation. See the -allpkgs option. |
Table B-1  installvcs and uninstallvcs options (continued)

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| `installminpkgs`  | Select the minimum packages for installation.  
                  See the `-minpkgs` option. |
| `installrecpkgs`  | Select the recommended packages for installation.  
                  See the `-recpkgs` option. |
| `-jumpstart dir_path` | Use this option to generate the finish scripts that the Solaris  
                          JumpStart Server can use for Veritas products. The `dir_path` indicates  
                          the path to an existing directory where the installer must store the  
                          finish scripts. |
| `-keyfile ssh_key_file` | Specify a key file for SSH. The option passes `-i ssh_key_file` with  
                                       each SSH invocation. |
| `-license`        | Register or update product licenses on the specified systems. This  
                  option is useful to replace a demo license. |
| `-logpath log_path` | Specify that `log_path`, not `/opt/VRTS/install/logs`, is the location  
                  where installvcs log files, summary file, and response file are saved. |
| `-makeresponsefile` | Generate a response file. No actual software installation occurs when  
                      you use this option.  
                      Create a response file or to verify that your system configuration is  
                      ready for uninstalling VCS. |
| `-minpkgs`        | View a list of the minimal packages for VCS. The installvcs program  
                  lists the packages in the correct installation order. The list does not  
                  include the optional packages.  
                  You can use the output to create scripts for command-line installation,  
                  or for installations over a network.  
                  See the `-allpkgs` and the `-recpkgs` options. |
| `-nolic`          | Install product packages on systems without licensing or  
                  configuration. License-based features or variants are not installed  
                  when you use this option. |
<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-pkginfo</td>
<td>Display a list of packages in the order of installation in a user-friendly format. Use this option with one of the following options: ■ -allpkgs ■ -minpkgs ■ -recpks If you do not specify an option, all three lists of packages are displayed.</td>
</tr>
<tr>
<td>-pkgpath pkg_path</td>
<td>Specify that <em>pkg_path</em> contains all packages that the installvcs program is about to install on all systems. The <em>pkg_path</em> is the complete path of a directory, usually NFS mounted.</td>
</tr>
<tr>
<td>-pkgset</td>
<td>Discover and lists the 6.0 packages installed on the systems that you specify.</td>
</tr>
<tr>
<td>-pkgtable</td>
<td>Display the VCS 6.0 packages in the correct installation order.</td>
</tr>
<tr>
<td>-postcheck</td>
<td>Check 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>-precheck</td>
<td>Verify that systems meet the installation requirements before proceeding with VCS installation. Symantec recommends doing a precheck before you install VCS. See “Performing automated preinstallation check” on page 72.</td>
</tr>
<tr>
<td>-recpks</td>
<td>View a list of the recommended packages for VCS. The installvcs program lists the packages in the correct installation order. The list does not include the optional packages. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -minpkgs options.</td>
</tr>
<tr>
<td>-requirements</td>
<td>View a list of required operating system version, required patches, file system space, and other system requirements to install VCS.</td>
</tr>
</tbody>
</table>
Table B-1: installvcs and uninstallvcs options (continued)

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-responsefile</code></td>
<td>Perform automated VCS installation using the system and the configuration information that is stored in a specified file instead of prompting for information. The response file must be specified with the <code>-responsefile</code> option. If not specified, the response file is automatically generated as <code>installernumber.response</code> where <code>number</code> is random. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. See “Installing VCS using response files” on page 179. See “Configuring VCS using response files” on page 185. See “Upgrading VCS using response files” on page 291.</td>
</tr>
<tr>
<td><code>-rootpath</code></td>
<td>Specify that <code>root_path</code> is the root location for the installation of all packages. On Solaris, <code>-rootpath</code> passes <code>-R root_path</code> to <code>pkgadd</code> command.</td>
</tr>
<tr>
<td><code>-redirect</code></td>
<td>Specify that the installer need not display the progress bar details during the installation.</td>
</tr>
<tr>
<td><code>-rsh</code></td>
<td>Specify that <code>rsh</code> and <code>rcp</code> are to be used for communication between systems instead of <code>ssh</code> and <code>scp</code>. This option requires that systems be preconfigured such that <code>rsh</code> commands between systems execute without prompting for passwords or confirmations.</td>
</tr>
<tr>
<td><code>-security</code></td>
<td>Enable or disable secure mode in a VCS cluster. See the Veritas Cluster Server Administrator’s Guide for instructions.</td>
</tr>
<tr>
<td><code>-securityonenode</code></td>
<td>Form a secure cluster node by node in environments that do not support passwordless <code>ssh</code> or passwordless <code>rsh</code>. See “Configuring a secure cluster node by node” on page 123.</td>
</tr>
<tr>
<td><code>-securitytrust</code></td>
<td>Set up a trust relationship between your VCS cluster and a broker. See “Setting up trust relationships for your VCS cluster” on page 122.</td>
</tr>
<tr>
<td><code>-serial</code></td>
<td>Perform the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems.</td>
</tr>
</tbody>
</table>
### Table B-1  
installvcs and uninstallvcs options (continued)

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-start`          | Start the daemons and processes for VCS.  
If the installvcs program failed to start up all the VCS processes, you can use the `-stop` option to stop all the processes and then use the `-start` option to start the processes.  
See the `-stop` option.  
See “Starting and stopping processes for the Veritas products ” on page 500. |
| `-stop`           | Stop the daemons and processes for VCS.  
If the installvcs program failed to start up all the VCS processes, you can use the `-stop` option to stop all the processes and then use the `-start` option to start the processes.  
See the `-start` option.  
See “Starting and stopping processes for the Veritas products ” on page 500. |
| `-timeout`        | Specifies the timeout value (in seconds) for each command that the installer issues during the installation. The default timeout value is set to 600 seconds. |
| `-tmp_path`       | Specify that `tmp_path` is the working directory for installvcs program. This path is different from the `/var/tmp` path. This destination is where the installvcs program performs the initial logging and where the installvcs program copies the packages on remote systems before installation. |
| `-uninstall`      | Uninstall VCS from the systems that you specify. |
| `-upgrade`        | Upgrade the installed packages on the systems that you specify. |
| `-rollingupgrade_phase1` | Upgrade the product kernel packages to the latest version during rolling upgrade Phase 1. |
| `-rollingupgrade_phase2` | Upgrade the VCS and other agent packages to the latest version during rolling upgrade Phase 2. Product kernel drivers are rolling-upgraded to the latest protocol version. |
Table B-1  installvcs and uninstallvcs options (continued)

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-version</td>
<td>Check and display the installed product and version. Identify the installed and missing packages for the product. Provide a summary that includes the count of the installed and any missing packages. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.</td>
</tr>
<tr>
<td>-settunables</td>
<td>Set tunable parameters after a product is installed and configured. Processes of the installed product may need to be restarted for the tunable parameter values to take effect. This option must be used together with -tunablesfile option.</td>
</tr>
<tr>
<td>-tunablesfile</td>
<td>Specify a tunables file including tunable parameters to be set.</td>
</tr>
<tr>
<td>-upgrade_kernelpkgs</td>
<td>Has been renamed to -rollingupgrade_phase1</td>
</tr>
<tr>
<td>-upgrade_nonkernelpkgs</td>
<td>Has been renamed to -rollingupgrade_phase2</td>
</tr>
</tbody>
</table>

Command options for uninstallvcs program

The uninstallvcs command usage takes the following form:

```
uninstallvcs [ system1 system2... ]
[ -uninstall ]
[ -responsefile response_file ]
[ -logpath log_path ]
[ -tmppath tmp_path ]
[ -tunablesfile tunables_file ]
[ -timeout timeout_value ]
[ -keyfile ssh_key_file ]
[ -hostfile hostfile_path ]
[ -pkgpath pkg_path ]
[ -rootpath root_path ]
[ -jumpstart jumpstart_path ]
[ -flash_archive flash_archive_path ]
[ -serial | -rsh | -redirect | -makeresponsefile
 | -comcleanup | -version | -nolic | -ignorepatchreqs
 | -settunables | -security | -securityonenode
 | -securitytrust | -addnode | -fencing | -upgrade_kernelpkgs
 | -upgrade_nonkernelpkgs | -rolling_upgrade
```
For description of the `uninstallvcs` command options:

See Table B-1 on page 420.
Command options for\nuninstallvcs program
Changes to bundled agents in VCS 6.0

This appendix includes the following topics:

- Deprecated agents
- New agents
- New and modified attributes for VCS 6.0 agents
- Manually removing deprecated resource types and modifying attributes
- Creating new VCS accounts if you used native operating system accounts

Deprecation agents

The following agents are no longer supported:

- CampusCluster
- CFSQlogckd
- ClusterMonitorConfig
- DiskReservation
- NFSLock
- Service group heartbeat (ServiceGroupHB)
- SANVolume
- VRTSWebApp

**Note:** No agents were deprecated since the 5.1 SP1 release.
New agents

The following new agent is added in the 6.0 release:

- **AlternateIO**—Monitors VCS storage and network service groups that in turn monitor redundant I/O services exported from the control domain and alternate I/O domain to a guest logical domain.

