

Symantec™ Storage Foundation and High Availability Solutions 6.2.1 Installation Guide - Linux

Maintenance Release

RHEL 6, 7, OL 6, 7, SLES 11

Symantec Storage Foundation and High Availability Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 6.2.1

Document version: 6.2.1 Rev 0

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. See the Third-party Legal Notices document for this product, which is available online or included in the base release media.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan customercare_apac@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America supportsolutions@symantec.com

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>

Documentation

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

<https://sort.symantec.com/documents>

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

doc_feedback@symantec.com

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

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

Contents

| | |
|--|----|
| Technical Support | 4 |
| Section 1 Installing, upgrading, and removing SFHA Solutions | 16 |
| Chapter 1 About Symantec™ Storage Foundation and High Availability Solutions | 17 |
| About Symantec™ Storage Foundation and High Availability Solutions 6.2.1 | 17 |
| Supported operating systems and database software | 19 |
| Chapter 2 Installing the products for the first time | 20 |
| Supported types of Installation | 20 |
| Installing the Symantec software using the Install Bundles feature | 20 |
| Chapter 3 Upgrading to 6.2.1 from releases earlier than 6.2 | 22 |
| Planning to upgrade to SFHA Solutions 6.2.1 | 22 |
| Supported upgrade types for SFHA Solutions 6.2.1 | 22 |
| Supported upgrade paths for SFHA Solutions 6.2.1 | 23 |
| About using the installer to upgrade from releases earlier than 6.2 when the root disk is encapsulated | 28 |
| Preparing to upgrade Volume Replicator | 29 |
| Downloading SFHA Solutions 6.2.1 | 31 |
| Performing a full upgrade with Install Bundles | 32 |
| Performing a full upgrade of VCS using Install Bundles | 32 |
| Performing a full upgrade of SFHA using Install Bundles | 34 |
| Performing a full upgrade of SFCFSHA using Install Bundles | 37 |
| Performing a full upgrade of SF Oracle RAC using Install Bundles | 41 |
| Performing a phased upgrade using Install Bundles | 47 |
| Performing a phased VCS upgrade using Install Bundles | 48 |

| | | |
|-----------|---|-----|
| | Performing a phased SFHA upgrade using Install Bundles | 62 |
| | Performing a phased SFCFSHA upgrade using Install Bundles | 77 |
| | Performing a phased SF Oracle RAC upgrade using Install Bundles | 84 |
| | Performing a rolling upgrade using Install Bundles | 95 |
| | Supported rolling upgrade paths | 95 |
| | OS upgrade support during rolling upgrades on Linux | 96 |
| | Performing a rolling upgrade of VCS, SFHA, and SFCFSHA with Install Bundles | 96 |
| | Performing a rolling upgrade of SF Oracle RAC with Install Bundles | 99 |
| | Performing an automated upgrade using response files with Install Bundles | 107 |
| | Performing an automated upgrade using response files with Install Bundles | 107 |
| Chapter 4 | Upgrading to 6.2.1 from 6.2 | 108 |
| | Prerequisites for upgrading to 6.2.1 | 108 |
| | Downloading required software to upgrade to 6.2.1 | 109 |
| | Performing a full upgrade to 6.2.1 on a cluster | 109 |
| | Performing a full upgrade to 6.2.1 on a Symantec Cluster Server | 109 |
| | Performing a full upgrade to 6.2.1 on an SFHA cluster | 110 |
| | Performing a full upgrade to 6.2.1 on an SFCFSHA cluster | 111 |
| | Performing a full upgrade to 6.2.1 on an SF Oracle RAC cluster | 113 |
| | Upgrading to 6.2.1 on a standalone system | 116 |
| | Performing a phased upgrade to SFCFSHA and SFRAC | 118 |
| | Performing a phased upgrade of SFCFSHA | 118 |
| | Performing phased upgrade of SF Oracle RAC to version 6.2.1 | 128 |
| | Upgrading to 6.2.1 on a system that has encapsulated boot disk | 141 |
| | Performing a rolling upgrade using the installer | 141 |
| | About rolling upgrades | 142 |
| | Prerequisites for a rolling upgrade | 142 |
| | Performing a rolling upgrade using the installer | 143 |
| | Upgrading the operating system | 151 |
| | Upgrading SFHA with the Veritas Web-based installer | 152 |
| | Verifying software versions | 153 |

| | | |
|------------|--|-----|
| Chapter 5 | Removing Symantec Storage Foundation and High Availability Solutions | 154 |
| | About removing Symantec Storage Foundation and High Availability Solutions 6.2.1 | 154 |
| | Uninstalling Symantec Storage Foundation Cluster File System High Availability 6.2.1 | 155 |
| | Preparing to uninstall Symantec Storage Foundation Cluster File System High Availability | 155 |
| | Uninstalling Symantec Storage Foundation Cluster File System High Availability | 157 |
| | Uninstalling Symantec Storage Foundation for Oracle RAC 6.2.1 | 158 |
| Appendix A | About the installation script | 160 |
| | About the installation script | 160 |
| | The installmr script options | 160 |
| Section 2 | Installing and configuring SFSYBASECE on RHEL 6 | 166 |
| Chapter 6 | Installation overview and planning | 168 |
| | Introducing SF Sybase ASE CE | 168 |
| | About Symantec Storage Foundation for Sybase ASE CE | 168 |
| | Benefits of SF Sybase CE | 169 |
| | About SF Sybase CE components | 170 |
| | About SF Sybase ASE CE optional features | 170 |
| | About Cluster Manager (Java Console) | 173 |
| | About Veritas Operations Manager | 173 |
| | About Symantec Operations Readiness Tools | 173 |
| | SF Sybase CE cluster setup models | 175 |
| | System requirements | 180 |
| | Release notes | 180 |
| | Important preinstallation information for SF Sybase CE | 180 |
| | Hardware requirements | 180 |
| | Supported operating systems | 181 |
| | Coordinator disk requirements for I/O fencing | 181 |
| | Supported Sybase ASE CE releases | 182 |
| | Supported SF Sybase CE configurations | 182 |
| | Supported replication technologies for global clusters | 182 |
| | Checking installed product versions and downloading maintenance releases and patches | 183 |

| | | |
|-----------|--|-----|
| | Planning to install SF Sybase ASE CE | 185 |
| | Planning your network configuration | 185 |
| | Planning the storage | 186 |
| | Planning volume layout | 188 |
| | About planning to configure I/O fencing | 188 |
| | Planning for cluster management | 190 |
| | Licensing SF Sybase ASE CE | 191 |
| | About Symantec product licensing | 191 |
| | Setting or changing the product level for keyless licensing | 193 |
| | Installing Symantec product license keys | 195 |
| Chapter 7 | Preparing to install SF Sybase CE | 196 |
| | About preparing to install and configure SF Sybase CE | 196 |
| | Synchronizing time settings on cluster nodes | 197 |
| | Setting up inter-system communication | 198 |
| | Setting up ssh on cluster systems | 198 |
| | Setting up shared storage | 199 |
| | Setting the environment variables for Sybase ASE CE | 200 |
| | Setting the kernel.panic tunable | 200 |
| | Configuring the I/O scheduler | 201 |
| | Optimizing LLT media speed settings on private NICs | 201 |
| | Guidelines for setting the media speed for LLT interconnects | 201 |
| | Verifying the systems before installation | 202 |
| | About installation and configuration methods | 202 |
| Chapter 8 | Installation of SF Sybase ASE CE using the script-based installer | 204 |
| | Installing SF Sybase ASE CE | 204 |
| | About the script-based installer | 204 |
| | Installing SF Sybase CE using the Veritas script-based installation program | 206 |
| | Configuring SF Sybase ASE CE | 209 |
| | About configuring SF Sybase CE | 209 |
| | Configuring the SF Sybase CE components using the script-based installer | 210 |
| | Configuring the SF Sybase ASE CE cluster | 212 |
| | Configuring the cluster name | 213 |
| | Configuring private heartbeat links | 213 |
| | Configuring the virtual IP of the cluster | 218 |
| | Configuring Symantec Storage Foundation for Sybase ASE CE in secure mode | 219 |
| | Configuring a secure cluster node by node | 220 |

| | | |
|------------|--|-----|
| | Adding VCS users | 224 |
| | Configuring SMTP email notification | 225 |
| | Configuring SNMP trap notification | 227 |
| | Configuring global clusters | 228 |
| | Setting up disk-based I/O fencing using installsfsybasece | 229 |
| | Configuring disk-based I/O fencing using installsfsybasece | 230 |
| | Initializing disks as VxVM disks | 232 |
| | Identifying disks to use as coordinator disks | 233 |
| | Checking shared disks for I/O fencing | 233 |
| Chapter 9 | Managing your Symantec deployments | 238 |
| | About the Deployment Server | 239 |
| | Deployment Server overview | 240 |
| | Installing the Deployment Server | 241 |
| | Setting up a Deployment Server | 242 |
| | Setting deployment preferences | 245 |
| | Specifying a non-default repository location | 247 |
| | Downloading the most recent release information | 247 |
| | Loading release information and patches on to your Deployment Server | 248 |
| | Viewing or downloading available release images | 249 |
| | Viewing or removing repository images stored in your repository | 254 |
| | Deploying Symantec product updates to your environment | 256 |
| | Finding out which releases you have installed, and which upgrades or updates you may need | 257 |
| | Defining Install Bundles | 259 |
| | Creating Install Templates | 264 |
| | Deploying Symantec releases | 266 |
| | Connecting the Deployment Server to SORT using a proxy server | 269 |
| Chapter 10 | Post-installation tasks | 270 |
| | Verifying the installation | 270 |
| | Performing a postcheck on a node | 270 |
| | Verifying SF Sybase CE installation using VCS configuration file | 270 |
| | Verifying LLT, GAB, and cluster operation | 271 |
| | Performing additional post-installation and configuration tasks | 278 |
| | About enabling LDAP authentication for clusters that run in secure mode | 278 |
| | Configuring Volume Replicator | 287 |

| | | |
|------------|--|-----|
| | Running SORT Data Collector to collect configuration information | 287 |
| Chapter 11 | Installing and configuring Sybase ASE CE | 289 |
| | Before installing Sybase ASE CE | 289 |
| | Preparing for local mount point on VxFS for Sybase ASE CE binary installation | 290 |
| | Preparing for shared mount point on CFS for Sybase ASE CE binary installation | 291 |
| | Installing Sybase ASE CE software | 292 |
| | Preparing to create a Sybase ASE CE cluster | 292 |
| | Creating the Sybase ASE CE cluster | 294 |
| | Preparing to configure the Sybase instances under VCS control | 294 |
| | Language settings for the Sybase agent | 294 |
| | Configuring Sybase for detail monitoring | 295 |
| | Encrypting passwords for Sybase | 297 |
| | About setting up detail monitoring for the agent for Sybase | 297 |
| | Configuring a Sybase CE cluster under VCS control using the SF Sybase CE installer | 299 |
| Chapter 12 | Automated installation using response files | 308 |
| | About response files | 308 |
| | Response file syntax | 309 |
| | Guidelines for creating the SF Sybase CE response file | 310 |
| | Installation scenarios for response files | 311 |
| | Performing an automated SF Sybase CE installation | 311 |
| | Installing SF Sybase CE using response files | 311 |
| | Response file variables to install SF Sybase CE | 312 |
| | Sample response file for installing SF Sybase CE | 315 |
| | Performing an automated SF Sybase CE configuration | 315 |
| | Configuring SF Sybase CE using response files | 315 |
| | Response file variables to configure SF Sybase CE | 316 |
| | Sample response files for configuring SF Sybase CE | 326 |
| | Performing an automated I/O fencing configuration using response files | 327 |
| | Configuring I/O fencing using response files | 327 |
| | Response file variables to configure disk-based I/O fencing | 328 |
| | Sample response file for configuring disk-based I/O fencing | 331 |
| | Configuring a Sybase cluster under VCS control using a response file | 332 |
| | Configuring a Sybase cluster under VCS control with a response file | 332 |

| | | |
|------------|---|-----|
| | Response file variables to configure SF Sybase CE in VCS | 333 |
| Chapter 13 | Adding and removing nodes | 335 |
| | Adding a node to SF Sybase CE clusters | 335 |
| | About adding a node to a cluster | 335 |
| | Before adding a node to a cluster | 336 |
| | Adding the node to a cluster manually | 338 |
| | Adding a node to a cluster using the SF Sybase CE installer | 346 |
| | Adding the new instance to the Sybase ASE CE cluster | 349 |
| | Removing a node from SF Sybase CE clusters | 353 |
| | About removing a node from a cluster | 353 |
| | Removing a node from a cluster | 354 |
| | Modifying the VCS configuration files on existing nodes | 356 |
| | Modifying the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node | 359 |
| | Removing security credentials from the leaving node | 359 |
| Chapter 14 | Configuration of disaster recovery environments | 360 |
| | Disaster recovery options for SF Sybase CE | 360 |
| | About setting up a global cluster environment for SF Sybase CE | 361 |
| | About configuring a parallel global cluster using Volume Replicator (VVR) for replication | 361 |
| Chapter 15 | Uninstallation of Sybase ASE CE | 364 |
| | Preparing to uninstall SF Sybase CE from a cluster | 364 |
| | Uninstalling SF Sybase CE with the script-based installer | 365 |
| | Performing an automated uninstallation of SF Sybase CE using response files | 365 |
| | Uninstalling SF Sybase CE using a response file | 365 |
| | Response file variables to uninstall SF Sybase CE | 366 |
| | Sample response file for uninstalling SF Sybase CE | 367 |
| Appendix B | SF Sybase CE installation RPMs | 368 |
| | SF Sybase CE installation RPMs | 368 |
| Appendix C | Installation scripts | 371 |
| | Installation script options | 371 |
| | About using the postcheck option | 378 |