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.
- **Disk**—Monitors a physical disk or a partition.
- **Project**—Adds, deletes, and monitors Solaris projects.

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.
- **LDom**—Monitors and manages logical domains on Solaris SPARC.
- **Zpool**—Monitors ZFS storage pools.
- **SambaServer**—Monitors the smbd process.
- **SambaShare**—Use to make a Samba Share highly available or to monitor it.
- **NetBios**—Use to make the nmbd process highly available or to monitor it.

The following agents were added in the 5.0 release:

- **Apache** (now bundled on all platforms)—Provides high availability to an Apache Web server.
- **NFSRestart**—Provides high availability for NFS record locks.
- **ProcessOnOnly**—Starts and monitors a user-specified process.
- **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 VCS 6.0 agents

- Table C-1 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.1 SP1 to VCS 6.0.
Table C-2 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.1 to VCS 5.1 SP1.

Table C-3 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.0 MP3 to VCS 5.1.

Table C-4 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.0 to VCS 5.0 MP3.

Table C-5 lists the attributes that VCS adds or modifies when you upgrade from VCS 4.1 to VCS 5.0.

Table C-1  Changes to attributes from VCS 5.1 SP1 to VCS 6.0

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlternateIO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td>AgentFile</td>
<td>bin/Script51Agent</td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ StorageSG, NetworkSG }</td>
<td></td>
</tr>
<tr>
<td>StorageSG</td>
<td>{}</td>
<td></td>
</tr>
<tr>
<td>NetworkSG</td>
<td>{}</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ State, IState, User, StartProgram, StopProgram, CleanProgram, MonitorProgram, PidFiles, MonitorProcesses, EnvFile, UseSUDash }</td>
<td></td>
</tr>
<tr>
<td>IMF</td>
<td>{ Mode = 3, MonitorFreq = 1, RegisterRetryLimit = 3 }</td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>{ &quot;program.vfd&quot;, &quot;user.vfd&quot;, &quot;cksum.vfd&quot;, getcksum, propcv }</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UseGSSAPI</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Table C-1</td>
<td>Changes to attributes from VCS 5.1 SP1 to VCS 6.0 (continued)</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Agent</strong></td>
<td><strong>New and modified attributes</strong></td>
<td><strong>Default value</strong></td>
</tr>
<tr>
<td>RefreshInterval</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>CleanRRKeys</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td><strong>Modified attribute</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ Domain, TTL, TSIGKeyFile, StealthMasters, ResRecord, CreatePTR, OffDelRR, UseGSSAPI, RefreshInterval, CleanRRKeys }</td>
<td></td>
</tr>
<tr>
<td><strong>DiskGroup</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Modified attributes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PanicSystemOnDGLoss</td>
<td>int PanicSystemOnDGLoss = 0</td>
<td></td>
</tr>
<tr>
<td><strong>ArgList</strong></td>
<td>{ DiskGroup, StartVolumes, StopVolumes, MonitorOnly, MonitorReservation, tempUseFence, PanicSystemOnDGLoss, DiskGroupType, UmountVolumes, Reservation, ConfidenceLevel }</td>
<td></td>
</tr>
<tr>
<td><strong>DiskGroupSnap</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>New attribute</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDTypet</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Modified attribute</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ TargetResName, FDSiteName, FDTypet }</td>
<td></td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Modified attribute</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RegList</td>
<td>{ NetMask }</td>
<td></td>
</tr>
<tr>
<td><strong>IPMultiNIC</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Modified attribute</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ToleranceLimit</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Table C-1  Changes to attributes from VCS 5.1 SP1 to VCS 6.0 (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDom</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>Netmask</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>CEInfo</td>
<td>{ Enabled=0, CESystem=NONE, FaultOnHBLoss=1 }</td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>ConfigureNetwork</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>IPAddress</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>IntentionalOffline</td>
<td>1</td>
</tr>
<tr>
<td>RemoveLDomConfigForMigration</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td><strong>Modified attributes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AEPTimeout</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ArgList</td>
<td>{ State, IState, LDomName, CfgFile, MonitorCPU, NumCPU, ConfigureNetwork, IPAddress, Netmask, Gateway, DNS, Memory, Memory, RemoveLDomConfigForMigration }</td>
</tr>
<tr>
<td></td>
<td>(new attribute added to list)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AgentFile</td>
<td>bin/Script51Agent</td>
</tr>
<tr>
<td></td>
<td>RegList</td>
<td>{ NumCPU, Memory }</td>
</tr>
<tr>
<td></td>
<td>(new attribute added to list)</td>
<td></td>
</tr>
<tr>
<td><strong>Mount</strong></td>
<td><strong>Modified attributes</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AEPTimeout</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>IMF</td>
<td>{ Mode = 3, MonitorFreq = 1, RegisterRetryLimit = 3 }</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>SecondLevelMonitor</td>
<td></td>
<td>{ MountPoint, BlockDevice, FSType, MountOpt, FsckOpt, SnapUmount, CkptUmount, OptCheck, CreateMntPt, MntPtPermission, MntPtOwner, MntPtGroup, AccessPermissionChk, RecursiveMnt, VxFSMountLock }</td>
</tr>
<tr>
<td>SecondLevelTimeout</td>
<td></td>
<td>{ MountPoint, BlockDevice, FSType, MountOpt, FsckOpt, SnapUmount, CkptUmount, OptCheck, CreateMntPt, MntPtPermission, MntPtOwner, MntPtGroup, AccessPermissionChk, RecursiveMnt, VxFSMountLock }</td>
</tr>
<tr>
<td>ArgList</td>
<td>(list updated for deprecated attributes)</td>
<td>{ MountPoint, BlockDevice, FSType, MountOpt, FsckOpt, SnapUmount, CkptUmount, OptCheck, CreateMntPt, MntPtPermission, MntPtOwner, MntPtGroup, AccessPermissionChk, RecursiveMnt, VxFSMountLock }</td>
</tr>
</tbody>
</table>

**Process**

| Modified attribute                |                                                                                             | { Mode = 3, MonitorFreq = 5, RegisterRetryLimit = 3 } |

**RVGPrimary**

| Modified attribute                |                                                                                             | { RvgResourceName, "RvgResourceName:RVG", "RvgResourceName:DiskGroup", AutoTakeover, AutoResync, BunkerSyncTimeOut, BunkerSyncElapsedTime } |

**Zone**

| New attributes                   |                                                                                             | {}                                                                                     |

| DROpts                          |                                                                                             | {}                                                                                     |
| DeleteVCSZoneUser               |                                                                                             | 0                                                                                      |

**Modified attributes**

| IMF                             |                                                                                             | static int IMF = { Mode = 3, MonitorFreq = 5, RegisterRetryLimit = 3 } |
| (attribute data type change)    |                                                                                             | {}                                                                                     |
### Table C-1
Changes to attributes from VCS 5.1 SP1 to VCS 6.0 (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AEPTTimeout</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>IMFRegList</td>
<td></td>
<td>{ BootState }</td>
</tr>
<tr>
<td>ArgList (new attributes added to list)</td>
<td>{ Pool, BootState, ShutdownGracePeriod, RunFsck, DetachZonePath, ForceAttach, DeleteVCSZoneUser, DROpts }</td>
<td></td>
</tr>
</tbody>
</table>