| | | |
|------------|--|-----|
| Appendix D | Sample installation and configuration values | 381 |
| | SF Sybase CE installation and configuration information | 381 |
| | SF Sybase CE worksheet | 381 |
| Appendix E | Tunable files for installation | 386 |
| | Setting tunables for an installation, configuration, or upgrade | 386 |
| | Setting tunables with no other installer-related operations | 387 |
| | Setting tunables with an un-integrated response file | 388 |
| | Preparing the tunables file | 389 |
| | Setting parameters for the tunables file | 390 |
| | Tunables value parameter definitions | 390 |
| Appendix F | Configuration files | 399 |
| | About sample main.cf files | 399 |
| | Sample main.cf files for Sybase ASE CE configurations | 399 |
| | Sample main.cf for a basic Sybase ASE CE cluster configuration under VCS control with shared mount point on CFS for Sybase binary installation | 400 |
| | Sample main.cf for a basic Sybase ASE CE cluster configuration with local mount point on VxFS for Sybase binary installation | 404 |
| | Sample main.cf for a primary CVM VVR site | 409 |
| | Sample main.cf for a secondary CVM VVR site | 415 |
| Appendix G | Configuring the secure shell or the remote shell for communications | 422 |
| | About configuring secure shell or remote shell communication modes before installing products | 422 |
| | Manually configuring passwordless ssh | 423 |
| | Setting up ssh and rsh connection using the installer -comsetup command | 426 |
| | Setting up ssh and rsh connection using the pwdutil.pl utility | 427 |
| | Restarting the ssh session | 431 |
| | Enabling rsh for Linux | 431 |
| Appendix H | High availability agent information | 434 |
| | About agents | 434 |
| | VCS agents included within SF Sybase CE | 435 |
| | VCS agent for Sybase included within SF Sybase CE | 435 |
| | CVMCluster agent | 436 |

| | |
|---|-----|
| Entry points for CVMCluster agent | 436 |
| Attribute definition for CVMCluster agent | 436 |
| CVMCluster agent type definition | 437 |
| CVMCluster agent sample configuration | 438 |
| CVMVxconfigd agent | 438 |
| Entry points for CVMVxconfigd agent | 438 |
| Attribute definition for CVMVxconfigd agent | 439 |
| CVMVxconfigd agent type definition | 440 |
| CVMVxconfigd agent sample configuration | 441 |
| CVMVoidg agent | 441 |
| Entry points for CVMVoidg agent | 441 |
| Attribute definition for CVMVoidg agent | 442 |
| CVMVoidg agent type definition | 444 |
| CVMVoidg agent sample configuration | 444 |
| CVMVoidg agent sample configuration | 445 |
| CFSMount agent | 445 |
| Entry points for CFSMount agent | 445 |
| Attribute definition for CFSMount agent | 446 |
| CFSMount agent type definition | 448 |
| CFSMount agent sample configuration | 449 |
| Process agent | 449 |
| Agent functions | 449 |
| State definitions | 450 |
| Attributes | 450 |
| Resource type definition | 451 |
| Sample configurations | 452 |
| Monitoring options for the Sybase agent | 452 |
| Sybase resource type | 452 |
| Type definition for the Sybase agent | 453 |
| Attribute definitions for the Sybase agent | 453 |

Appendix I

| | |
|--|-----|
| Compatibility issues when installing Storage Foundation for Sybase ASE CE with other products | 460 |
| Installing, uninstalling, or upgrading Storage Foundation products when other Symantec products are present | 460 |
| Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present | 461 |
| Installing, uninstalling, or upgrading Storage Foundation products when ApplicationHA is already present | 461 |
| Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present | 462 |

Installing, upgrading, and removing SFHA Solutions

- [Chapter 1. About Symantec™ Storage Foundation and High Availability Solutions](#)
- [Chapter 2. Installing the products for the first time](#)
- [Chapter 3. Upgrading to 6.2.1 from releases earlier than 6.2](#)
- [Chapter 4. Upgrading to 6.2.1 from 6.2](#)
- [Chapter 5. Removing Symantec Storage Foundation and High Availability Solutions](#)
- [Appendix A. About the installation script](#)

About Symantec™ Storage Foundation and High Availability Solutions

This chapter includes the following topics:

- [About Symantec™ Storage Foundation and High Availability Solutions 6.2.1](#)
- [Supported operating systems and database software](#)

About Symantec™ Storage Foundation and High Availability Solutions 6.2.1

Symantec™ Storage Foundation and High Availability Solutions 6.2.1 provides patch updates for the following products:

- Symantec Dynamic Multi-Pathing (DMP)
- Veritas Volume Manager (VxVM)
- Veritas File System (VxFS)
- Symantec Storage Foundation (SF)
- Symantec Cluster Server (VCS)
- Symantec Storage Foundation and High Availability (SFHA)
- Symantec Storage Foundation Cluster File System and High Availability (SFCFSHA)
- Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)
- Symantec Storage Foundation for Sybase ASE CE (SFSYBASECE)

- Symantec ApplicationHA (ApplicationHA)

Note: SFSYBASECE is supported on RHEL6. See *Section 2: Installing and configuring SFSYBASECE on RHEL 6* for more information.

You can install or upgrade to the patches included in this release by using the `installmr` script. For information on the various options that you can use with the script:

The release supports the following installation and upgrade scenarios:

Table 1-1 Supported installation and upgrade scenarios

| Scenario | Install and upgrade process |
|--|--|
| No product is installed on the target system | Run <code>installmr</code> with <code>-base_path</code> option to install 6.2.1 |
| The product version before 6.2 is installed on the target system | Run <code>installmr</code> with <code>-base_path</code> option to upgrade to 6.2.1 |
| The product version 6.2 is installed on the target system | Run <code>installmr</code> to upgrade to 6.2.1 |

To install or upgrade the product to 6.2.1 from releases before 6.2, invoke the `installmr` script with `-base_path` option to install or upgrade to 6.2.1.

For installation:

```
./installmr -base_path /tmp/sfha6.2/
```

For upgrade:

```
./installmr -base_path /tmp/sfha6.2/ -upgrade
```

For more information regarding installing 6.2.1 using Install Bundles feature:

See *Using Install Bundles to simultaneously install or upgrade base releases, maintenance patches, and hot fixes* in 6.2 Installation Guides.

Symantec strongly recommends you to use the Install Bundles feature to install or upgrade Symantec Storage Foundation and High Availability Solutions 6.2.1.

Supported operating systems and database software

For information on supported operating systems and database software, see the *Symantec™ Storage Foundation and High Availability Solutions 6.2.1 Release Notes - Linux*.

Installing the products for the first time

This chapter includes the following topics:

- [Supported types of Installation](#)
- [Installing the Symantec software using the Install Bundles feature](#)

Supported types of Installation

SFHA Solutions 6.2.1 supports the following types of Installation:

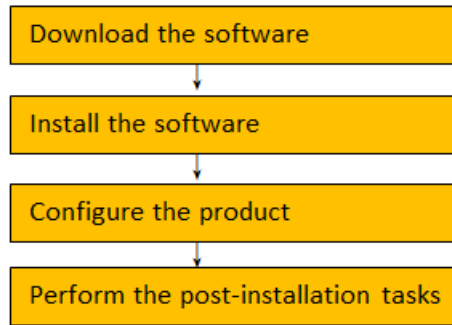
- Installing Symantec products with the script-based installer

Note: Symantec recommends you to install 6.2.1 with Install Bundles.

Installing the Symantec software using the Install Bundles feature

This section describes how to install a Symantec Storage Foundation and High Availability Solutions product of 6.2 and 6.2.1 using the Install Bundles feature in one step.

Figure 2-1 Install flow of SFHA Solutions



To install the Symantec software 6.2.1 using Install Bundles:

- 1 Download Storage Foundation and High Availability Solutions 6.2 from <http://fileConnect.symantec.com>.
 - 2 Extract the tar ball into the `/tmp/sfha6.2/` directory.
 - 3 Download SFHA Solutions 6.2.1 from <https://sort.symantec.com/patches>.
 - 4 Extract it to the `/tmp/sfha6.2.1` directory.
 - 5 Change to the `/tmp/sfha6.2.1` directory by entering:

```
# cd /tmp/sfha6.2.1
```
 - 6 Invoke the `installmr` script with `-base_path` option to install 6.2 and 6.2.1.
Enter:

```
./installmr -base_path /tmp/sfha6.2/
```
 - 7 In the Task Menu, enter `i` to install a product.
- See the 6.2 Installation Guide for configuration steps.

Upgrading to 6.2.1 from releases earlier than 6.2

This chapter includes the following topics:

- [Planning to upgrade to SFHA Solutions 6.2.1](#)
- [Performing a full upgrade with Install Bundles](#)
- [Performing a phased upgrade using Install Bundles](#)
- [Performing a rolling upgrade using Install Bundles](#)
- [Performing an automated upgrade using response files with Install Bundles](#)

Planning to upgrade to SFHA Solutions 6.2.1

This section includes the following topics:

- [Supported upgrade paths for SFHA Solutions 6.2.1](#)
- [About using the installer to upgrade from releases earlier than 6.2 when the root disk is encapsulated](#)
- [Preparing to upgrade Volume Replicator](#)
- [Downloading SFHA Solutions 6.2.1](#)

Supported upgrade types for SFHA Solutions 6.2.1

SFHA Solutions supports various ways of upgrading your cluster to the latest version. Choose a method that best suits your environment and supports your planned upgrade path.

[Table 3-1](#) lists the supported types of upgrade.

Table 3-1 Supported types of upgrade

| Type of upgrade | Abstract |
|-----------------|---|
| Full upgrade | A full upgrade involves upgrading all the nodes in the cluster at the same time. All components are upgraded during the process. The cluster remains unavailable for the duration of the upgrade. |
| Online upgrade | The online upgrade involves upgrading the whole cluster and supporting customer's application zero down time during the upgrade procedure. Now it only support VCS and ApplicationHA. |
| Phased upgrade | The phased upgrade methodology involves upgrading half of the nodes in the cluster at a time. |
| Rolling upgrade | The rolling upgrade minimizes downtime for highly available clusters to the amount of time that it takes to perform a service group failover. |

Supported upgrade paths for SFHA Solutions 6.2.1

You can run the `installmr` script with Install Bundles to upgrade SFHA Solutions to 6.2.1.

For information on operating systems that are supported for 6.2.1, see *System requirements* in *Symantec™ Storage Foundation and High Availability Solutions 6.2.1 Release Notes*.

The following tables describe upgrading to 6.2.1.

Table 3-2 RHEL 6 x64 upgrades

| Symantec product versions | RHEL 5 | RHEL 6 |
|---------------------------|----------------|--------|
| 5.1 | Not supported. | N/A |
| 5.1 RPs | | |
| 5.1 PR1 | | |
| 5.1 SP1 | | |
| 5.1 SP1 RP1 | | |

Table 3-2 RHEL 6 x64 upgrades (*continued*)

| Symantec product versions | RHEL 5 | RHEL 6 |
|--|----------------|---|
| 5.1 SP1 PR2 | N/A | Upgrade OS to RHEL 6 U4 or above. Upgrade the product to 6.2.1 using the <code>installmr</code> script with Install Bundles. |
| 5.1 SP1 PR3 5.1 SP1 RP2 5.1 SP1 RP3 6.0 6.0 RP1 6.0.1 6.0.2 6.0.3 | Not supported. | Upgrade OS to RHEL 6 U4 or above. Upgrade the product to 6.2.1 using the <code>installmr</code> script with Install Bundles. |
| 5.1 SP1 RP4 6.0.5 6.1 6.1.1 | Not supported. | Upgrade to 6.2.1 using the <code>installmr</code> script with Install Bundles. |
| 6.2 | N/A | Upgrade to 6.2.1 using the <code>installmr</code> script. |

Table 3-3 RHEL 7 x64 upgrades

| Symantec product versions | RHEL 5 | RHEL 6 | RHEL 7 |
|---------------------------|--------|----------------|--------|
| 5.1 SP1 PR2 | N/A | Not supported. | N/A |

Table 3-3 RHEL 7 x64 upgrades (*continued*)

| Symantec product versions | RHEL 5 | RHEL 6 | RHEL 7 |
|---------------------------|----------------|----------------|---|
| 5.1 SP1 PR3 | Not supported. | Not supported. | N/A |
| 5.1 SP1 RP2 | | | |
| 5.1 SP1 RP3 | | | |
| 5.1 SP1 RP4 | | | |
| 6.0 | | | |
| 6.0 RP1 | | | |
| 6.0.1 | | | |
| 6.0.2 | | | |
| 6.0.3 | | | |
| 6.0.5 | | | |
| 6.1 | | | |
| 6.1.1 | | | |
| 6.2 | N/A | Not supported. | Upgrade to 6.2.1 using the <code>installmr</code> script. |

Table 3-4 OL 6 x64 (RHEL Compatible mode) upgrades

| Symantec product versions | OL 5 (RHEL Compatible mode) | OL 6 (RHEL Compatible mode) |
|---------------------------|-----------------------------|--|
| 5.1 | Not supported. | N/A |
| 5.1 RPs | | |
| 5.1 PR1 | | |
| 5.1 SP1 | | |
| 5.1 SP1 RP1 | | |
| 5.1 SP1 PR2 | N/A | Upgrade OS to OL6 U4 or above. Upgrade to 6.2.1 using the <code>installmr</code> script with Install Bundles. |

Table 3-4 OL 6 x64 (RHEL Compatible mode) upgrades (*continued*)

| Symantec product versions | OL 5 (RHEL Compatible mode) | OL 6 (RHEL Compatible mode) |
|--|-----------------------------|--|
| 5.1 SP1 PR3 5.1 SP1 RP2 5.1 SP1 RP3 6.0 6.0 RP1 6.0.1 6.0.2 6.0.3 | Not supported. | Upgrade OS to OL6 U4 or above. Upgrade to 6.2.1 using the <code>installmr</code> script with Install Bundles. |
| 5.1 SP1 RP4 6.0.5 6.1 6.1.1 | Not supported. | Upgrade to 6.2.1 using the <code>installmr</code> script with Install Bundles. |
| 6.2 | N/A | Upgrade to 6.2.1 using the <code>installmr</code> script. |

Table 3-5 OL 7 x64 (RHEL Compatible mode) upgrades

| Symantec product versions | OL 5 (RHEL Compatible mode) | OL 6 (RHEL Compatible mode) | OL 7 (RHEL Compatible mode) |
|---|-----------------------------|-----------------------------|-----------------------------|
| 5.1 5.1 RPs 5.1 PR1 5.1 SP1 5.1 SP1 RP1 | Not supported. | Not supported. | Not supported. |
| 5.1 SP1 PR2 | Not supported. | Not supported. | Not supported. |

Table 3-5 OL 7 x64 (RHEL Compatible mode) upgrades (*continued*)

| Symantec product versions | OL 5 (RHEL Compatible mode) | OL 6 (RHEL Compatible mode) | OL 7(RHEL Compatible mode) |
|---|-----------------------------|-----------------------------|---|
| 5.1 SP1 PR3 5.1 SP1 RP2 5.1 SP1 RP3 5.1 SP1 RP4 6.0 6.0 RP1 6.0.1 6.0.2 6.0.3 | Not supported. | Not supported. | Not supported. |
| 6.0.5 6.1 6.1.1 | Not supported. | Not supported. | N/A |
| 6.2 | Not supported. | Not supported. | Upgrade to 6.2.1 using the <code>installmr</code> script. |

Table 3-6 OL6 x64 (UEK) upgrades

| Symantec product versions | OL6 (UEK) |
|---------------------------|--|
| 6.0.4 | Upgrade to 6.2.1 using the <code>installmr</code> script with Install Bundles. |
| 6.0.5 | Upgrade to 6.2.1 using the <code>installmr</code> script with Install Bundles. |
| 6.2 | Upgrade to 6.2.1 using the <code>installmr</code> script. |

Note: Only VCS supports OL UEK.

Table 3-7 SLES 11 x64 upgrades

| Symantec product versions | SLES 11 |
|--|---|
| 5.1 5.1 RPs 5.1 P1 5.1 SP1 5.1 SP1 RPs 5.1 SP1 PR1 (VCS only) 5.1 SP1 PR4 (VCS only) | Upgrade OS to SLES11 SP2 or above. Use the <code>installmr</code> script with Install Bundles to upgrade the product to 6.2.1. |
| 6.0 6.0 RP1 | Upgrade OS to SLES11 SP2 or above. Use the <code>installmr</code> script with Install Bundles to upgrade the product to 6.2.1. |
| 6.0.1 6.0.2 6.0.3 6.0.5 6.0.4 6.1 6.1.1 | Use the <code>installmr</code> script with Install Bundles to upgrade the product to 6.2.1. |
| 6.2 | Use the <code>installmr</code> script to upgrade the product to 6.2.1. |

About using the installer to upgrade from releases earlier than 6.2 when the root disk is encapsulated

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

Table 3-8 Upgrading using the installer from releases earlier than 6.2 when the root disk is encapsulated

| Starting version | Ending version | Action required |
|---|----------------|--|
| 5.1 5.1 RP1 5.1 RP2 5.1 PR1 | 6.2.1 | Do not unencapsulate. The installer runs normally. Reboot after upgrade. |
| 5.1 SP1 5.1 SP1 RP1 5.1 SP1 RP2 5.1 SP1 RP3 5.1 SP1 RP4 5.1 SP1 PR2 5.1 SP1 PR3 | 6.2.1 | Do not unencapsulate. The installer runs normally. Reboot after upgrade. |
| 6.0 6.0 RP1 | 6.2.1 | Do not unencapsulate. The installer runs normally. Reboot after upgrade. |
| 6.0.1 6.0.2 6.0.3 6.0.4 6.0.5 | 6.2.1 | Do not unencapsulate. The installer runs normally. Reboot after upgrade. |

Note: On RHEL6, only for 5.1 SP1 RP4 ,6.0.1, and later, do not unencapsulate. For other releases on RHEL6, you need to unencapsulate.

Preparing to upgrade Volume Replicator

Before installing or upgrading Volume Replicator (VVR):

- Confirm that your system has enough free disk space to install VVR.
- Make sure you have root permissions. You must have root permissions to perform the install and upgrade procedures.
- If replication using VVR is configured, Symantec recommends that the disk group version is at least 110 prior to upgrading.

You can check the Disk Group version using the following command:

```
# vxdg list diskgroup
```

- If replication using VVR is configured, make sure the size of the SRL volume is greater than 110 MB.
Refer to the *Symantec™ Storage Foundation and High Availability Solutions Replication Administrator's Guide*.
- If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date on all the hosts.

```
# /usr/sbin/vxlink -g diskgroup status rlink_name
```

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

- If VCS is used to manage VVR replication, follow the preparation steps to upgrade VVR and VCS agents.

See the *Symantec™ Storage Foundation and High Availability Solutions Replication Administrator's Guide* for more information.

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

Planning an upgrade from the previous VVR version

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

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

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

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in [Table 3-9](#), if either the Primary or Secondary are running a version of VVR prior to 6.2.1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 6.2.1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

Table 3-9 VVR versions and checksum calculations

| VVR prior to 6.2.1 (DG version <= 140) | VVR 6.2.1 (DG version >= 150) | VVR calculates checksum TCP connections? |
|---|----------------------------------|---|
| Primary | Secondary | Yes |
| Secondary | Primary | Yes |
| Primary and Secondary | | Yes |
| | Primary and Secondary | No |

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

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

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

Downloading SFHA Solutions 6.2.1

The following procedure describes how to upgrade to 6.2.1 with Install Bundles from releases earlier than 6.2.

Note: If you are upgrading from releases earlier than 6.2, Symantec suggests you upgrade with Install Bundles.

- 1 Download Storage Foundation and High Availability Solutions 6.2 from <http://fileConnect.symantec.com>.
- 2 Extract the tar ball into a directory called /tmp/sfha6.2

- 3 Download SFHA Solutions 6.2.1 from <https://sort.symantec.com/patches>.
- 4 Extract it to a directory called /tmp/sfha6.2.1

Performing a full upgrade with Install Bundles

- [Performing a full upgrade of VCS using Install Bundles](#)
- [Performing a full upgrade of SFHA using Install Bundles](#)
- [Performing a full upgrade of SFCFSHA using Install Bundles](#)
- [Performing a full upgrade of SF Oracle RAC using Install Bundles](#)

Performing a full upgrade of VCS using Install Bundles

You can use the installer to upgrade VCS.

To upgrade VCS using the product installer

- 1 Log in as superuser.
- 2 Change to the /tmp/sfha6.2.1 directory.
- 3 Invoke the `installmr` script with `-base_path` option to upgrade to 6.2.1:

```
# ./installmr -base_path /tmp/sfha6.2/
```
- 4 From the opening Selection Menu, choose: **G** for "Upgrade a Product."
- 5 Choose **1** for Full Upgrade.
- 6 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.
- 7 When the verification checks are complete, the installer asks if you agree with the terms of the End User License Agreement. Press **y** to agree and continue.
The installer lists the RPMs to upgrade.

- 8 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 9 The installer asks if you want to stop VCS processes. Press the Enter key to continue.

The installer stops VCS processes, uninstalls RPMs, installs or upgrades RPMs, configures, and startsVCS.

The installer lists the nodes that Symantec recommends you to restart, if needed.

- 10 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.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

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

Performing a full upgrade of SFHA using Install Bundles

This section describes how to perform a full upgrade of SFHA using Install Bundles.

- [Upgrading SFHA using with Install Bundles](#)

Upgrading SFHA using with Install Bundles

Use this procedure to upgrade SFHA with Install Bundles.

Note: The installer doesn't support upgrading with Install Bundles when the boot disk is encapsulated. If the boot disk is encapsulated, you need to un-encapsulate the boot disk first, and then run Install Bundles to perform upgrade.

To upgrade SFHA from previous versions to 6.2.1

- 1 Log in as superuser.
- 2 Use the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# df -T | grep vxfs
```

- 3 Unmount all Storage Checkpoints and file systems:

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

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

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

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

Perform the following steps in the order listed:

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

```
# fsck -t vxfs raw_device  
# mount -t vxfs block_device mountpoint  
# umount /mountpoint
```

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

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

```
file system device busy
```

You know for certain that an extended operation is pending if the following message is generated on the console:

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

- If an extended operation is pending, you must leave the file system mounted for a longer time to allow the operation to complete. Removing a very large RPM clone can take several hours.
 - Repeat this step to verify that the unclean file system is now clean.
- 5 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.
 - 6 Stop all the volumes by entering the following command for each disk group:

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

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

```
# vxprint -Aht -e v_open
```
 - 7 Make a record of the mount points for VxFS file systems and VxVM volumes that are defined in the `/etc/fstab` file. You will need to recreate these entries in the `/etc/fstab` file on the freshly installed system.
 - 8 Perform any necessary preinstallation checks.
 - 9 To invoke the installer, run the `installmr` command as shown in this example:

```
# cd /tmp/sfha6.2.1  
# ./installmr -base_path /tmp/sfha6.2/
```
 - 10 Enter `g` to upgrade and press Return.

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

```
Enter the 64 bit <platform> system names separated  
by spaces : [q, ?] host1 host2
```

where <platform> is the platform on which the system runs, such as RHEL5.

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

During the system verification phase, the installer checks if the boot disk is encapsulated and the upgrade's path. If the upgrade is not supported, you need to un-encapsulate the boot disk.

- 12 The installer asks if you agree with the terms of the End User License Agreement. Press **y** to agree and continue.
- 13 The installer lists the RPMs to upgrade.
- 14 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to/  
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 15 The installer asks if you want to stop SFHA processes, enter **y** to continue.

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

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

- 16 The installer stops, uninstalls, reinstalls, and starts specified RPMs.
- 17 If necessary, reinstate any missing mount points in the `/etc/fstab` file on each node that you recorded in step 7.
- 18 Restart all the volumes by entering the following command for each disk group:

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

- 19 Remount all VxFS file systems and Storage Checkpoints on all nodes:

```
# mount /filesystem  
# mount /checkpoint_name
```

- 20 You can perform the following optional configuration steps:
 - If you want to use features of Symantec Storage Foundation 6.2.1 for which you do not currently have an appropriate license installed, obtain the license and run the `vxlicinst` command to add it to your system.
 - To upgrade VxFS Disk Layout versions and VxVM Disk Group versions, follow the upgrade instructions.
- 21 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

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

Performing a full upgrade of SFCFSHA using Install Bundles

This section describes how to perform a full upgrade of SFCFSHA using Install Bundles.

- [Performing a full SFCFSHA upgrade with Install Bundles](#)

Performing a full SFCFSHA upgrade with Install Bundles

Performing a full upgrade involves the following tasks:

- Ensuring that the file systems are clean

- Performing the upgrade

Ensuring the file systems are clean

Before upgrading to SFCFSHA 6.2.1, ensure that the file systems are clean. To ensure that the logs have been replayed and the file systems are marked clean:

To ensure the file systems are clean

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

```
# hagrps -offline group -any
```

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

Repeat this step for each SFCFSHA service group.

Note: This unmounts the CFS file systems.

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

```
# umount /mount_point
```

- 4 Check and repair each VxFS file system:

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

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

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

Repeat this step for each file system.

Performing the upgrade

To perform the upgrade

- 1 Log in as superuser.
- 2 Change to the `/tmp/sfha6.2.1` directory:

```
# cd /tmp/sfha6.2.1
```

- 3 Change to the `/tmp/sfha6.2.1` directory. Invoke the `installmr` script with `-base_path` option to upgrade to 6.2.1:

```
# ./installmr -base_path /tmp/sfha6.2/
```

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

```
# mount -t vxfs
```

If any VxFS file systems are mounted, offline the group on each node of the cluster. For details, see step 2 and step 3 of [Ensuring the file systems are clean](#).

- 5 From the opening Selection Menu, choose: **G** for **Upgrade a Product**. Choose **1** for **Full Upgrade**.
- 6 You are prompted to enter the system names (in the following example, "node01" and "node02") on which the software is to be upgraded. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces on which to
install SFCFSHA: node01 node02
```

- 7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA). Press **y** to agree and continue.
- 8 During the initial system check, the installer verifies that communication between systems has been set up.

If the installer hangs or asks for a login password, setup passwordless ssh or setup rsh from the system that run `installmr` to the system that need to be upgraded to 6.2.1. Then run the installer again.

- 9 After you accept EULA and the system checks complete, the installer displays a list of the RPMs that will be upgraded. Press Enter to continue with the upgrade.

- 10 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 11 Output shows information that SFCFSHA must be stopped on a running system. Enter **y** to continue.
- 12 The installer stops, uninstalls, reinstalls, and starts specified RPMs.
- 13 Press **Enter** again for summary information about logs and reboots.

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

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

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

Performing a full upgrade of SF Oracle RAC using Install Bundles

This section describes how to perform a full upgrade of SF Oracle RAC using Install Bundles.

- [Preparing to perform a full upgrade to 6.2.1 on an SF Oracle RAC cluster](#)
- [Upgrading SF Oracle RAC and operating system \(minor OS upgrade\)](#)

Preparing to perform a full upgrade to 6.2.1 on an SF Oracle RAC cluster

Perform the preparatory steps in this section if you are performing a full upgrade of the cluster. Before you upgrade, make sure that your systems meet the hardware and software requirements for this release.

To prepare to upgrade SF Oracle RAC

- 1 Log in as superuser to one of the nodes in the cluster.
- 2 Back up the following configuration files on your system: `main.cf`, `types.cf`, `CVMTTypes.cf`, `CFSTypes.cf`, `OracleTypes.cf`, `OracleASMTTypes.cf`, `PrivNIC.cf`, `MultiPrivNIC.cf`, `CRSResource.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmode`

For example:

```
# cp /etc/VRTSvcs/conf/config/main.cf \  
/etc/VRTSvcs/conf/config/main.cf.save
```

- 3 Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.

If not, a warning message will be displayed after `installmr` upgrade prechecks.