### Zpool

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td>ForceOpt</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>DeviceDir</td>
<td></td>
<td>[]</td>
</tr>
<tr>
<td>FailMode</td>
<td></td>
<td>continue</td>
</tr>
<tr>
<td>ForceRecoverOpt</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList (new attribute added to list)</td>
<td>{ PoolName, AltRootPath, ChkZFSMounts, ZoneResName, &quot;ZoneResName:State&quot;, DeviceDir, FailMode, ForceOpt, ForceRecoverOpt }</td>
<td></td>
</tr>
</tbody>
</table>

### Table C-2
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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td>EnvFile</td>
<td></td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>UseSUDash</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>RegList</td>
<td></td>
<td>{ MonitorProcesses, User }</td>
</tr>
<tr>
<td>IMFRegList</td>
<td></td>
<td>{ MonitorProcesses, User, PidFiles, MonitorProgram }</td>
</tr>
<tr>
<td>Modified attributes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Table C-2**  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>User</td>
<td>(change in default value)</td>
<td>&quot;root&quot;</td>
</tr>
<tr>
<td>ArgList</td>
<td>(new attribute added to list)</td>
<td>{ User, StartProgram, StopProgram, CleanProgram, MonitorProgram, PidFiles, MonitorProcesses, EnvFile, UseSUDash }</td>
</tr>
<tr>
<td>Disk</td>
<td>(new agent)</td>
<td></td>
</tr>
<tr>
<td>New attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partition</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ Partition }</td>
<td></td>
</tr>
<tr>
<td>OfflineMonitorInterval</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>&quot;None&quot;</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>IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ExclusiveIPZone</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Modified 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>ArgList</td>
<td>(new attribute added to list)</td>
<td>{ Device, Address, NetMask, Options, ArpDelay, IfconfigTwice, RouteOptions, PrefixLen, ExclusiveIPZone }</td>
</tr>
<tr>
<td>IPMultiNICB</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Options</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>(new attribute added to list)</td>
<td>{ BaseResName, Address, NetMask, DeviceChoice, RouteOptions, PrefixLen, IgnoreMultiNICBFailure, &quot;BaseResName:Protocol&quot;, Options }</td>
</tr>
<tr>
<td>Mount</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IMFRegList</td>
<td>{ MountPoint, BlockDevice, FSType }</td>
</tr>
<tr>
<td>MultiNICA</td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protocol (change in default value)</td>
<td>&quot;IPv4&quot;</td>
</tr>
<tr>
<td>MultiNICB</td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protocol (change in default value)</td>
<td>&quot;IPv4&quot;</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>
<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>NFS</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td>CleanRmtab</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList (new attribute added to list)</td>
<td>{ UseSMF, Nservers, LockFileTimeout, CleanRmtab }</td>
<td></td>
</tr>
<tr>
<td>NFSRestart</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td>Lower</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList (new attribute added to list)</td>
<td>{ LocksPathName, NFSLockFailover, LockServers, NFSRes, &quot;NFSRes:Nservers&quot;, &quot;NFSRes:LockFileTimeout&quot;, &quot;NFSRes:UseSMF&quot;, Lower, State }</td>
<td></td>
</tr>
<tr>
<td>NIC</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td>ExclusiveIPZone</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ContainerOpts</td>
<td>{ RunInContainer=0, PassCInfo=1 }</td>
<td></td>
</tr>
<tr>
<td>Modified attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>&quot;IPv4&quot;</td>
<td></td>
</tr>
</tbody>
</table>
## Table C-2

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>ArgList</td>
<td>(new attribute added to list)</td>
<td>{ Device, PingOptimize, NetworkHosts, Protocol, NetworkType, ExclusiveIPZone }</td>
</tr>
<tr>
<td>NotifierMngr</td>
<td><em>New attribute</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NotifierSourceIP</td>
<td>&quot;=&quot;</td>
</tr>
<tr>
<td></td>
<td><em>Modified attribute</em></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>(new attribute added to list)</td>
<td>{ EngineListeningPort, MessagesQueue, NotifierListeningPort, NotifierSourceIP, SnmpdTrapPort, SnmpCommunity, SnmpConsoles, SmtpServer, SmtpServerVrfyOff, SmtpServerTimeout, SmtpReturnPath, SmtpFromPath, SmtpRecipients }</td>
</tr>
<tr>
<td>RemoteGroup</td>
<td><em>New attributes</em></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><em>Modified attributes</em></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>ArgList</td>
<td>(new attribute added to list)</td>
<td>{ IpAddress, Port, Username, Password, GroupName, VCSSysName, ControlMode, OfflineWaitTime, DomainType, BrokerIp, ReturnIntOffline }</td>
</tr>
<tr>
<td>RVGPrimary</td>
<td><em>New attributes</em></td>
<td></td>
</tr>
</tbody>
</table>
### Table C-2: 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></td>
<td>BunkerSyncTimeOut</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>BunkerSyncElapsedTime</td>
<td>0</td>
</tr>
<tr>
<td>Modified attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>(new attribute added to list)</td>
<td>{ RvgResourceName, AutoTakeover, AutoResync, BunkerSyncTimeOut, BunkerSyncElapsedTime }</td>
</tr>
<tr>
<td>SupportedActions</td>
<td>(new action added to keylist)</td>
<td>{ fbsync, ElectPrimary }</td>
</tr>
<tr>
<td>RVGSnapshot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VCSResLock</td>
<td></td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>SambaServer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PidFile</td>
<td></td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>SocketAddress</td>
<td></td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>(new attribute added to list)</td>
<td>{ ConfFile, SambaTopDir, LockDir, Ports, IndepthMonitorCyclePeriod, ResponseTimeout, PidFile, SocketAddress }</td>
</tr>
<tr>
<td>SambaShare</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table C-2
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 (new agent)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DiskGroup</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>VolumeSet</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ DiskGroup, VolumeSet }</td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RunFsck</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>DetachZonePath</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ForceAttach</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BootState</td>
<td>&quot;multi-user&quot;</td>
<td></td>
</tr>
<tr>
<td>(change in default value)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArgList</td>
<td>{ Pool, BootState, ShutdownGracePeriod, RunFsck, DetachZonePath, ForceAttach }</td>
<td></td>
</tr>
</tbody>
</table>

### Table C-3
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>Apache</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ContainerName (deleted attribute)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ContainerType (deleted 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></td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerOpts</td>
<td>RunInContainer=1, PassCInfo=0</td>
</tr>
<tr>
<td>Application</td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerType</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerOpts</td>
<td>RunInContainer=1, PassCInfo=0</td>
</tr>
<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>StartVolumes</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>StopVolumes</td>
<td>1</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>RouteOptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PrefixLen</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerOpts</td>
<td>RunInContainer=0, PassCInfo=1</td>
</tr>
</tbody>
</table>
Table C-3  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></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerName</td>
<td>(deleted attribute)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPMultiNIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PrefixLen</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerOpts</td>
<td>RunInContainer=0, PassCInfo=1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerName</td>
<td>(deleted attribute)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPMultiNICB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OnlineRetryLimit</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ContainerOpts</td>
<td>RunInContainer=0, PassCInfo=1</td>
</tr>
<tr>
<td></td>
<td>IgnoreMultiNICBFailure</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>RouteOptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PrefixLen</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerName</td>
<td>(deleted attribute)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDOM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MonitorCPU</td>
<td>1</td>
</tr>
<tr>
<td>Mount</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New 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>OptCheck</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>CreateMountPt</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>ReuseMntPt</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>MntPtPermission</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MntPtOwner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MntPtGroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AccessPermissionChk</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>RecursiveMnt</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>ContainerOpts</td>
<td></td>
<td>RunInContainer=0, PassCInfo=0</td>
</tr>
</tbody>
</table>

**Modified attributes**

| ContainerName    |                             |               |
| ContainerType    |                             | Zone          |

**MultiNICA**

**New attributes**

| Protocol         |                             |               |

**MultiNICB**

**Modified attribute**

| MpathdCommand    |                             | /usr/lib/inet/in.mpathd |

**New attribute**

| Protocol         |                             |               |

**NFS**

**New attribute**

| UseSMF           |                             | 0             |
### Table C-3

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>NFSRestart</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LockServers</td>
<td>20</td>
</tr>
<tr>
<td>NIC</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Phantom</td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dummy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerOpts</td>
<td>RunInContainer=1, PassCInfo=0</td>
</tr>
<tr>
<td></td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerType</td>
<td>Zone</td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
<tr>
<td>ProcessOnOnly</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerOpts</td>
<td>RunInContainer=0, PassCInfo=1</td>
</tr>
<tr>
<td></td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerType</td>
<td>Zone</td>
</tr>
<tr>
<td></td>
<td>(deleted attribute)</td>
<td></td>
</tr>
</tbody>
</table>
### Table C-3  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>
<tr>
<td>Zone</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerOpts</td>
<td>RunInContainer=1, PassCInfo=0</td>
</tr>
<tr>
<td></td>
<td>BootState</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ZoneName</td>
<td>(deleted attribute)</td>
</tr>
</tbody>
</table>

### Table C-4  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 attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SupportedActions</td>
<td>&quot;checkconffile.vfd&quot;</td>
</tr>
<tr>
<td></td>
<td>ContainerType</td>
<td>Zone</td>
</tr>
<tr>
<td></td>
<td>PidFile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IntentionalOffline</td>
<td>0</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></td>
<td>ResRecord</td>
<td></td>
</tr>
</tbody>
</table>
### Table C-4  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>CreatePTR</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>OffDelRR</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>DiskGroup</td>
<td><strong>New attributes</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SupportedActions</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>MountedVolumes</strong></td>
<td>0</td>
</tr>
<tr>
<td>Mount</td>
<td><strong>New attribute</strong></td>
<td></td>
</tr>
<tr>
<td>VxFSMountLock</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Modified attribute</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SupportedActions</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>NFSRestart</td>
<td><strong>New attributes</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SupportedActions</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Share</td>
<td><strong>New attributes</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SupportedActions</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

### Table C-5  Changes to attributes from VCS 4.1 to VCS 5.0

<table>
<thead>
<tr>
<th>Agent</th>
<th>New and modified attributes</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td><strong>New attributes</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Table C-5

Changes to attributes from VCS 4.1 to VCS 5.0 (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>program.vfd, user.vfd, cksum.vfd, getcksum</td>
<td></td>
</tr>
<tr>
<td>DiskGroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SupportedActions</td>
<td>&quot;license.vfd&quot;, &quot;disk.vfd&quot;, &quot;numdisks&quot;</td>
<td></td>
</tr>
<tr>
<td>PanicSystemOnDGLoss</td>
<td>1</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>tempUseFence</td>
<td>Invalid</td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attributes</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>ContainerName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IfconfigTwice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPMultiNIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ContainerName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IfconfigTwice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPMultiNICB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ToleranceLimit</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>MonitorInterval</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>ContainerName</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></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DeviceChoice</td>
<td>0</td>
</tr>
<tr>
<td>Mount</td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SupportedActions</td>
<td>&quot;mountpoint.vfd&quot;, &quot;mounted.vfd&quot;, &quot;vxfslic.vfd&quot;</td>
</tr>
<tr>
<td></td>
<td>VxFSMountLock</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ContainerName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ContainerType</td>
<td>Zone</td>
</tr>
<tr>
<td></td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SnapUmount</td>
<td></td>
</tr>
<tr>
<td>MultiNICA</td>
<td>Modified attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IfconfigTwice</td>
<td></td>
</tr>
<tr>
<td>MultiNICB</td>
<td>New attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GrNew attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GroupName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modified attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NoBroadcast</td>
<td></td>
</tr>
<tr>
<td>NFS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New attributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LockFileTimeout</td>
<td>180</td>
</tr>
<tr>
<td>NIC</td>
<td></td>
<td></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 `/etcVRTSvcs/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.
See Table C-3 on page 441.
See Table C-4 on page 446.
See Table C-5 on page 447.

Save the main.cf.

Reformat the main.cf file.

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

4 Verify the configuration.

```bash
# 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
```
Configuration files

This appendix includes the following topics:

- About the LLT and GAB configuration files
- About the AMF configuration files
- About the VCS configuration files
- About I/O fencing configuration files
- Sample configuration files for CP server

About the LLT and GAB configuration files

Low Latency Transport (LLT) and Group Membership and Atomic Broadcast (GAB) are VCS communication services. LLT requires /etc/llthosts and /etc/llttab files. GAB requires /etc/gabtab file.

Table D-1 lists the LLT configuration files and the information that these files contain.
Table D-1  LLT configuration files

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/default/llt</td>
<td>This file stores the start and stop environment variables for LLT:</td>
</tr>
<tr>
<td></td>
<td>■ LLT_START—Defines the startup behavior for the LLT module after a system reboot. Valid values include:</td>
</tr>
<tr>
<td></td>
<td>1—Indicates that LLT is enabled to start up.</td>
</tr>
<tr>
<td></td>
<td>0—Indicates that LLT is disabled to start up.</td>
</tr>
<tr>
<td></td>
<td>■ LLT_STOP—Defines the shutdown behavior for the LLT module during a system shutdown. Valid values include:</td>
</tr>
<tr>
<td></td>
<td>1—Indicates that LLT is enabled to shut down.</td>
</tr>
<tr>
<td></td>
<td>0—Indicates that LLT 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, make sure you set the values of these environment variables to 1.</td>
</tr>
<tr>
<td>/etc/llhosts</td>
<td>The file llhosts 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.</td>
</tr>
<tr>
<td></td>
<td>For example, the file /etc/llhosts contains the entries that resemble:</td>
</tr>
<tr>
<td></td>
<td>0   galaxy</td>
</tr>
<tr>
<td></td>
<td>1   nebula</td>
</tr>
</tbody>
</table>
### Table D-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 private network links that correspond to the specific system. For example, the file /etc/llttab contains the entries that resemble the following:  

  - **For Solaris SPARC:**
    
    ```
    set-node galaxy  
    set-cluster 2  
    link qfe0 /dev/qfe:0 - ether - -  
    link qfe1 /dev/qfe:1 - ether - -  
    ```

  - **For Solaris x64:**
    
    ```
    set-node galaxy  
    set-cluster 2  
    link e1000g1 /dev/e1000g:1 - ether - -  
    link e1000g2 /dev/e1000g:2 - ether - -  
    ```

    The first line identifies the system. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines begin with the *link* command. These lines identify the two network cards that the LLT protocol uses.  

    If you configured a low priority link under LLT, the file also includes a "link-lowpri" line.  

    Refer to the *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 D-2 lists the GAB configuration files and the information that these files contain.
### Table D-2  
**GAB configuration files**

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
</table>
| /etc/default/gab   | This file stores the start and stop environment variables for GAB:  
  - **GAB_START**—Defines the startup behavior for the GAB module after a system reboot. Valid values include:  
    1—Indicates that GAB is enabled to start up.  
    0—Indicates that GAB is disabled to start up.  
  - **GAB_STOP**—Defines the shutdown behavior for the GAB module during a system shutdown. Valid values include:  
    1—Indicates that GAB is enabled to shut down.  
    0—Indicates that GAB is disabled to shut down.  
  The installer sets the value of these variables to 1 at the end of 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:  
  ```bash  
  /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. |

### About the AMF configuration files

Asynchronous Monitoring Framework (AMF) kernel driver provides asynchronous event notifications to the VCS agents that are enabled for intelligent resource monitoring.

*Table D-3* lists the AMF configuration files.
### Table D-3  AMF configuration files

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
</table>
| /etc/default/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 command that configures the AMF driver for use.  
The AMF init script uses this file to configure the AMF driver. The /etc/amftab file contains the following line by default:  
/optVRTSamf/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 459.  
See “Sample main.cf file for global clusters” on page 460.

- **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/default/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.

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 Solaris systems.

Sample main.cf file for VCS clusters

The following sample main.cf file is for a three-node cluster in secure mode.

```bash
include "types.cf"
include "OracleTypes.cf"
include "OracleASMTypes.cf"
include "Db2udbTypes.cf"
include "SybaseTypes.cf"

cluster vcs02 {
    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
}

NIC csgnic {
    Device = hme0
    NetworkHosts = { "10.182.13.1" }
}

NotifierMngr ntfr {
    SnmpConsoles = { jupiter" = SevereError }
    SmtpServer = "smtp.example.com"
}````
SmtpRecipients = { "ozzie@example.com" = SevereError }

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.