Warning: Backup `/etc/vx/cbr/bk` directory.

- 4 Stop all applications that use VxFS or VxVM disk groups, whether local or CFS. If the applications are under VCS control:

```
# hagrps -offline grp_name -any
```

If the applications are not under VCS control:

Use native application commands to stop the application.

- 5 Stop all Oracle RAC resources.

- If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:

```
# hagrps -offline oracle_group -any
```

- If the database instances are not managed by VCS, then run the following on one node:

- For Oracle RAC 11g:

```
$ srvctl stop database -d db_name
```

- For Oracle RAC 12c:

```
$ srvctl stop database -db db_name
```

- 6 ■ If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts:

```
# haconf -makerw  
# hagrps -modify oracle_group AutoStart 0  
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to MANUAL:

- For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

- For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

- 7 Stop VCS on all nodes:

```
# hastop -all
```

- 8 Unmount the VxFS file system, which is not under VCS control.

```
# mount |grep vxfs  
  
# fuser -m /mount_point  
  
# umount /mount_point
```

Make sure that no processes are running which make use of mounted shared file system or shared volumes.

```
# fuser -cu /mount_point
```

- 9 If you plan to continue using the Storage Foundation for Databases (SFDB) tools, you must prepare to migrate the SFDB repository database before upgrading to 6.2.1.

See [“Pre-upgrade tasks for migrating the SFDB repository database”](#) on page 43.

- 10 If you plan to upgrade the operating system, stop all ports.

```
# /opt/VRTS/install/installsfrac -stop
```

Pre-upgrade tasks for migrating the SFDB repository database

Perform the following before upgrading SF Oracle RAC.

Note: The Sfua_Base repository resource group will be removed from the main.cf file. It is not required as a separate service group for SF Oracle RAC 6.2.1.

To prepare to migrate the repository database

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

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

Warning: The Database Flashsnap clone database will not be able to be carried over after upgrading. You must create a new Database Flashsnap clone database after upgrading to 6.2.1.

Upgrading SF Oracle RAC and operating system (minor OS upgrade)

This section provides instructions for SF Oracle RAC and minor operating system upgrade.

Perform the steps in the following procedure if you plan to perform a minor upgrade of the operating system, for example from SLES11 SP1 to SLES11 SP2, along with SF Oracle RAC.

- If required, upgrade the operating system.
- Upgrade to SF Oracle RAC 6.2.1.
- Bring the SF Oracle RAC online.

Upgrading the operating system

If you want to upgrade the operating system, perform the following steps:

- 1 Rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

- 2 Upgrade the operating system on all nodes in the cluster.

For instructions, see the operating system documentation.

Note: If reboot is required, use `shutdown -r now` command to reboot the nodes.

- 3 After the system restarts, restore the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

Upgrading SF Oracle RAC using Install Bundles

Use the `installmr` script-based installation programs to upgrade SF Oracle RAC.

The installer performs the following tasks to upgrade SF Oracle RAC:

- Verifies the compatibility of the systems before the upgrade.
- Stops the SF Oracle RAC processes before the upgrade.
- Uninstalls SF Oracle RAC.
- Installs the SF Oracle RAC 6.2 RPMs on the nodes.

- Installs the SF Oracle RAC 6.2.1 patches on the nodes.
- Starts the SF Oracle RAC processes after the upgrade.
- Displays the location of the log files, summary file, and response file.

To upgrade to SF Oracle RAC 6.2.1 using the installmr program

- 1 Log in as superuser.
- 2 Change to the `/tmp/sfha6.2.1` directory.
- 3 Invoke the `installmr` script with `-base_path` option to upgrade to 6.2.1:

```
# ./installmr -base_path /tmp/sfha6.2/
```

- 4 From the opening Selection Menu, choose: **G** for "Upgrade a Product."
- 5 Select 1 for **Full upgrade**.

The installer displays the copyright message and specifies the directory where the running logs are created.

The installer verifies the systems for compatibility.

Note: If `had` is stopped before upgrade, the installer displays the following warning:

VCS is not running before upgrade. Please make sure all the configurations are valid before upgrade.

If the configuration files are valid, you may ignore the message.

During the system verification phase, the installer checks if the boot disk is encapsulated and the upgrade path. If the upgrade is not supported, you need to un-encapsulate the boot disk.

Review the messages displayed and make sure that you meet the requirements before proceeding with the upgrade.

- 6 Press **Enter** to continue with the upgrade.

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

The installer displays the list of RPMs that will be uninstalled. Press **Enter** to view the list of RPMs that will be upgraded.

- 7 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 8 Enter **y** to stop the SF Oracle RAC processes.

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

The installer stops the processes and uninstalls SF Oracle RAC. After the uninstallation, the installer installs SF Oracle RAC 6.2.1 and starts 6.2.1 on all the nodes.

If the product is licensed with stale (old) key, the installer prompts users to update the key.

- 9 Relink the SF Oracle RAC libraries with Oracle:

The installer prompts a menu after upgrade. If you want the installer to relink the Oracle Database Binary, choose the option **Relink Oracle Database Binary** from the menu.

Complete the remaining tasks to finish the upgrade.

Bringing the Oracle database online

- 1 Bring the Oracle database service group online.

- If the Oracle database is managed by VCS:

```
# hagrps -online oracle_group -any
```

- If the Oracle database is not managed by VCS:

- For Oracle RAC 11g:

```
# srvctl start database -d db_name
```

- For Oracle RAC 12c:

```
# srvctl start database -db db_name
```

2 Start all applications that are not managed by VCS. Use native application commands to start the applications.

- 3 ■ If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrps -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:

- For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

- For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

4 Complete other post-upgrade steps.

For instructions, see the chapter *Performing post-upgrade tasks* in *Symantec™ Storage Foundation for Oracle RAC 6.2 Installation and Configuration Guide*.

5 If you want to upgrade all application clusters to version 6.2.1, make sure that you upgraded CP server systems that use VCS or SFHA to 6.2.1. Then, upgrade all application clusters to version 6.2.1.

For instructions to upgrade VCS or SFHA on the CP server systems, see the 6.2 VCS or SFHA installation guide.

Performing a phased upgrade using Install Bundles

This section explains how to perform a phased upgrade of SFHA Solutions on four nodes with four service groups. Note that in this scenario, SFHA Solutions 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.

- [Performing a phased VCS upgrade using Install Bundles](#)
- [Performing a phased SFHA upgrade using Install Bundles](#)
- [Performing a phased SFCFSA upgrade using Install Bundles](#)
- [Performing a phased SF Oracle RAC upgrade using Install Bundles](#)

Performing a phased VCS upgrade using Install Bundles

You can perform a phased VCS upgrade with the following steps:

- 1 Moving the service groups to the second subcluster.
See [“Moving the service groups to the second subcluster”](#) on page 48.
- 2 Upgrading the operating system on the first subcluster.
See [“Upgrading the operating system on the first subcluster”](#) on page 52.
- 3 Upgrading the first subcluster.
See [“Upgrading the first subcluster”](#) on page 52.
- 4 Preparing the second subcluster.
See [“Preparing the second subcluster”](#) on page 54.
- 5 Activating the first subcluster.
See [“Activating the first subcluster”](#) on page 57.
- 6 Upgrading the operating system on the second subcluster.
See [“Upgrading the operating system on the second subcluster”](#) on page 59.
- 7 Upgrading the second subcluster.
See [“Upgrading the second subcluster”](#) on page 59.
- 8 Finishing the phased upgrade.
See [“Finishing the phased upgrade”](#) on page 60.

Moving the service groups to the second subcluster

Perform the following steps to establish the service group's status and to switch the service groups.

To move service groups to the second subcluster

- 1 On the first subcluster, determine where the service groups are online.

```
# hagrps -state
```

The output resembles:

```
#Group   Attribute System Value
sg1      State     node01 | ONLINE |
sg1      State     node02 | ONLINE |
sg1      State     node03 | ONLINE |
sg1      State     node04 | ONLINE |
sg2      State     node01 | ONLINE |
sg2      State     node02 | ONLINE |
sg2      State     node03 | ONLINE |
sg2      State     node04 | ONLINE |
sg3      State     node01 | ONLINE |
sg3      State     node02 | OFFLINE |
sg3      State     node03 | OFFLINE |
sg3      State     node04 | OFFLINE |
sg4      State     node01 | OFFLINE |
sg4      State     node02 | ONLINE |
sg4      State     node03 | OFFLINE |
sg4      State     node04 | OFFLINE |
```

- 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). For SFHA, vxfen sg is the parallel service group.

```
# hagrps -offline sg1 -sys node01
# hagrps -offline sg2 -sys node01
# hagrps -offline sg1 -sys node02
# hagrps -offline sg2 -sys node02
# hagrps -switch sg3 -to node03
# hagrps -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:

```
# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/sda1                26G   3.3G   22G   14% /
udev                   1007M   352K 1006M    1% /dev
tmpfs                   4.0K     0   4.0K    0% /dev/vx
/dev/vx/dsk/dg2/dg2vol1
                        3.0G   18M   2.8G    1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2
                        1.0G   18M   944M    2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3
                        10G   20M   9.4G    1% /mnt/dg2/dg2vol3
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

- 4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

- 5 Freeze the nodes in the first subcluster.

```
# hasys -freeze -persistent node01
# hasys -freeze -persistent node02
```

- 6 Dump the configuration and make it read-only.

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

- 7 Verify that the service groups are offline on the first subcluster that you want to upgrade.

```
# hagrps -state
```

Output resembles:

```
#Group Attribute System Value
sg1 State node01 |OFFLINE|
sg1 State node02 |OFFLINE|
sg1 State node03 |ONLINE|
sg1 State node04 |ONLINE|
sg2 State node01 |OFFLINE|
sg2 State node02 |OFFLINE|
sg2 State node03 |ONLINE|
sg2 State node04 |ONLINE|
sg3 State node01 |OFFLINE|
sg3 State node02 |OFFLINE|
sg3 State node03 |ONLINE|
sg3 State node04 |OFFLINE|
sg4 State node01 |OFFLINE|
sg4 State node02 |OFFLINE|
sg4 State node03 |OFFLINE|
sg4 State node04 |ONLINE|
```

- 8 Backup 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
/var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
/var/VRTSat/.VRTSat/profile/certstore
/var/VRTSat/ABAuthSource
/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.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting `LLT_START = 0`.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the first subcluster

Perform the following procedure to upgrade the first subcluster (node01 and node02).

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 Start the `installmr` program, specify the nodes in the first subcluster (node01 and node02).

```
# cd /tmp/sfha6.2.1
```

```
# ./installmr -base_path /tmp/sfha6.2/ node01 node02
```

The program starts with a copyright message and specifies the directory where it creates the logs.

- 4 From the opening Selection Menu, choose: G for **Upgrade a Product**.
- 5 From the following menu, choose: 1 for **Full Upgrade**.

- 1) Full Upgrade
- 2) Rolling Upgrade
- b) Back to previous menu

```
Select the way by which you want to upgrade product: [1-2,b,q] (1)
```

- 6 The installer performs a series of checks and tests to ensure communications, licensing, and compatibility.

- 7 Enter **y** to agree to the End User License Agreement (EULA).
- 8 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 9 The installer displays the list of RPMs that get removed, installed, or upgraded on the selected systems.
- 10 The installer ends for the first subcluster with the following output:

```
Configuring VCS: 100%
```

```
Estimated time remaining: 0:00
```

```
Performing VCS upgrade configuration ..... Done
```

```
Symantec Cluster Server Configure completed successfully
```

```
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 Preparing the second subcluster  
procedure.
```

Preparing the second subcluster

Perform the following steps on the second subcluster before rebooting nodes in the first subcluster.

To prepare to upgrade the second subcluster

1 Get the summary of the status of your resources.

```
# hastatus -sum
-- 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 -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/sda1                  26G   3.3G   22G   14% /
udev                      1007M 352K 1006M   1% /dev
tmpfs                     4.0K    0   4.0K   0% /dev/vx
/dev/vx/dsk/dg2/dg2vol1   3.0G   18M   2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2   1.0G   18M   944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3   10G   20M   9.4G   1% /mnt/dg2/dg2vol3

# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

- 3 Make the configuration writable on the second subcluster.

```
# haconf -makerw
```

- 4 Unfreeze the service groups.

```
# hagrps -unfreeze sg1 -persistent
# hagrps -unfreeze sg2 -persistent
# hagrps -unfreeze sg3 -persistent
# hagrps -unfreeze sg4 -persistent
```

- 5 Dump the configuration and make it read-only.

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

- 6 Take the service groups offline on node03 and node04.

```
# hagrps -offline sg1 -sys node03
# hagrps -offline sg1 -sys node04
# hagrps -offline sg2 -sys node03
# hagrps -offline sg2 -sys node04
# hagrps -offline sg3 -sys node03
# hagrps -offline sg4 -sys node04
```


7 Verify the state of the service groups.

```
# hagrps -state
#Group      Attribute  System  Value
sg1         State     node01  |OFFLINE|
sg1         State     node02  |OFFLINE|
sg1         State     node03  |OFFLINE|
sg1         State     node04  |OFFLINE|
sg2         State     node01  |OFFLINE|
sg2         State     node02  |OFFLINE|
sg2         State     node03  |OFFLINE|
sg2         State     node04  |OFFLINE|
sg3         State     node01  |OFFLINE|
sg3         State     node02  |OFFLINE|
sg3         State     node03  |OFFLINE|
sg3         State     node04  |OFFLINE|
```

8 Stop VCS, I/O Fencing, GAB, and LLT on node03 and node04.

```
# hystop -local
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

9 Make sure that the VXFEN, GAB, and LLT modules on node03 and node04 are not added.

```
# /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
```

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 [Preparing the second subcluster](#).

To activate the first subcluster

- 1 Start LLT and GAB.

```
# /etc/init.d/llt start  
# /etc/init.d/gab start
```

- 2 Seed node01 and node02 in the first subcluster.