In the following main.cf file example, bold text highlights global cluster specific entries.

include "types.cf"

cluster vcs03 (
    ClusterAddress = "10.182.13.50"
    SecureClus = 1
)

system sysA ( )

system sysB ( )

system sysC ( )

group ClusterService ( SystemList = { sysA = 0, sysB = 1, sysC = 2 } AutoStartList = { sysA, sysB, sysC } )
OnlineRetryLimit = 3
OnlineRetryInterval = 120
)

Application wac {
    StartProgram = "/opt/VRTSvcs/bin/wacstart"
    StopProgram = "/opt/VRTSvcs/bin/wacstop"
    MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
    RestartLimit = 3
}

IP gcoip {
    Device = hme0
    Address = "10.182.13.50"
    NetMask = "255.255.240.0"
}

NIC csgnic {
    Device = hme0
    NetworkHosts = { "10.182.13.1" }
}

NotifierMngr ntfr {
    SnmpConsoles = { jupiter" = 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

About I/O fencing configuration files

Table D-4 lists the I/O fencing configuration files.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/default/vxfen</td>
<td>This file stores the start and stop environment variables for I/O fencing:</td>
</tr>
</tbody>
</table>
|                     |  ■ VXFEN_START—Defines the startup behavior for the I/O fencing module after a system reboot. Valid values include:  
|                     |  1—Indicates that I/O fencing is enabled to start up.  
|                     |  0—Indicates that I/O fencing is disabled to start up.  
|                     |  ■ VXFEN_STOP—Defines the shutdown behavior for the I/O fencing module during a system shutdown. Valid values include:  
|                     |  1—Indicates that I/O fencing is enabled to shut down.  
|                     |  0—Indicates that I/O fencing is disabled to shut down.  
|                     | The installer sets the value of these variables to 1 at the end of VCS configuration.  
|                     | If you manually configured VCS, you must make sure to set the values of these environment variables to 1.                                                                                                     |
| /etc/vxefndg        | This file includes the coordinator disk group information.                                                                                                                                                   |
|                     | This file is not applicable for server-based fencing.                                                                                                                                                       |
### Table D-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 a server-based fencing can include coordinator disks, CP servers, or a mix of both. If you use coordinator disks, you must create a coordinator disk group with the coordinator disk names.</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 D-4  I/O fencing configuration files (continued)

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/vxfentab</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The /etc/vxfentab file is a generated file; do not modify this file.</td>
</tr>
<tr>
<td></td>
<td>For disk-based I/O fencing, the /etc/vxfentab file on each node contains a list of all paths to each coordinator disk. An example of the /etc/vxfentab file in a disk-based fencing configuration on one node resembles as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Raw disk:</td>
</tr>
<tr>
<td></td>
<td>/dev/rdsk/c1t1d0s2</td>
</tr>
<tr>
<td></td>
<td>/dev/rdsk/c2t1d0s2</td>
</tr>
<tr>
<td></td>
<td>/dev/rdsk/c3t1d2s2</td>
</tr>
<tr>
<td></td>
<td>■ DMP disk:</td>
</tr>
<tr>
<td></td>
<td>/dev/vx/rdmp/c1t1d0s2</td>
</tr>
<tr>
<td></td>
<td>/dev/vx/rdmp/c2t1d0s2</td>
</tr>
<tr>
<td></td>
<td>/dev/vx/rdmp/c3t1d0s2</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 470.

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 465.

■ 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 467.
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: mycps1

```
include "types.cf"
include "/opt/VRTScps/bin/Quorum/QuorumTypes.cf"

// cluster name: cps1
// CP server: mycps1

cluster cps1 {
  UserNames = { admin = bMNfMHmJNiNNlVNhMK, haris = fopKojNvpHouNn,
    "mycps1.symantecexample.com@root@vx" = aj,
    "root@mycps1.symantecexample.com" = hq }
  Administrators = { admin, haris,
    "mycps1.symantecexample.com@root@vx",
    "root@mycps1.symantecexample.com" }
  SecureClus = 1
  HacliUserLevel = COMMANDROOT
}

system mycps1 {
}

group CPSSG {
  SystemList = { mycps1 = 0 }
  AutoStartList = { mycps1 }
}

IP cpsvip1 {
  Critical = 0
  Device @mycps1 = hme0
  Address = "10.209.3.1"
```
IP cpsvip2 {
    Critical = 0
    Device @mycps1 = qfe:0
    Address = "10.209.3.2"
    NetMask = "255.255.252.0"
}

NIC cpsnic1 {
    Critical = 0
    Device @mycps1 = hme0
    PingOptimize = 0
    NetworkHosts @mycps1 = { "10.209.3.10" }
}

NIC cpsnic2 {
    Critical = 0
    Device @mycps1 = qfe:0
    PingOptimize = 0
}

Process vxcpser ( PathName = "/opt/VRTScps/bin/vxcpser" ConfInterval = 30 RestartLimit = 3 )

Quorum quorum { QuorumResources = { cpsvip1, cpsvip2 } }

cpsvip1 requires cpsnic1
cpsvip2 requires cpsnic2
vxcpser requires quorum

// resource dependency tree
//
// group CPSSG
// {
//    // IP cpsvip1
Sample main.cf file for CP server hosted on a two-node SFHA cluster

The following is an example of a main.cf, where the CP server is hosted on an SFHA cluster.

For this CP server hosted on an SFHA cluster main.cf, note the following values:

- **Cluster name:** cps1
- **Nodes in the cluster:** mycps1, mycps2

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "/opt/VRTScps/bin/Quorum/QuorumTypes.cf"

// cluster: cps1
// CP servers:
// mycps1
// mycps2

cluster cps1 {
    UserNames = { admin = ajkCjeJgkFkkIskEjh,
                   "mycps1.symantecexample.com@root@vx" = JK,
                   "mycps2.symantecexample.com@root@vx" = dl }
    Administrators = { admin, "mycps1.symantecexample.com@root@vx",
                   "mycps2.symantecexample.com@root@vx" }
    SecureClus = 1
}

system mycps1 {
```

Sample configuration files for CP server
system mycps2 {
}

group CPSSG {
    SystemList = { mycps1 = 0, mycps2 = 1 }
    AutoStartList = { mycps1, mycps2 }
}

DiskGroup cpsdg {
    DiskGroup = cps_dg
}

IP cpsvip1 {
    Critical = 0
    Device @mycps1 = hme0
    Device @mycps2 = hme0
    Address = "10.209.81.88"
    NetMask = "255.255.252.0"
}

IP cpsvip2 {
    Critical = 0
    Device @mycps1 = qfe:0
    Device @mycps2 = qfe:0
    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 @mycps1 = hme0
    Device @mycps2 = hme0
    PingOptimize = 0
    NetworkHosts @mycps1 = { "10.209.81.10" }
NIC cpsnic2 {
    Critical = 0
    Device @mycps1 = qfe:0
    Device @mycps2 = qfe:0
    PingOptimize = 0
}

Process vxcpserv {
    PathName = "/opt/VRTScps/bin/vxcpserv"
}

Quorum quorum {
    QuorumResources = { cpsvip1, cpsvip2 }
}

Volume cpsvol {
    Volume = cps_volume
    DiskGroup = cps_dg
}

cpsmount requires cpsvol
cpsvip1 requires cpsnic1
cpsvip2 requires cpsnic2
cpsvol requires cpsdg
vxcpserv requires cpsmount
vxcpserv requires quorum

// resource dependency tree
//
// group CPSSG
// {
// IP cpsvip1
// { 
//    NIC cpsnic1
// } 
// IP cpsvip2
// { 
//    NIC cpsnic2
// } 
// Process vxcpserv
// { 

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=mycps1
vip=[10.209.81.88]
vip=[10.209.81.89]:56789
port=14250
security=1
db=/etc/VRTScps/db
```
About installing VCS on a single node

You can install VCS 6.0 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 472.

See “Creating a single-node cluster manually” on page 473.
Creating a single-node cluster using the installer program

Table E-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 472.</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 472.</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 25.

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 E-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 473.</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 474.</td>
</tr>
<tr>
<td>Remove any LLT or GAB configuration files and rename LLT and GAB startup files. A single-node cluster does not require the node-to-node communication service, LLT, or the membership communication service, GAB.</td>
<td></td>
</tr>
<tr>
<td>Create and modify the VCS configuration files.</td>
<td>See “Configuring VCS” on page 474.</td>
</tr>
<tr>
<td>Start VCS and verify single-node operation.</td>
<td>See “Verifying single-node operation” on page 474.</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 68.
Installing VCS software manually on a single node

Install the VCS 6.0 packages manually and install the license key.
Refer to the following sections:

- See “Installing VCS software manually” on page 209.
- See “Adding a license key for a manual installation” on page 213.

Configuring VCS

You now need to configure VCS.
See “Configuring VCS manually” on page 228.

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
   ```

   **Note:** You can also use SMF command to start VCS as a single-node cluster.

   ```
   # svcadm enable system/vcs-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.
See “Broadcast address in the /etc/llttab file” on page 476.

- Make sure that each NIC has an IP address that is configured before configuring LLT.
- Make sure the IP addresses in the /etc/llttab files are consistent with the IP addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port. See “Selecting UDP ports” on page 478.
- Set the broadcast address correctly for direct-attached (non-routed) links. See “Sample configuration: direct-attached links” on page 480.
- For the links that cross an IP router, disable broadcast features and specify the IP address of each link manually in the /etc/llttab file. See “Sample configuration: links crossing IP routers” on page 482.

Broadcast address in the /etc/llttab file

The broadcast address is set explicitly for each link in the following example.

- Display the content of the /etc/llttab file on the first node galaxy:

  galaxy # cat /etc/llttab
  set-node galaxy
  set-cluster 1
  link link1 /dev/udp - udp 50000 - 192.168.9.1 192.168.9.255
  link link2 /dev/udp - udp 50001 - 192.168.10.1 192.168.10.255

  Verify the subnet mask using the ifconfig command to ensure that the two links are on separate subnets.

- Display the content of the /etc/llttab file on the second node nebula:

  nebula # cat /etc/llttab
  set-node nebula
  set-cluster 1
  link link1 /dev/udp - udp 50000 - 192.168.9.2 192.168.9.255
  link link2 /dev/udp - udp 50001 - 192.168.10.2 192.168.10.255

  Verify the subnet mask using the ifconfig command to ensure that the two links are on separate subnets.
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 480.
- See “Sample configuration: links crossing IP routers” on page 482.

Table F-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 /dev/udp.</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 478.</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 482.

Table F-2 describes the fields of the set-addr command.
Table F-2  Field description for set-addr command in /etc/ltttab

<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:

```
# netstat -a | more
```

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Remote Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.sunrpc</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>.*</td>
<td></td>
<td>Unbound</td>
</tr>
<tr>
<td>*.32771</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>*.32776</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>*.32777</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>*.name</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>*.biff</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>*.talk</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>*.32779</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.55098</td>
<td></td>
<td>Idle</td>
</tr>
<tr>
<td>*.syslog</td>
<td></td>
<td>Idle</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.

Configuring the netmask for LLT

For nodes on different subnets, set the netmask so that the nodes can access the subnets in use. Run the following command and answer the prompt to set the netmask:

```
# ifconfig interface_name netmask netmask
```

For example:

- For the first network interface on the node galaxy:
  
  IP address=192.168.9.1, Broadcast address=192.168.9.255, Netmask=255.255.255.0

- For the first network interface on the node nebula:
  
  IP address=192.168.9.2, Broadcast address=192.168.9.255, Netmask=255.255.255.0

- For the second network interface on the node galaxy:
  
  IP address=192.168.10.1, Broadcast address=192.168.10.255, Netmask=255.255.255.0

- For the second network interface on the node nebula:
  
  IP address=192.168.10.2, Broadcast address=192.168.10.255, Netmask=255.255.255.0

Configuring the broadcast address for LLT

For nodes on different subnets, set the broadcast address in /etc/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.
Sample configuration: direct-attached links

Figure F-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.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
  IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.1 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.1 192.1.3.255
```

The file for Node 1 resembles:

```
set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
  IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.2 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.2 192.1.3.255
```

**Sample configuration: links crossing IP routers**

Figure F-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 /dev/udp - udp 50000 - 192.1.3.1 -
link link2 /dev/udp - udp 50001 - 192.1.4.1 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 0 link1 192.1.1.1
set-addr 0 link2 192.1.2.1
set-addr 2 link1 192.1.5.2
set-addr 2 link2 192.1.6.2
set-addr 3 link1 192.1.7.3
set-addr 3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb 0
set-arp 0

The /etc/llttab file on Node 0 resembles:

set-node Node0
set-cluster 1

link link1 /dev/udp - udp 50000 - 192.1.1.1 -
link link2 /dev/udp - udp 50001 - 192.1.2.1 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 1 link1 192.1.3.1
set-addr 1 link2 192.1.4.1
set-addr 2 link1 192.1.5.2
set-addr 2 link2 192.1.6.2
set-addr 3 link1 192.1.7.3
set-addr 3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb 0
set-arp 0

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 486.
- 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 489.

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 487.
- See “Sample configuration: links crossing IP routers” on page 489.

Note that some of the fields in Table F-3 differ from the command for standard LLT links.

Table F-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 path of the UDP protocol; for example /dev/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 486.</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>IPv6 address</td>
<td>IPv6 address of the link on the local node.</td>
</tr>
</tbody>
</table>
The set-addr command in the /etc/littab file

The `set-addr` command in the /etc/littab 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 489.

Table F-4 describes the fields of the set-addr command.

<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 -a | more
```

**UDP: IPv4**

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Remote Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.sunrpc</td>
<td></td>
<td>Idle</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 F-3 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 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 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -  
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -  

The file for Node 1 resembles:

set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \  
IP-address mcast-address
link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -  
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -  

Sample configuration: links crossing IP routers

Figure F-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 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -

#set address of each link for all peer nodes in the cluster
```
#format: set-addr node-id link tag-name address
set-addr 0 link1 fe80::21a:64ff:fe92:1b46
set-addr 0 link2 fe80::21a:64ff:fe92:1b47
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb 0
set-arp 0

The /etc/llttab file on Node 0 resembles:

set-node Node0
set-cluster 1

link link1 /dev/udp - udp 50000 - fe80::21a:64ff:fe92:1b46 -
link link2 /dev/udp - udp 50001 - fe80::21a:64ff:fe92:1b47 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 1 link1 fe80::21a:64ff:fe92:1a92
set-addr 1 link2 fe80::21a:64ff:fe92:1a93
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb 0
set-arp 0

LLT over UDP sample /etc/llttab

The following is a sample of LLT over UDP in the etc/llttab file.

set-node galaxy
set-cluster clus1
link e1000g1 /dev/udp - udp 50000 - 192.168.10.1 -
link e1000g2 /dev/udp - udp 50001 - 192.168.11.1 -
link-lowpri e1000g0 /dev/udp - udp 50004 - 10.200.58.205 -
set-addr 1 e1000g1 192.168.10.2
set-addr 1 e1000g2 192.168.11.2
set-addr 1 e1000g0 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.

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.

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 in as root on the source system from which you want to install the Veritas product.

2. To generate a DSA key pair on the source system, type the following:

   ```
   # ssh-keygen -t dsa
   ```

   System output similar to the following is displayed:
   
   Generating public/private dsa key pair.
   Enter file in which to save the key (/.ssh/id_dsa):

3. Press **Enter** to accept the default location of /.ssh/id_dsa. System output similar to the following is displayed:

   Enter passphrase (empty for no passphrase):

4. Do not enter a passphrase. Press **Enter**. Enter same passphrase again. Press **Enter** again.

5. Make sure the /.ssh directory is on all the target installation systems. If that directory is absent, create it on the target system and set the write permission to root only:

   ```
   # mkdir /.ssh
   # chmod go-w /
   # chmod 700 /.ssh
   # chmod go-rwx /.ssh
   ```
Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems. To enable SFTP, the `/etc/ssh/sshd_config` file must contain the following two lines:

```
PermitRootLogin yes
Subsystem sftp /usr/lib/ssh/sftp-server
```

If the lines are not there, add them and restart SSH. To restart SSH on Solaris 10, type the following command:

```
# svcadm restart ssh
```

To copy the public DSA key, `/.ssh/id_dsa.pub` to each target system, type the following commands:

```
# sftp target_sys
```

If you run this step for the first time on a system, output similar to the following appears:

```
Connecting to target_sys...
The authenticity of host 'target_sys (10.182.00.00)' can't be established. DSA key fingerprint is fb:6f:9e:61:91:9e:44:6b:87:86:ef:68:a6:fd:87:7d.
Are you sure you want to continue connecting (yes/no)?
```

Enter `yes`. Output similar to the following is displayed:

```
Warning: Permanently added 'target_sys,10.182.00.00' (DSA) to the list of known hosts.
root@target_sys password:
```

Enter the root password.

At the `sftp` prompt, type the following command:

```
sftp> put /.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /.ssh/id_dsa.pub to /id_dsa.pub
```

To quit the SFTP session, type the following command:

```
sftp> quit
```
To begin the ssh session on the target system, type the following command:

```bash
# ssh target_sys
```

14 Enter the root password at the prompt:

```bash
password:
```

15 After you log in, enter the following command to append the authorization key to the id_dsa.pub file:

```bash
# cat /id_dsa.pub >> ~/.ssh/authorized_keys
```

16 Delete the id_dsa.pub public key file. Before you delete this public key file, make sure to complete the following tasks:

- The file is copied to the target (host) system
- The file is added to the authorized keys file

To delete the id_dsa.pub public key file, type the following command:

```bash
# rm /id_dsa.pub
```

17 To log out of the ssh session, type the following command:

```bash
# exit
```

18 When you install from a source system that is also an installation target, add the local system id_dsa.pub key to the local .ssh/authorized_key file. The installation can fail if the installation source system is not authenticated.
Run the following commands on the source installation system. These commands bring the private key into the shell environment and makes the key globally available for the user root:

```
# exec /usr/bin/ssh-agent $SHELL
# ssh-add
Identity added: ~/.ssh/identity
```

This step is shell-specific and is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

To verify that you can connect to the target system, type the following command:

```
# ssh -l root target_sys uname -a
```

The commands should execute on the remote system without any requests for a passphrase or password from the system.
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
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:
  
  ```bash
  # /opt/VRTS/bin/vxkeyless
  ```

- 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:

  ```bash
  # ./installer -stop
  ```
To start the processes

- Use the -start option to start the product installation script.

For example, to start the product’s processes, enter the following command:

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

## 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.

```
# /opt/VRTSvcs/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

Check the log files that get generated in the /var/svc/log directory for any errors.

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 vxfsentsthdw utility fails when SCSI TEST UNIT READY command fails

While running the vxfsentsthdw 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 H-1  Fencing startup issues on VCS cluster (client cluster) nodes

<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. |
Table H-1  Fencing startup issues on VCS cluster (client cluster) nodes

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description and resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization failure</td>
<td>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 239.</td>
</tr>
</tbody>
</table>
| 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 I-1 on page 506.
- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:
- Two node campus cluster that is served be remote CP server and 2 SCSI-3 disks:
- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:

Two unique client clusters served by 3 CP servers

Figure I-1 displays a configuration where two unique client clusters are being served by 3 CP servers (coordination points). Each client cluster has its own unique user ID (UUID1 and UUID2).
In the `vxfenmode` file on the client nodes, `vxfenmode` is set to customized with `vxfen mechanism` set to `cps`.

**Figure I-1**  Two unique client clusters served by 3 CP servers

Client cluster served by highly available CPS and 2 SCSI-3 disks

**Figure I-2** displays a configuration where a client cluster is served by one highly available CP server and 2 local SCSI-3 LUNs (disks).
In the `vxfenmode` file on the client nodes, `vxfenmode` is set to customized with `vxfen` mechanism set to `cps`.

The two SCSI-3 disks are part of the disk group `vxfencoorddg`. The third coordination point is a CP server hosted on an SFHA cluster, with its own shared database and coordinator disks.

**Figure I-2** Client cluster served by highly available CP server and 2 SCSI-3 disks
Two node campus cluster served by remote CP server and 2 SCSI-3 disks

Figure I-3 displays a configuration where a two node campus cluster is being served by one remote CP server and 2 local SCSI-3 LUN (disks).

In the vxfenmode file on the client nodes, vxfenmode is set to customized with vxfen mechanism set to cps.

The two SCSI-3 disks (one from each site) are part of disk group vxfencoorddg. The third coordination point is a CP server on a single node VCS cluster.
Figure I-3  Two node campus cluster served by remote CP server and 2 SCSI-3

On the client cluster:
\texttt{vxfenmode=customized}\n\texttt{vxfen\_mechanism=cps}\n\texttt{cps1=[VIP]:14250}\n\texttt{vxfenbg=vxfencoordbg}\n
The coordinator disk group specified in /etc/vxfenmode should have one SCSI3 disk from site1 and another from site2.

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 I-4 displays a configuration where multiple client clusters are being served by one highly available CP server and 2 local SCSI-3 LUNS (disks).

In the `vxfenmode` file on the client nodes, `vxfenmode` is set to `customized` with the `vxfen mechanism` set to `cps`.

The two SCSI-3 disks are part of the disk group `vxfencoorddg`. The third coordination point is a CP server, hosted on an SFHA cluster, with its own shared database and coordinator disks.
Figure I-4  Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

The coordinator disk group specified in /etc/vxfenmode 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
Reconciling major/minor numbers for NFS shared disks

This appendix includes the following topics:

■ Reconciling major/minor numbers for NFS shared disks

Reconciling major/minor numbers for NFS shared disks

Your configuration may include disks on the shared bus that support NFS. You can configure the NFS file systems that you export on disk partitions or on Veritas Volume Manager volumes.

An example disk partition name is /dev/dsk/c1t1d0s2.

An example volume name is /dev/vx/dsk/sharreddg/vol3. Each name represents the block device on which the file system is to be mounted.

In a VCS cluster, block devices providing NFS service must have the same major and minor numbers on each cluster node. Major numbers identify required device drivers (such as a Solaris partition or a VxVM volume). Minor numbers identify the specific devices themselves. NFS also uses major and minor numbers to identify the exported file system.

Major and minor numbers must be verified to ensure that the NFS identity for the file system is the same when exported from each node.
Checking major and minor numbers for disk partitions

The following sections describe checking and changing, if necessary, the major and minor numbers for disk partitions used by cluster nodes.

To check major and minor numbers on disk partitions

- Use the following command on all nodes exporting an NFS file system. This command displays the major and minor numbers for the block device.

  # ls -lL block_device

  The variable block_device refers to a partition where a file system is mounted for export by NFS. Use this command on each NFS file system. For example, type:

  # ls -lL /dev/dsk/c1t1d0s2

  Output on Node A resembles:

  crw-r----- 1 root  sys 32,1 Dec 3 11:50 /dev/dsk/c1t1d0s2

  Output on Node B resembles:

  crw-r----- 1 root  sys 32,1 Dec 3 11:55 /dev/dsk/c1t1d0s2

  Note that the major numbers (32) and the minor numbers (1) match, satisfactorily meeting the requirement for NFS file systems.

To reconcile the major numbers that do not match on disk partitions

1. Reconcile the major and minor numbers, if required. For example, if the output in the previous section resembles the following, perform the instructions beginning step 2:

   Output on Node A:

   crw-r----- 1 root  sys 32,1 Dec 3 11:50 /dev/dsk/c1t1d0s2

   Output on Node B:

   crw-r----- 1 root  sys 36,1 Dec 3 11:55 /dev/dsk/c1t1d0s2

2. Place the VCS command directory in your path.

   # export PATH=$PATH:/usr/sbin:/sbin:/opt/VRTS/bin
3 Attempt to change the major number on System B (now 36) to match that of System A (32). Use the command:

```
# haremajor -sd major_number
```

For example, on Node B, enter:

```
# haremajor -sd 32
```

4 If the command succeeds, go to step 8.

5 If the command fails, you may see a message resembling:

```
Error: Preexisting major number 32
These are available numbers on this system: 128...
Check /etc/name_to_major on all systems for available numbers.
```

6 Notice that the number 36 (the major number on Node A) is not available on Node B. Run the `haremajor` command on Node B and change it to 128.

```
# haremajor -sd 128
```

7 Run the same command on Node A. If the command fails on Node A, the output lists the available numbers. Rerun the command on both nodes, setting the major number to one available to both.