```
# gabconfig -x
```

- 3 On the first half of the cluster, start VCS:

```
# cd /opt/VRTS/install  
# ./installvcs<version> -start node01 node02
```

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

- 4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

- 5 Unfreeze the nodes in the first subcluster.

```
# hasys -unfreeze -persistent node01  
# hasys -unfreeze -persistent node02
```

- 6 Unfreeze service groups in the first subcluster.

```
# hagrps -unfreeze sg1 -persistent  
# hagrps -unfreeze sg2 -persistent
```

- 7 Dump the configuration and make it read-only.

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

- 8 Bring the service groups online on node01 and node02.

```
# hagrps -online sg1 -sys node01  
# hagrps -online sg1 -sys node02  
# hagrps -online sg2 -sys node01  
# hagrps -online sg2 -sys node02  
# hagrps -online sg3 -sys node01  
# hagrps -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.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting `LLT_START = 0`.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the second subcluster

Perform the following procedure to upgrade the second subcluster (node03 and node04).

To start the installer to upgrade the second subcluster

- 1 Confirm that you are logged on as the superuser and you mounted the product disc.
- 2 Navigate to the folder that contains the SFHA Solutions 6.2.1 binary.

```
# cd /tmp/sfha6.2.1
```

- 3 Confirm that VCS is stopped on node03 and node04. Specify the nodes in the second subcluster (node03 and node04).

```
# ./installmr -base_path /tmp/sfha6.2/ node03 node04
```

The program starts with a copyright message and specifies the directory where it creates the logs.

- 4 From the opening Selection Menu, choose: G for **Upgrade a Product**.
- 5 From the following menu, choose: 1 for **Full Upgrade**.

- 1) Full Upgrade
- 2) Rolling Upgrade
- b) Back to previous menu

```
Select the way by which you want to upgrade product: [1-2,b,q] (1)
```

- 6 The installer performs a series of checks and tests to ensure communications, licensing, and compatibility.

- 7 Enter **y** to agree to the End User License Agreement (EULA).
- 8 The installer displays the list of RPMs that get removed, installed, or upgraded on the selected systems.
- 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 node01 [node02 ...]
```

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

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

- 2 On the second half of the cluster, start VCS:

```
# cd /opt/VRTS/install  
  
# ./installvcs<version> -start node03 node04
```

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

3 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
```

4 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
```

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 and node02.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

Performing a phased SFHA upgrade using Install Bundles

You can perform a phased upgrade from any supported SFHA versions to SFHA 6.2.1.

Performing a phased upgrade involves the following tasks:

- 1 Moving the service groups to the second subcluster.
See [“Moving the service groups to the second subcluster”](#) on page 63.
- 2 Upgrading the operating system on the first subcluster.
See [“Upgrading the operating system on the first subcluster”](#) on page 67.
- 3 Upgrading the first subcluster.
See [“Upgrading the first subcluster”](#) on page 67.
- 4 Preparing the second subcluster.
See [“Preparing the second subcluster”](#) on page 68.
- 5 Activating the first subcluster.
See [“Activating the first subcluster”](#) on page 71.
- 6 Upgrading the operating system on the second subcluster.
See [“Upgrading the operating system on the second subcluster”](#) on page 73.

- 7 Upgrading the second subcluster.
See [“Upgrading the second subcluster”](#) on page 73.
- 8 Finishing the phased upgrade.
See [“Finishing the phased upgrade”](#) on page 74.

Moving the service groups to the second subcluster

Perform the following steps to establish the service group's status and to switch the service groups.

To move service groups to the second subcluster

- 1 On the first subcluster, determine where the service groups are online.

```
# hagrps -state
```

The output resembles:

```
#Group   Attribute System Value
sg1      State     node01 | ONLINE |
sg1      State     node02 | ONLINE |
sg1      State     node03 | ONLINE |
sg1      State     node04 | ONLINE |
sg2      State     node01 | ONLINE |
sg2      State     node02 | ONLINE |
sg2      State     node03 | ONLINE |
sg2      State     node04 | ONLINE |
sg3      State     node01 | ONLINE |
sg3      State     node02 | OFFLINE |
sg3      State     node03 | OFFLINE |
sg3      State     node04 | OFFLINE |
sg4      State     node01 | OFFLINE |
sg4      State     node02 | ONLINE |
sg4      State     node03 | OFFLINE |
sg4      State     node04 | OFFLINE |
```

- 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). For SFHA, vxfs sg is the parallel service group.

```
# hagrps -offline sg1 -sys node01
# hagrps -offline sg2 -sys node01
# hagrps -offline sg1 -sys node02
# hagrps -offline sg2 -sys node02
# hagrps -switch sg3 -to node03
# hagrps -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:

```
# df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/sda1                  26G   3.3G   22G   14% /
udev                      1007M 352K 1006M   1% /dev
tmpfs                     4.0K   0   4.0K   0% /dev/vx
/dev/vx/dsk/dg2/dg2vol1   3.0G   18M   2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2   1.0G   18M   944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3   10G   20M   9.4G   1% /mnt/dg2/dg2vol3
# 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.

```
# haconf -makerw
```

- 6 Freeze the nodes in the first subcluster.

```
# hasys -freeze -persistent node01
# hasys -freeze -persistent node02
```

- 7 Dump the configuration and make it read-only.

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

- 8 Verify that the service groups are offline on the first subcluster that you want to upgrade.

```
# hagrps -state
```

Output resembles:

```
#Group Attribute System Value
sg1 State node01 |OFFLINE|
sg1 State node02 |OFFLINE|
sg1 State node03 |ONLINE|
sg1 State node04 |ONLINE|
sg2 State node01 |OFFLINE|
sg2 State node02 |OFFLINE|
sg2 State node03 |ONLINE|
sg2 State node04 |ONLINE|
sg3 State node01 |OFFLINE|
sg3 State node02 |OFFLINE|
sg3 State node03 |ONLINE|
sg3 State node04 |OFFLINE|
sg4 State node01 |OFFLINE|
sg4 State node02 |OFFLINE|
sg4 State node03 |OFFLINE|
sg4 State node04 |ONLINE|
```

- 9 Back up the llttab, llthosts, gabtab, types.cf, main.cf and AT configuration files on the first subcluster.

```
# cp /etc/llttab /etc/llttab.bkp
# cp /etc/llthosts /etc/llthosts.bkp
# cp /etc/gabtab /etc/gabtab.bkp
# cp /etc/VRTSvcs/conf/config/main.cf \
  /etc/VRTSvcs/conf/config/main.cf.bkp
# cp /etc/VRTSvcs/conf/config/types.cf \
  /etc/VRTSvcs/conf/config/types.cf.bkp
# /opt/VRTSat/bin/vssat showbackuplist
B|/var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
B|/var/VRTSat/.VRTSat/profile/certstore
B|/var/VRTSat/ABAuthSource
B|/etc/vx/vss/VRTSat.conf
Quiescing ...
Snapshot Directory :/var/VRTSatSnapshot
```

Upgrading the operating system on the first subcluster

You can perform the operating system upgrade on the first subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting `LLT_START = 0`.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the first subcluster

After step 1 and step 2, you now navigate to the installer program and start it.

To start the installer for the phased upgrade

- 1 Confirm that you are logged on as the superuser and you mounted the product disc.
- 2 Navigate to the folder that contains the SFHA Solutions 6.2.1 binary.

```
# cd /tmp/sfha6.2.1.
```

- 3 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.
- 4 Start the `installmr` program, specify the nodes in the first subcluster (node01 and node02).

```
# ./installmr -base_path /tmp/sfha6.2/ node01 node02
```

The program starts with a copyright message and specifies the directory where it creates the logs. It performs a system verification and outputs upgrade information.

- 5 From the opening Selection Menu, choose: G for **Upgrade a Product**.
- 6 From the following menu, choose: 1 for **Full Upgrade**.

- 1) Full Upgrade
- 2) Rolling Upgrade
- b) Back to previous menu

Select the way by which you want to upgrade product: [1-2,b,q] (1)

- 7 Enter **y** to agree to the End User License Agreement (EULA).
- 8 The installer displays the list of RPMs that get removed, installed, and upgraded on the selected systems.
- 9 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 10 When you are prompted, reply **y** to stop appropriate processes.

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

The installer stops processes, uninstalls RPMs, and installs RPMs.

The upgrade is finished on the first subcluster. Do not reboot the nodes in the first subcluster until you complete the [Upgrading the second subcluster](#) procedure.

Preparing the second subcluster

Perform the following steps on the second subcluster before rebooting nodes in the first subcluster.

To prepare to upgrade the second subcluster

1 Get the summary of the status of your resources.

```
# hastatus -sum
-- 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 -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/sda1                  26G   3.3G   22G   14% /
udev                      1007M 352K 1006M   1% /dev
tmpfs                      4.0K    0   4.0K   0% /dev/vx
/dev/vx/dsk/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol1   3.0G   18M   2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol2   1.0G   18M   944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3
/dev/vx/dsk/dg2/dg2vol3   10G   20M   9.4G   1% /mnt/dg2/dg2vol3

# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

- 3 Make the configuration writable on the second subcluster.

```
# haconf -makerw
```

- 4 Unfreeze the service groups.

```
# hagrps -unfreeze sg1 -persistent
# hagrps -unfreeze sg2 -persistent
# hagrps -unfreeze sg3 -persistent
# hagrps -unfreeze sg4 -persistent
```

- 5 Dump the configuration and make it read-only.

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

- 6 Take the service groups offline on node03 and node04.

```
# hagrps -offline sg1 -sys node03
# hagrps -offline sg1 -sys node04
# hagrps -offline sg2 -sys node03
# hagrps -offline sg2 -sys node04
# hagrps -offline sg3 -sys node03
# hagrps -offline sg3 -sys node04
# hagrps -offline sg4 -sys node03
# hagrps -offline sg4 -sys node04
```

7 Verify the state of the service groups.

```
# hagrps -state
#Group      Attribute  System  Value
sg1         State     node01  |OFFLINE|
sg1         State     node02  |OFFLINE|
sg1         State     node03  |OFFLINE|
sg1         State     node04  |OFFLINE|
sg2         State     node01  |OFFLINE|
sg2         State     node02  |OFFLINE|
sg2         State     node03  |OFFLINE|
sg2         State     node04  |OFFLINE|
sg3         State     node01  |OFFLINE|
sg3         State     node02  |OFFLINE|
sg3         State     node03  |OFFLINE|
sg3         State     node04  |OFFLINE|
```

8 Stop all VxVM volumes (for each disk group) that VCS does not manage.

9 Stop VCS, I/O Fencing, GAB, and LLT on node03 and node04.

```
# hastop -local
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

10 Make sure that the VXFEN, GAB, and LLT modules on node03 and node04 are not added.

```
# /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
```

Activating the first subcluster

Get the first subcluster ready for the service groups.

To activate the first subcluster

- 1 Start LLT and GAB.

```
# /etc/init.d/llt start  
# /etc/init.d/gab start
```

- 2 Seed node01 and node02 in the first subcluster.

```
# gabconfig -x
```

- 3 If the product doesn't start automatically, on the first half of the cluster, start SFHA:

```
# cd /opt/VRTS/install  
# ./installsfha<version> -start node01 node02
```

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

- 4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

- 5 Unfreeze the nodes in the first subcluster.

```
# hasys -unfreeze -persistent node01  
# hasys -unfreeze -persistent node02
```

- 6 Unfreeze service groups in the first subcluster:

```
# hagrps -unfreeze sg1 -persistent  
# hagrps -unfreeze sg2 -persistent
```


- 7 Dump the configuration and make it read-only.

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

- 8 Bring the service groups online on node01 and node02.

```
# hagrps -online sg1 -sys node01
# hagrps -online sg1 -sys node02
# hagrps -online sg2 -sys node01
# hagrps -online sg2 -sys node02
# hagrps -online sg3 -sys node01
# hagrps -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.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting `LLT_START = 0`.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the second subcluster

After step 4 to step 6, 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 the SFHA Solutions 6.2.1 binary.

```
# cd /tmp/sfha6.2.1.
```

- 3 Confirm that SFHA is stopped on node03 and node04. Start the installmr program, specify the nodes in the second subcluster (node03 and node04).

```
# ./installmr -base_path /tmp/sfha6.2/ node03
node04
```

The program starts with a copyright message and specifies the directory where it creates the logs.

- 4 From the opening Selection Menu, choose: G for **Upgrade a Product**.
- 5 From the following menu, choose: 1 for **Full Upgrade**.

- 1) Full Upgrade
- 2) Rolling Upgrade
- b) Back to previous menu

```
Select the way by which you want to upgrade product: [1-2,b,q] (1)
```

- 6 The installer displays the list of RPMs that get removed, installed, and upgraded on the selected systems.
- 7 When you are prompted, reply **y** to stop appropriate processes.

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

The installer stops processes, uninstalls RPMs, and installs RPMs.

- 8 Enter **y** to agree to the End User License Agreement (EULA).
- 9 Monitor the installer program answering questions as appropriate until the upgrade completes.

After this step, for finishing the phased upgrade, see *Symantec™ Storage Foundation and High Availability 6.2 Installation Guide*.

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 node01 [node02 ...]
```

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

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

- 2 On the second half of the cluster, start SFHA:

```
# cd /opt/VRTS/install
# ./installsfha<version> -start node03 node04
```

Where <version> is the specific release version.

- 3 Check to see if SFHA 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
```

4 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
```

5 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 SFHA. The service groups were down when you took them offline on node03 and node04, to the time SFHA brought them online on node01 or node02.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

Performing a phased SFCFSHA upgrade using Install Bundles

Performing a phased upgrade involves the following tasks:

- 1 Moving the service groups to the second subcluster.
See [“Moving the service groups to the second subcluster”](#) on page 78.
- 2 Upgrading the SFCFSHA stack on the first subcluster.
See [“Upgrading the SFCFSHA stack on the first subcluster”](#) on page 79.
- 3 Preparing the second subcluster.
See [“Preparing the second subcluster”](#) on page 81.
- 4 Activating the first subcluster.
See [“Activating the first subcluster”](#) on page 82.
- 5 Upgrading the operating system on the second subcluster.
See [“Upgrading the operating system on the second subcluster”](#) on page 83.
- 6 Upgrading the second subcluster.
See [“Upgrading the second subcluster”](#) on page 83.
- 7 Finishing the phased upgrade.
See [“Finishing the phased upgrade”](#) on page 84.

Moving the service groups to the second subcluster

To move the service groups to the second subcluster

- 1 Switch failover groups from the first half of the cluster to one of the nodes in the second half of the cluster. In this procedure, `node01` is a node in the first half of the cluster and `node04` is a node in the second half of the cluster. Enter the following:

```
# hagrps -switch failover_group -to node04
```

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

```
# mount | grep vxfs
```

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

```
# fuser -c /mount_point
```

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

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

```
# umount /mount_point
```

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

```
# hagrps -offline group_name -sys node01
```

When the CVM group becomes OFFLINE, all the parallel service groups such as the CFS file system will also become OFFLINE on the first half of the cluster nodes.

- 5 Verify that the VCS service groups are offline on all the nodes in first half of the cluster. Enter the following:

```
# hagrps -state group_name
```

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

```
# haconf -makerw
```

```
# hasys -freeze -persistent node01
```

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

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

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

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

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

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

Verify that no volumes remain open. Enter the following:

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

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

When the node starts, prevent LLT from starting automatically with one of the following methods. For example, . Or, change the /etc/default/llt file by setting LLT_START = 0. After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

- Enter:

```
# mv /etc/llttab /etc/llttab.save
```

OR:

- Set LLT_START = 0 in the /etc/default/llt file

Note: After upgrading the OS, change the LLT configuration to its original configuration.

Upgrading the SFCFSHA stack on the first subcluster

After step 1, 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.
- 2 Navigate to the folder that contains the SFHA Solutions 6.2.1 binary.

```
#cd /tmp/sfha6.2.1
```

- 3 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.
- 4 Start the installmr program, specify the nodes in the first subcluster (node01 and node02).

```
#./installmr -base_path /tmp/sfha6.2/ node01 node02
```

- 5 The program starts with a copyright message and specifies the directory where it creates the logs. It performs a system verification and outputs upgrade information.

To upgrade the SFCFSHA stack on the first subcluster

- 1 From the opening Selection Menu, choose: G for **Upgrade a Product**.
- 2 From the following menu, choose: 1 for **Full Upgrade**.

- 1) Full Upgrade
- 2) Rolling Upgrade
- b) Back to previous menu

```
Select the way by which you want to upgrade product: [1-2,b,q] (1)
```


Preparing the second subcluster

To prepare the second subcluster

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

```
# mount | grep vxfs
```

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

```
# fuser -c /mount_point
```

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

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

```
# umount /mount_point
```

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

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

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

```
# hagr -offline group_name -sys node04
```

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

```
# hagr -state group_name
```

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

```
# hastop -local
```

- 7 On the second half of the cluster, stop the following SFCFSHA modules: GLM, ODM, GMS, VxFEN, GAB, and LLT. Enter the following:

```
# /etc/init.d/vxglm stop
# /etc/init.d/vxodm stop
# /etc/init.d/vxgms stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

Activating the first subcluster

To activate the first subcluster

- 1 Start LLT and GAB:

```
# /etc/init.d/llt start
# /etc/init.d/gab start
```

- 2 Force GAB to form a cluster in the first half of the cluster.

```
# /sbin/gabconfig -x
```

GAB port a appear in `gabconfig -a` command output.

- 3 If the product doesn't start automatically, on the first half of the cluster, start SFCFSHA:

```
# cd /opt/VRTS/install
# ./installsfcfsha<version> -start node01 node02
```

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

- 4 Unfreeze the nodes in the first half of the cluster. Enter the following:

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

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

```
# hagrps -online group_name -sys node_name
```

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

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

Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting `LLT_START = 0`.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the second subcluster

After step 3 to step 5, upgrade the second subcluster.

To upgrade the second subcluster

- 1 Enter the following:

```
# ./installmr -base_path /tmp/sfha6.2/ node_name
```

- 2 From the opening Selection Menu, choose: G for **Upgrade a Product**.
- 3 From the following menu, choose: 1 for **Full Upgrade**.

- 1) Full Upgrade
- 2) Rolling Upgrade
- b) Back to previous menu

```
Select the way by which you want to upgrade product: [1-2,b,q] (1)
```

Finishing the phased upgrade

To finish the phased upgrade

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

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

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

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

- 2 Run the installer to start SFCFSHA on the second subcluster:

```
# ./opt/VRTS/install/installsfcfsha61 node03 node04
```
- 3 Manually mount the VxFS and CFS file systems that are not managed by VCS in the second half of the cluster.
- 4 Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

- 5 On the CVM master node, upgrade the CVM protocol. Enter the following:

```
# vxdctl upgrade
```

Performing a phased SF Oracle RAC upgrade using Install Bundles

The phased upgrade methodology involves upgrading half of the nodes in the cluster at a time. The procedure involves the following tasks:

- 1 Performing pre-upgrade tasks on the first half of the cluster.
[Step 1: Performing pre-upgrade tasks on the first half of the cluster](#)
- 2 Upgrading the first half of the cluster.
[Step 2: Upgrading the first half of the cluster](#)
- 3 Performing pre-upgrade tasks on the second half of the cluster.
[Step 3: Performing pre-upgrade tasks on the second half of the cluster](#)

- 4 Performing post-upgrade tasks on the first half of the cluster.
[Step 4: Performing post-upgrade tasks on the first half of the cluster](#)
- 5 Upgrading the second half of the cluster.
[Step 5: Upgrading the second half of the cluster](#)
- 6 Performing post-upgrade tasks on the second half of the cluster.
[Step 6: Performing post-upgrade tasks on the second half of the cluster](#)

Step 1: Performing pre-upgrade tasks on the first half of the cluster

Perform the following pre-upgrade steps on the first half of the cluster.

To perform the pre-upgrade tasks on the first half of the cluster

- 1 Back up the following configuration files: `main.cf`, `types.cf`, `CVMTypes.cf`, `CFSTypes.cf`, `OracleTypes.cf`, `OracleASMTTypes.cf`, `PrivNIC.cf`, `MultiPrivNIC.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmodemain.cf`, `types.cf`, `CVMTypes.cf`, `CFSTypes.cf`, `SybaseTypes.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmode`

For example:

```
# cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.save
```

The installer verifies that recent backups of configuration files in the VxVM private region are saved in `/etc/vx/cbr/bk`.

If not, the following warning message is displayed: `Warning: Backup /etc/vx/cbr/bk directory.`

- 2 Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.
- 3 Stop the applications configured under VCS. Stop the Oracle database:
 - If the Oracle RAC instance is managed by VCS:


```
# hagrps -offline oracle_group -sys node01
# hagrps -offline oracle_group -sys node02
```

- If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the first half of the cluster and shut down the instances:

For Oracle RAC 12c:

```
$ srvctl stop instance -db db_name \  
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \  
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \  
-i instance_name
```

- 4
- If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts:

```
# haconf -makerw  
# hagrps -modify oracle_group AutoStart 0  
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to manual:

For Oracle 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

- 5 Unmount the CFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the CFS mount point:

```
# mount | grep vxfs | grep cluster  
  
# fuser -cu /mount_point
```

- Unmount the CFS file system:

```
# umount /mount_point
```

- 6 Stop the parallel service groups and switch over failover service groups on each of the nodes in the first half of the cluster:

```
# hastop -local -evacuate
```

```
# hastop -local
```

- 7 Unmount the VxFS file systems that are not managed by VCS.
 - Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS mount point:

```
# mount | grep vxfs
```

```
# fuser -cu /mount_point
```

- Unmount the VxFS file system:

```
# umount /mount_point
```

- 8 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.

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

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

- 9 If a cache area is online, you must take the cache area offline before upgrading the VxVM RPM. On the nodes in the first subcluster, use the following command to take the cache area offline

```
# sfcache offline cachename
```

- 10 If you plan to upgrade the operating system, stop all ports.

```
# /opt/VRTS/install/installsfrac<version> -stop node01 node02
```

Step 2: Upgrading the first half of the cluster

Perform the following steps to upgrade the first half of the cluster.

To upgrade the first half of the cluster

- 1 If you plan to upgrade the operating system, rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

- 2 Upgrade the operating system, if required.
- 3 If you upgraded the operating system, restart the nodes:

```
# shutdown -r now
```

- 4 Rename the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

- 5 Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

- 6 On the first half of the cluster, upgrade SF Oracle RAC by using the `installmr` script. When you invoke the installer, select the **Full Upgrade** option. The installer automatically detects the phased upgrade though you select the Full Upgrade option.

```
# cd /tmp/sfha6.2.1
```

```
# ./installmr -base_path /tmp/sfha6.2 node01 node02
```

Note: Do not start the product in the first subcluster until you complete the instructions for preparing the second subcluster.

See [“Step 3: Performing pre-upgrade tasks on the second half of the cluster”](#) on page 89.

If the product is licensed with stale (old) key, the installer prompts users to update the key.

- 7 Relink the SF Oracle RAC libraries with Oracle:

If you want the installer to relink the Oracle Database Binary, you can choose the option **Relink Oracle Database Binary** from the menu.

Complete the remaining tasks to finish the upgrade.

Step 3: Performing pre-upgrade tasks on the second half of the cluster

Perform the following pre-upgrade steps on the second half of the cluster.

To perform the pre-upgrade tasks on the second half of the cluster

- 1 Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.

Note: The downtime starts now.

- 2 Stop all applications that are configured under VCS. Stop the Oracle database:

- If the Oracle RAC instance is managed by VCS:

```
# hagrps -offline oracle_group -sys node03
# hagrps -offline oracle_group -sys node04
```

- If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the second half of the cluster and shut down the instances:

For Oracle RAC 12c:

```
$ srvctl stop instance -db db_name \
-n node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \
-i instance_name
```

- 3 Unmount the CFS file systems that are not managed by VCS.
 - Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

```
# mount | grep vxfs | grep cluster
# fuser -cu /mount_point
```

- Unmount the non-system VxFS file system:

```
# umount /mount_point
```

- 4 Stop VCS on each of the nodes in the second half of the cluster:

```
# hastop -local
```

- 5 Unmount the VxFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

```
# mount | grep vxfs
```

```
# fuser -cu /mount_point
```

- Unmount the non-system VxFS file system:

```
# umount /mount_point
```

- 6 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.

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

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

- 7 If a cache area is online, you must take the cache area offline before upgrading the VxVM RPM. On the nodes in the second subcluster, use the following command to take the cache area offline:

```
# sfcache offline cachename
```

- 8 Stop all ports.

```
# /opt/VRTS/install/installsfrac -stop node03 node04
```

Step 4: Performing post-upgrade tasks on the first half of the cluster

Perform the following post-upgrade steps on the first half of the cluster.

To perform the post-upgrade tasks on the first half of the cluster

- 1 On any one node on the first half of the cluster, force GAB to form a cluster.

```
# /etc/init.d/llt start
# /etc/init.d/gab start

# gabconfig -x
```

- 2 On the first half of the cluster, start SF Oracle RAC:

```
# cd /opt/VRTS/install
# ./installsfrac<version> -start node01 node02
```

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

- 3 On the first half of the cluster, manually mount the VxFS or CFS file systems that are not managed by VCS.
- 4 Relink the SF Oracle RAC libraries with Oracle:

Choose the option **Relink Oracle Database Binary** from the program menu.

- 5 Bring the Oracle database service group online.

If the Oracle database is managed by VCS:

```
# hagrps -online oracle_group -sys node_name
```

If the Oracle database is not managed by VCS:

For Oracle RAC 12c:

```
$ srvctl start instance -db db_name \
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl start instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl start instance -d db_name \
-i instance_name
```

Note: The downtime ends here.

- 6 On the first half of the cluster, start all applications that are not managed by VCS. Use native application commands to start the applications.

Step 5: Upgrading the second half of the cluster

Perform the following steps to upgrade the second half of the cluster.

To upgrade the second half of the cluster

- 1 If you plan to upgrade the operating system, rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

- 2 Upgrade the operating system, if required.

For instructions, see the operating system documentation.

- 3 If you upgraded the operating system, restart the nodes:

```
# shutdown -r now
```

- 4 Rename the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

- 5 Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the second subcluster without requests for a password.
- 6 On the second half of the cluster, upgrade SF Oracle RAC with the `installmr` script.

When you invoke the installer, select the **Full Upgrade** option. The installer automatically detects the phased upgrade though you select the Full Upgrade option.

```
# cd /tmp/sfha6.2.1
```

```
# ./installmr -base_path /tmp/sfha6.2 node03 node04
```

If the product is licensed with stale (old) key, the installer prompts users to update the key.

- 7 Relink the SF Oracle RAC libraries with Oracle:

If you want the installer to relink the Oracle Database Binary, you can choose the option **Relink Oracle Database Binary** from the menu.

Complete the remaining tasks to finish the upgrade.

Step 6: Performing post-upgrade tasks on the second half of the cluster

Perform the following post-upgrade steps on the second half of the cluster.

To perform the post-upgrade tasks on the second half of the cluster

- 1 Manually mount the VxFS and CFS file systems that are not managed by VCS.
- 2 On the second half of the cluster, start SF Oracle RAC:

```
# cd /opt/VRTS/install
```

```
# ./installsfrac<version> -start node03 node04
```

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

- 3 Upgrade VxVM disk group version.

For instructions, see the chapter "Post-upgrade tasks" in the *Symantec™ Storage Foundation for Oracle RAC 6.2 Installation and Configuration Guide*.

4 Upgrade disk layout version.

For instructions, see the chapter "Post-upgrade tasks" in the *Symantec™ Storage Foundation for Oracle RAC 6.2 Installation and Configuration Guide*.

5 Bring the Oracle database service group online.

If the Oracle database is managed by VCS:

```
# hagrps -online oracle_group -sys node03
# hagrps -online oracle_group -sys node04
```

If the Oracle database is not managed by VCS:

For Oracle RAC 12c:

```
$ srvctl start instance -db db_name \
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl start instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl start instance -d db_name \
-i instance_name
```

- 6 ■ If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrps -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

- 7 Start all applications that are not managed by VCS. Use native application commands to start the applications.
- 8 Set or change the product license level, if required.
- 9 Migrate the SFDB repository database.

As root, dump out the old Sybase Adaptive Server Anywhere (Sybase ASA) repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.