8 Reboot each system on which the command succeeds.

9 Proceed to reconcile the major numbers for your next partition.

To reconcile the minor numbers that do not match on disk partitions

1 In the example, the minor numbers are 1 and 3 and are reconciled by setting to 30 on each node.

2 Type the following command on both nodes using the name of the block device:

```
# ls -l /dev/dsk/c1t1d0s2
```

Output from this command resembles the following on Node A:

```
lrwxrwxrwx 1 root root 83 Dec 3 11:50 /dev/dsk/c1t1d0s2 -> ../devices/sbus@1f,0/QLGC,isp@0,10000/sd@1,0:d,raw
```

The device name (in bold) includes the slash following the word `devices`, and continues to, but does not include, the colon.
3 Type the following command on both nodes to determine the instance numbers that the SCSI driver uses:

```
# grep sd /etc/path_to_inst | sort -n -k 2,2
```

Output from this command resembles the following on Node A:

```
"/sbus@1f,0/QLGC,isp@0,10000/sd@0,0" 0 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@1,0" 1 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@2,0" 2 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@3,0" 3 "sd"
```

In the output, the instance numbers are in the second field.

The instance number that is associated with the device name that matches the name for Node A displayed in step 2, is "1."

4 Compare instance numbers for the device in the output on each node.

After you review the instance numbers, perform one of the following tasks:

- If the instance number from one node is unused on the other— it does not appear in the output of step 3— edit `/etc/path_to_inst`. You edit this file to make the second node’s instance number similar to the number of the first node.

- If the instance numbers in use on both nodes, edit `/etc/path_to_inst` on both nodes. Change the instance number that is associated with the device name to an unused number. The number needs to be greater than the highest number that other devices use. For example, the output of step 3 shows the instance numbers that all devices use (from 0 to 29). You edit the file `/etc/path_to_inst` on each node and reset the instance numbers to 30.

5 Type the following command to reboot each node on which `/etc/path_to_inst` was modified:

```
# reboot -- -rv
```
Checking the major and minor number for VxVM volumes

The following sections describe checking and changing, if necessary, the major and minor numbers for the VxVM volumes that cluster systems use.

To check major and minor numbers on VxVM volumes

1. Place the VCS command directory in your path. For example:

   ```
   # export PATH=$PATH:/usr/sbin:/sbin:/opt/VRTS/bin
   ```

2. To list the devices, use the `ls -lL block_device` command on each node:

   ```
   # ls -lL /dev/vx/dsk/sharedd/vol3
   ```

   On Node A, the output may resemble:

   ```
   brw------- 1 root root 32,43000 Mar 22 16:4 1 /dev/vx/dsk/sharedd/vol3
   ```

   On Node B, the output may resemble:

   ```
   brw------- 1 root root 36,43000 Mar 22 16:4 1 /dev/vx/dsk/sharedd/vol3
   ```

3. Import the associated shared disk group on each node.
4 Use the following command on each node exporting an NFS file system. The command displays the major numbers for `vxio` and `vxspec` that Veritas Volume Manager uses. Note that other major numbers are also displayed, but only `vxio` and `vxspec` are of concern for reconciliation:

```bash
# grep vx /etc/name_to_major
```

Output on Node A:

```plaintext
vxrdmp 30
vxio 32
vxspec 33
vxfen 87
vxglm 91
```

Output on Node B:

```plaintext
vxrdmp 30
vxio 36
vxspec 37
vxfen 87
vxglm 91
```

5 To change Node B’s major numbers for `vxio` and `vxspec` to match those of Node A, use the command:

```bash
haremajor -vx major_number_vxio major_number_vxspec
```

For example, enter:

```bash
# haremajor -vx 32 33
```

If the command succeeds, proceed to step 8. If this command fails, you receive a report similar to the following:

```
Error: Preexisting major number 32
These are available numbers on this system: 128...
Check /etc/name_to_major on all systems for available numbers.
```
If you receive this report, use the `haremajor` command on Node A to change the major number (32/33) to match that of Node B (36/37). For example, enter:

```
# haremajor -vx 36 37
```

If the command fails again, you receive a report similar to the following:

```
Error: Preexisting major number 36
These are available numbers on this node: 126...
Check /etc/name_to_major on all systems for available numbers.
```

If you receive the second report, choose the larger of the two available numbers (in this example, 128). Use this number in the `haremajor` command to reconcile the major numbers. Type the following command on both nodes:

```
# haremajor -vx 128 129
```

Reboot each node on which `haremajor` was successful.

If the minor numbers match, proceed to reconcile the major and minor numbers of your next NFS block device.

If the block device on which the minor number does not match is a volume, consult the `vxdg(1M)` manual page. The manual page provides instructions on reconciling the Veritas Volume Manager minor numbers, and gives specific reference to the `reminor` option.

Node where the vxio driver number have been changed require rebooting.
Reconciling major/minor numbers for NFS shared disks
Compatability 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 NetBackup is already present

Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.
Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host packages as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

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

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx and VRTSicsco. It does not upgrade VRTSsat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx, VRTSicsco, and VRTSsat.
creating
Flash archive 219
post-deployment scripts 220

data disks
for I/O fencing 32
demo key 215
directives
LLT 225
disk space
directories 36
language pack 36
required 36
disks
adding and initializing 137
coordinator 234
testing with vxfentsthdw 140
verifying node access 142
documentation
accessing 337
eeprom
parameters 60
Ethernet controllers 60, 390

FC-AL controllers 67
fibre channel 36
flarcreate 219
Flash archive 219
post-deployment scripts 220
functions
go 69

G
GAB
description 25
manual configuration 227
port membership information 349
starting 231
verifying 349
gabconfig command 227, 349
-a (verifying GAB) 349
gabtab file
creating 227
verifying after installation 453

global clusters 27
configuration 131

H
hardware
configuration 24
configuring network and storage 36
hastart 401
hastatus -summary command 351
hasy -stop command 369
hasys -display command 351
hubs 60
independent 390

I
I/O fencing
checking disks 140
setting up 233
shared storage 140
I/O fencing requirements
non-SCSI-3 41
installer program
uninstalling language packages 362
Installing
VCS with the Web-based installer 163
installing
JumpStart 216
language packages 87
manually 213
manual 209
post 132
required disk space 36
simulator 342
installing manually
Chinese language packages 212
Japanese language packages 212
installing VCS
required information 73
installvcs
options 45
installvcs prompts
b 45
n 45
y 45

J
Japanese language packages 212
Java Console 29
installing 339
installing on UNIX 339
JumpStart
installing 216

L
language packages 362
Chinese 212
disk space 36
Japanese 212
license keys
adding with vxlicinst 134, 213
obtaining 54
replacing demo key 135, 215
licenses
information about 133
showing information 215
links
private network 453
Live Upgrade
preparing 303
upgrade paths 301
upgrading Solaris on alternate boot disk 307
LLT
description 25
directives 225
interconnects 70
manual configuration 223
starting 231
verifying 347
LLT directives
link 225
link-lowpri 225
set-cluster 225
set-node 225
lltconfig command 453
llthosts file
verifying after installation 453
llstat command 347
llttab file
verifying after installation 453

M
MAC addresses 60
main.cf file
contents after installation 459
main.cf files 464
major and minor numbers
checking 514, 517
shared devices 513
MANPATH variable
setting 68
manual installation
preparing 207
media speed 70
optimizing 70
membership information 349
mounting
software disc 71

N
network partition
preexisting 26
protecting against 24
Network partitions
protecting against 25
network switches 60
NFS 23
NFS services
shared storage 513
non-SCSI-3 fencing
manual configuration 250
setting up 250
non-SCSI-3 I/O fencing
requirements 41
non-SCSI3 fencing
setting up 154
using installvcs program 154

O
optimizing
media speed 70
overview
VCS 23

P
parameters
eeprom 60
PATH variable
setting 68
VCS commands 346
persistent reservations
SCSI-3 64
phased 269
variables
  MANPATH 68
  PATH 68

VCS
  basics 23
  command directory path variable 346
  configuration files
    main.cf 457
  configuring 113
  coordinator disks 234
  documentation 337
  manually installing 209
  notifications 27
  replicated states on each system 24
  starting 230–231

VCS features 27

VCS installation
  verifying
    cluster operations 346
    GAB operations 346
    LLT operations 346

VCS notifications
  SMTP notification 27
  SNMP notification 27

Veritas Operations Manager 29

Volume Manager
  Fibre Channel 67
  vxdisksetup command 137
  vxlicinst command 134, 213
  vxlicrep command 133, 215

W
  Web-based installer 163