```
# /opt/VRTSdbed/migrate/sfua_rept_migrate
```

Performing a rolling upgrade using Install Bundles

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

- [Supported rolling upgrade paths](#)
- [Performing a rolling upgrade of VCS, SFHA, and SFCFSHA with Install Bundles](#)
- [Performing a rolling upgrade of SF Oracle RAC with Install Bundles](#)

Supported rolling upgrade paths

You can perform a rolling upgrade using the `installmr` script with Install Bundles.

[Table 3-10](#) shows the versions for which you can perform a rolling upgrade to 6.2.1.

Table 3-10 Supported rolling upgrade paths for Install Bundles

| Platform | version |
|----------|---|
| Linux | 5.1SP1RP3, 5.1SP1RP4 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5 6.1, 6.1.1 |

Note: SLES11 doesn't support rolling upgrade to 6.2.1 from releases before 6.0.1.

Note: On RHEL6, SFHA Solutions only supports rolling upgrade to 6.2.1 from 5.1 SP1 RP4, 6.0.5, and 6.0.5 onwards.

Note: Before performing a rolling upgrade from version 5.1SP1RP3 to version 6.2.1, install patch VRTSvxfen-5.1SP1RP3P2. For downloading the patch, search VRTSvxfen-5.1SP1RP3P2 in [Patch Lookup](#) on the [SORT](#) website.

OS upgrade support during rolling upgrades on Linux

If the upgrade scenario involves operating system upgrades, SFHA Solutions supports rolling upgrade only for minor OS upgrades.

For the following scenarios, use phased upgrades instead of rolling upgrades:

- Upgrades from versions prior to 6.0.1 on SLES11 or SLES11 SP1 to 6.2.1 on SLES11 SP2.
- Upgrades from versions prior to 6.0.1 on RHEL6.1 or RHEL6.2 to 6.2.1 on RHEL6.4.

Performing a rolling upgrade of VCS, SFHA, and SFCFSHA with Install Bundles

Before you start the rolling upgrade, make sure that Symantec 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.
- 3 Change to the `/tmp/sfha6.2.1` directory.
- 4 Start the installer.

```
# ./installmr -base_path /tmp/sfha6.2
```

- 5 From the menu, select `Upgrade` and from the sub menu, select `Rolling Upgrade`.
- 6 Enter one system of the cluster on which you would like to perform rolling upgrade.
- 7 The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type **y** to continue.
- 8 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.

- 9 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.
- 10 Review the end-user license agreement, and type **y** if you agree to its terms.
- 11 After the installer shows the package list, it detects if there are online failover service groups on the nodes to be upgraded. If there are online failover service groups, the installer prompts you to do one of the following:
 - Manually switch service groups
 - Use the CPI to automatically switch service groups

The downtime is the time that it normally takes for the service group's failover.

- 12 The installer prompts you to stop the applicable processes. Type **y** to continue. The installer evacuates all service groups to the node or nodes that are not upgraded at this time. The installer stops parallel service groups on the nodes that are to be upgraded.
- 13 The installer stops relevant processes, uninstalls old kernel RPMs, and installs the new RPMs.

The installer performs the upgrade configuration and re-starts processes.

If some processes fail to start, you may need to reboot the nodes and manually check the cluster's status.

- 14 Complete the preparatory steps on the nodes that you have not yet upgraded.
- 15 The installer begins phase 1 of the upgrade on the remaining node or nodes. Type **y** to continue the rolling upgrade.

The installer repeats step 8 through step 13.

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.

Note: If there are Oracle Service Groups on your system, before you switch the Oracle Service Groups to the target nodes, make sure you does the ODM relink and ODM works normally on the target nodes. See the topic of *Configuring the Veritas Extension for Oracle Disk Manager in SFHA environment* in *Symantec Storage Foundation for Oracle RAC Administrator's Guide*.

- 16 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.

17 The installer determines the remaining RPMs to upgrade. Press **Enter** to continue.

18 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

19 The installer stops Symantec Cluster Server (VCS) processes but the applications continue to run. Type **y** to continue.

The installer performs prechecks, uninstalls old RPMs, and installs the new RPMs. It performs post-installation tasks, and the configuration for the upgrade.

20 A prompt message appears to ask if you would like to send the information about this installation to Symantec to help improve installation in the future?

Type **y** or **n** to help Symantec improve the installation.

- 21 If you have network connection to the Internet, the installer checks for updates. If updates are discovered, you can apply them now.
- 22 A prompt message appears to ask if the user would like to read the summary file. You can choose **y** if you want to read the install summary file.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

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

Performing a rolling upgrade of SF Oracle RAC with Install Bundles

Use a rolling upgrade to upgrade Symantec Storage Foundation for Oracle RAC to the latest release with minimal application downtime.

Using the `installmr` script with Install Bundles, you can upgrade to 6.2.1 from releases earlier than 6.2.

Note: If you need to upgrade operating system, upgrade the operating system on all nodes before upgrading the products.

- [Preparing to perform a rolling upgrade to SF Oracle RAC 6.2.1](#)
- [Using Install Bundles to perform a rolling upgrade of SF Oracle RAC](#)

Preparing to perform a rolling upgrade to SF Oracle RAC 6.2.1

Perform the preparatory steps in this section if you are performing a rolling upgrade of the cluster. Before you upgrade, make sure that your systems meet the hardware and software requirements for this release.

To prepare to upgrade SF Oracle RAC

Perform the steps on the subcluster.

- 1 Log in as superuser to one of the nodes in the subcluster.
- 2 Back up the following configuration files on your system: `main.cf`, `types.cf`, `CVMTypes.cf`, `CFSTypes.cf`, `OracleTypes.cf`, `OracleASMTypes.cf`, `PrivNIC.cf`, `MultiPrivNIC.cf`, `CRSResource.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmode`

For example:

```
# cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.save
```

- 3 Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.
 If not, a warning message will be displayed after `installmr` upgrade prechecks..

Warning: Backup `/etc/vx/cbr/bk` directory.

- 4 Stop the Oracle RAC resources on each node.
 - If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:

```
# hagrps -offline oracle_group -sys node_name
```

- If the database instances are not managed by VCS, then run the following on one node:
 For Oracle RAC 12c:

```
# srvctl stop instance -db db_name -node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \
-i instance_name
```

- 5 ■ If the Oracle database is managed by VCS, set the `AutoStart` value to 0 to prevent the database service group from starting automatically when VCS starts. Failing to perform this step results in the database attempting to

come online after the upgrade; the attempt fails due to the presence of old libraries on the system.

```
# haconf -makerw
# hagr -modify oracle_group AutoStart 0
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to manual:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

- 6 Unmount all the CFS file system which is not under VCS control.

```
# mount |grep vxfs | grep cluster
# fuser -m /mount_point
# umount /mount_point
```

Make sure that no processes are running which make use of mounted shared file system or shared volumes.

```
# fuser -cu /mount_point
```

- 7 Take all the parallel VCS service groups offline on each of the nodes in the current subcluster:

```
# hagr -offline grp_name -sys sys_name
```

- 8 Unmount all the VxFS file system which is not under VCS control.

```
# mount |grep vxfs

# fuser -m /mount_point

# umount /mount_point
```

- 9 If you plan to continue using the Storage Foundation for Databases (SFDB) tools, you must prepare to migrate the SFDB repository database before upgrading to SF Oracle RAC 6.2.1.

See [“Pre-upgrade tasks for migrating the SFDB repository database”](#) on page 43.

Using Install Bundles to perform a rolling upgrade of SF Oracle RAC

Before you start the rolling upgrade, make sure that Symantec Cluster Server (VCS) is running.

To perform a rolling upgrade

- 1 If you want to upgrade the operating system, perform the following steps:

Note: If you plan to upgrade the operating system, make sure that you upgrade all nodes before you start rolling upgrade of SF Oracle RAC.

- Change to the `/opt/VRTS/install` directory on the node where you want to upgrade the operating system:

```
# cd /opt/VRTS/install
```

- Stop SF Oracle RAC:

```
# ./installsfrac<version> -stop
```

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

- Upgrade the operating system. For instructions, see the operating system documentation.
- Reboot the nodes:

```
# shutdown -r now
```

- 2 Complete the preparatory steps on the first sub-cluster.

See [“Preparing to perform a rolling upgrade to SF Oracle RAC 6.2.1”](#) on page 99.

- 3 Log in as superuser.
- 4 Change to the `sfha6.2.1` directory.
- 5 Start the `installmr` script.

```
# ./installmr -base_path /tmp/sfha6.2/
```

- 6 From the menu, select `Upgrade a Product` and from the sub menu, select `Rolling Upgrade`.
- 7 The installer suggests system names for the upgrade. Enter `Yes` to upgrade the suggested systems, or enter `No`, and then enter the name of any one system in the cluster on which you want to perform a rolling upgrade.
- 8 The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type `y` to continue.
- 9 The installer inventories the running service groups and determines the node or nodes to upgrade in phase 1 of the rolling upgrade. Type `y` to continue. If you choose to specify the nodes, type `n` and enter the names of the nodes.
 See [“Pre-upgrade tasks for migrating the SFDB repository database”](#) on page 43.
- 10 The installer performs further prechecks on the nodes in the cluster and may present warnings. You can type `y` to continue or quit the installer and address the precheck's warnings.
- 11 Review the end-user license agreement, and type `y` if you agree to its terms.
- 12 The installer lists the RPMs to upgrade on the selected node or nodes.
- 13 After the installer shows the package list, it detects if there are online failover service groups on the nodes to be upgraded. If there are online failover service groups, the installer prompts you to do one of the following:
 - Manually switch service groups
 - Use the CPI to automatically switch service groups

The downtime is the time that it normally takes for the service group's failover.

- 14 The installer prompts you to stop the applicable processes. Type **y** to continue.

The installer evacuates all service groups to the node or nodes that are not upgraded at this time. The installer stops parallel service groups on the nodes that are to be upgraded.

- 15 The installer stops relevant processes, uninstalls old kernel RPMs, and installs the new RPMs.

The installer performs the upgrade configuration.

The installer asks the following question for updating license keys:

```
Symantec Storage Foundation for Oracle RAC Install completed
successfully
```

```
Found vxkeyless key(s) for previous release(s). It is
recommended to update them to fully utilize the new features
in the current release. Do you wish to update them to
the current version? [y,n,q] (y)
```

```
Keyless keys are updated to version 6.2 on vcslx013 (SFRACENT)
```

```
Keyless keys are updated to version 6.2 on vcslx014 (SFRACENT)
```

```
Checking system licensing
```

```
SF Oracle RAC is licensed on the systems
```

After asking the question, the installer re-starts processes.

If some processes fail to start, you may need to reboot the nodes and manually check the cluster's status.

Note: The Oracle service group is offline as the AutoStart attribute is set to 0 to prevent the service group from starting automatically. The service group is started later in the process.

- 16 Manually mount the VxFS and CFS file systems that are not managed by VCS.

- 17 Relink the SF Oracle RAC libraries with Oracle:

Choose the option **Relink Oracle Database Binary** from the program menu.

- 18 Bring the Oracle database service group online.

- If VCS manages the Oracle database:

```
# hagrps -online oracle_group -sys node_name
```


- If VCS does not manage the Oracle database:

For Oracle RAC 11g:

```
$ srvctl start database -d db_name
```

For Oracle RAC 12c:

```
$ srvctl start database -db db_name
```

- 19 Start all applications that are not managed by VCS. Use native application commands to start the applications.
- 20 Complete the preparatory steps on the nodes that you have not yet upgraded.
- 21 If the nodes are rebooted, restart the installer and continue phase-1 for second sub-cluster. Type **y** to continue the rolling upgrade.

The installer repeats step 7 through step 17.

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.

This completes phase 1 of the upgrade.

- 22 ■ If VCS manages the Oracle database, reset the AutoStart value to 1 to enable VCS to bring the database service group online when VCS starts:

```
# haconf -makerw
# hagrpl -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If VCS does not manage the Oracle database, change the management policy for the database to automatic:

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

- 23 Phase 2 of the rolling upgrade begins here. This phase includes downtime for the VCS engine (HAD), which does not include application downtime.

24 Migrate the SFDB repository database.

As root, dump out the old Sybase Adaptive Server Anywhere (Sybase ASA) repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.

```
# /opt/VRTSdbed/migrate/sfua_rept_migrate
```

25 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.

26 Phase 2 of the upgrade begins here. This phase includes downtime for the VCS engine (HAD), which does not include application downtime. Type **y** to continue.

27 The installer determines the remaining RPMs to upgrade. Press **Enter** to continue.

28 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

29 The installer stops Symantec Cluster Server (VCS) processes but the applications continue to run. Type **y** to continue.

The installer performs prechecks, uninstalls old RPMs, installs the new RPMs, and start the Symantec Cluster Server (VCS). It performs post-installation tasks, and the configuration for the upgrade.

- 30 When the following message appears, type **y** or **n** to help Symantec improve the installation:

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

- 31 If you have network connection to the Internet, the installer checks for updates. If updates are discovered, you can apply them now.
- 32 A prompt message appears to ask if the user would like to read the summary file. You can choose **y** if you want to read the install summary file.

Performing an automated upgrade using response files with Install Bundles

Depending on the installed product, use one of the following procedures:

- [Performing an automated upgrade using response files with Install Bundles](#)

Performing an automated upgrade using response files with Install Bundles

Typically, you can use the response file that the installer generates after you perform SFHA Solutions upgrade with Install Bundles on one system to upgrade SFHA Solutions on other systems. You can also create a response file using the `makeresponsefile` option of the installer.

To perform automated upgrade using response files

- 1 Make sure the systems where you want to upgrade meet the upgrade requirements.
- 2 Copy the response file to one of the systems where you want to upgrade SFHA.
- 3 Edit the values of the response file variables as necessary.
- 4 Navigate to the folder that contains the installation program.
- 5 Start the upgrade from the system to the `/tmp/sfha6.2.1` directory. For example:

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

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

- 6 Complete the post upgrade task as mentioned in particular upgrade method in 6.2 Installation Guides.

Upgrading to 6.2.1 from 6.2

This chapter includes the following topics:

- [Prerequisites for upgrading to 6.2.1](#)
- [Downloading required software to upgrade to 6.2.1](#)
- [Performing a full upgrade to 6.2.1 on a cluster](#)
- [Upgrading to 6.2.1 on a standalone system](#)
- [Performing a phased upgrade to SFCFSHA and SFRAC](#)
- [Upgrading to 6.2.1 on a system that has encapsulated boot disk](#)
- [Performing a rolling upgrade using the installer](#)
- [Upgrading the operating system](#)
- [Upgrading SFHA with the Veritas Web-based installer](#)
- [Verifying software versions](#)

Prerequisites for upgrading to 6.2.1

If you are upgrading from 6.2, see the following list for prerequisites for upgrading to the 6.2.1 release:

- For any product in the Symantec Storage Foundation stack, you must have the 6.2.1 release binaries.
- Each system must have sufficient free space to accommodate patches.
- The full list of prerequisites can be obtained by running `./installmr -precheck`.
- Make sure to download the latest patches for the installer.
See [“Downloading required software to upgrade to 6.2.1 ”](#) on page 109.

For information on supported upgrade types, See “[Supported upgrade types for SFHA Solutions 6.2.1](#)” on page 22.

Downloading required software to upgrade to 6.2.1

This section describes how to download the latest patches for the installer.

To download required software to upgrade to 6.2.1

- 1 Download SFHA 6.2.1 from <https://sort.symantec.com/patches>.
- 2 Extract it to a directory, say /tmp/sfha621.

Performing a full upgrade to 6.2.1 on a cluster

Performing a full upgrade on a cluster requires stopping cluster failover functionality during the entire procedure.

Depending on your cluster’s configuration, select one of the following procedures to upgrade to 6.2.1:

- [Performing a full upgrade to 6.2.1 on a Symantec Cluster Server](#)
- [Performing a full upgrade to 6.2.1 on an SFHA cluster](#)
- [Performing a full upgrade to 6.2.1 on an SFCFSHA cluster](#)
- [Performing a full upgrade to 6.2.1 on an SF Oracle RAC cluster](#)

Performing a full upgrade to 6.2.1 on a Symantec Cluster Server

The following procedure describes performing a full upgrade on a Symantec Cluster Server (VCS) cluster.

Note: You need to make sure that IPv4RouteOptions attribute is configured for MultiNICA resources, otherwise network connection may be interrupted.

To upgrade VCS

- 1 Make sure you have downloaded the latest software required for the upgrade. Refer to the appropriate 6.2 installation guide.
- 2 Log in as superuser.

Note: Upgrade the Operating System and reboot the systems if required.

- 3 Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 6.2.1 rolling patch binaries, change to the directory that contains the `installmr` script. Start the pre-upgrade check:

```
# ./installmr -precheck node01 node02 ... nodeN
```

- 4 Resolve any issues that the precheck finds.
- 5 Start the upgrade:

```
# ./installmr node01 node02 ... nodeN
```

- 6 After the upgrade, review the log files for any issues.

Performing a full upgrade to 6.2.1 on an SFHA cluster

The following procedure describes performing a full upgrade on an SFHA and VCS cluster.

To perform a full upgrade to 6.2.1 on an SFHA cluster

- 1 Make sure you have downloaded the latest software required for the upgrade.
- 2 Log in as superuser.
- 3 From the directory that contains the extracted and untarred 6.2.1 rolling patch binaries, change to the directory that contains the `installmr` script. Check the readiness of the nodes where you plan to upgrade. Start the pre-upgrade check:

```
# ./installmr -precheck node01 node02... nodeN
```

where `node01`, `node02` and `nodeN` are nodes to be upgraded.

- 4 If service groups have VxFS file systems mounted, make the service groups offline.
- 5 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```

- 6 Start the upgrade:

```
# ./installmr node01 node02... nodeN
```

where `node01`, `node02` and `nodeN` are nodes to be upgraded.

Performing a full upgrade to 6.2.1 on an SFCFSHA cluster

The following procedure describes performing a full upgrade on an SFCFSHA cluster.

To perform a full upgrade to 6.2.1 on an SFCFSHA cluster

- 1 Make sure you have downloaded the latest software required for the upgrade.

See “[Downloading required software to upgrade to 6.2.1](#)” on page 109.

- 2 Log in as superuser.
- 3 If applications are not managed by VCS, make the applications offline.
- 4 On each node, enter the following command to check if any Storage Checkpoints or VxFS file systems out of VCS control are mounted:

```
# mount | grep vxfs
```

If any Storage Checkpoints or VxFS file systems are mounted, on each node in the cluster unmount all Storage Checkpoints.

```
# umount /checkpoint_name
```

- 5 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:
 - Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
 - Use the vxrvg stop command to stop each RVG individually:

```
# vxrvg -g diskgroup stop rvg_name
```

- On the Primary node, use the vxrlink status command to verify that all RLINKs are up-to-date:

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

Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

- 6 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```

- 7** Stop activity to all VxVM volumes.

For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes

- 8** Stop all VxVM volumes by entering the following command for each disk group on master node:

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

Verify that no volumes remain open:

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

- 9** On each node, stop the VCS command server:

```
# ps -ef | grep CmdServer
# kill -9 pid_of_CmdServer
```

pid_of_CmdServer is the process ID of CmdServer.

- 10** If required, apply the OS kernel patches.

- 11** From the directory that contains the extracted and untarred 6.2.1 rolling patch binaries, change to the directory that contains the `installmr` script. Start the upgrade.

```
# ./installmr node01 node02
```

where *node01* and *node02* are nodes which are to be upgraded.

- 12** After all nodes in the cluster are upgraded, the processes will be restarted automatically. Should there be any problem, the `installmr` script will ask you to reboot the system. Then the application failover capability will be available.

- 13** If necessary, reinstate any missing mount points in the `/etc/filesystems` file on each node.

- 14** Restart all the volumes by entering the following command on the master node, for each disk group:

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

- 15** If you stopped any RVGs in step 5, restart each RVG:

```
# vxrvg -g diskgroup start rvg_name
```

- 16** Remount all VxFS file systems and Storage Checkpoints on all nodes:

```
# mount /filesystem
```


Performing a full upgrade to 6.2.1 on an SF Oracle RAC cluster

The following procedure describes performing a full upgrade on an SF for Oracle RAC cluster.

To upgrade to 6.2.1 on an SF Oracle RAC cluster

- 1 Make sure you have downloaded the latest software required for the upgrade.
- 2 Log in as superuser.
- 3 Verify that `/opt/VRTSvcs/bin` is in your `PATH` so that you can execute all product commands.
- 4 From any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

- 5 Enter the following command to freeze HA service group operations on each node:

```
# hasys -freeze -persistent nodename
```

- 6 Make the configuration read-only:

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

- 7
 - If the Oracle database is managed by VCS, set the `AutoStart` value to 0 to prevent the database service group from starting automatically when VCS starts:

```
# haconf -makerw
# hagrps -modify oracle_group AutoStart 0
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to manual:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

- 8 If Oracle Clusterware is not controlled by VCS, enter the following command on each node of the cluster to stop Oracle Clusterware:

```
# GRID_HOME/bin/crsctl stop crs
```

- 9 Stop all applications that use VxFS or VxVM disk groups, whether local or CFS. If the applications are under VCS control:

```
# hagrps -offline grp_name -any
```

If the applications are not under VCS control:

Use native application commands to stop the application.

- 10 Unmount the VxFS file system, which is not under VCS control.

```
# mount |grep vxfs
```

```
# fuser -m /mount_point
```

```
# umount /mount_point
```

Make sure that no processes are running which make use of mounted shared file system or shared volumes.

```
# fuser -cu /mount_point
```

- 11 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```

- 12 Stop VCS.

```
# hastop -all
```

- 13 If required, apply the OS kernel patches.

See *Oracle's* documentation for the procedures.

- 14 From the directory that contains the extracted and untarred 6.2.1 rolling patch binaries, change to the directory that contains the `installmr` script. Enter:

```
# ./installmr node01 node02
```

where `node01` and `node02` are nodes which are to be upgraded.

- 15 Follow the instructions from the installer. If there is some module load/unload issue, reboot all of the nodes of the cluster.

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

- 16 If necessary, reinstate any missing mount points in the `/etc/fstab` file on each node.

- 17 Relink the SF Oracle RAC libraries with Oracle:

Choose the option **Relink Oracle Database Binary** from the program menu.

- 18 From any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

- 19 Enter the following command on each node to unfreeze HA service group operations:

```
# hasys -unfreeze -persistent nodename
```

- 20 Make the configuration read-only:

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

- 21 Enter the following command on each node to take service groups online:

```
# hagrps -online service_group -sys nodename
```

- 22 Restart all the volumes by entering the following command for each disk group:

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

- 23 Remount all VxFS file systems on all nodes:

```
# mount /filesystem
```

- 24 If Oracle Clusterware is not controlled by VCS, enter the following command on each node to start Oracle Clusterware.

```
# $CRS_HOME/bin/crsctl start crs
```

- 25 Bring the Oracle database service group online.

- If the Oracle database is managed by VCS:

```
# hagrps -online Oracle_group -any
```

- If the Oracle database is not managed by VCS:

For Oracle RAC 11g:

```
$ srvctl start database -d db_name
```

For Oracle RAC 12c:

```
$ srvctl start database -db db_name
```

- 26 ■ If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrpl -modify oracle_groupname AutoStart 1
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

27 Upgrade Oracle RAC.

For information on Oracle RAC support, see:

<http://www.symantec.com/docs/DOC5081>

For instructions, see the chapter *Upgrading Oracle RAC* in *Symantec™ Storage Foundation for Oracle® RAC Installation and Configuration Guide*.

Note: The procedure for Oracle RAC 12c is the same with that for Oracle RAC 11g Release 2.

Upgrading to 6.2.1 on a standalone system

You can use this procedure to upgrade on a standalone system that runs SF.

To upgrade to 6.2.1 on a standalone system

- 1 Make sure you have downloaded the latest software required for the upgrade.
- 2 Log in as superuser.
- 3 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.
- 4 If required, apply the OS kernel patches.
- 5 Enter the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# df -T | grep vxfs
```

- 6 Unmount all Storage Checkpoints and file systems:

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

- 7 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:
 - Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
 - Use the `vxrvrg stop` command to stop each RVG individually:

```
# vxrvrg -g diskgroup stop rvg_name
```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

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

Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

- 8 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```

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

- 10 Stop all VxVM volumes by entering the following command for each disk group:

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

Verify that no volumes remain open:

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

- 11 Navigate to the folder that contains the installation program. Run the `installmr` script:

```
# ./installmr nodename
```

- 12 If necessary, reinstate any missing mount points in the `/etc/fstab` file.

- 13 Restart all the volumes by entering the following command for each disk group:

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

- 14 If you stopped any RVGs in step 7, restart each RVG:

```
# vxrvrg -g diskgroup start rvg_name
```

- 15 Remount all VxFS file systems and Storage Checkpoints:

```
# mount /filesystem
```

```
# mount /checkpoint_name
```

Performing a phased upgrade to SFCFSHA and SFRAC

This section describes how to perform a phased upgrade to SFCFSHA and SFRAC.

Performing a phased upgrade of SFCFSHA

Performing a phased upgrade involves the following tasks:

- Preparing the first subcluster
- Upgrading the SFCFSHA stack on the first subcluster
- Preparing the second subcluster
- Activating the first subcluster
- Upgrading the operating system on the second subcluster
- Upgrading the second subcluster

- Finishing the phased upgrade

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

Prerequisites for a phased upgrade

Before you start the upgrade, confirm that you have licenses for all the nodes that you plan to upgrade. Note that your applications have downtime during this procedure.

Planning for a phased upgrade

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

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

Phased upgrade limitations

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

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

Preparing the first subcluster

To move the service groups to the second subcluster

- 1 Switch failover groups from the first half of the cluster to one of the nodes in the second half of the cluster. In this procedure, `node01` is a node in the first half of the cluster and `node04` is a node in the second half of the cluster. Enter the following:

```
# hagrps -switch failover_group -to node04
```

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

```
# mount | grep vxfs
```

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

```
# fuser -c /mount_point
```

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

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

```
# umount /mount_point
```

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

```
# hagrps -offline group_name -sys node01 node02
```

When the CVM group becomes OFFLINE, all the parallel service groups such as the CFS file system will also become OFFLINE on the first half of the cluster nodes.

- 5 Verify that the VCS service groups are offline on all the nodes in first half of the cluster. Enter the following:

```
# hagrps -state group_name
```

- 6 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```


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

```
# haconf -makerw
# hasys -freeze -persistent node01
# haconf -dump -makero
```

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

If you are in the CPS fencing mode, Symantec recommends you making a backup of the `/etc/vxfenmode` file for future use:

```
# cp /etc/vxfenmode /etc/vxfenmode.bak
```

To change the contents of the `/etc/vxfenmode` file to configure I/O fencing in disabled mode, enter the following:

```
# cp /etc/vxfen.d/vxfenmode_disabled /etc/vxfenmode
# cat /etc/vxfenmode
[root@swlx08 ~]# cat /etc/vxfenmode
#
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=disabled
```

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

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

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

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

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

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

Verify that no volumes remain open. Enter the following:

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

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

Upgrading the SFCFSHA stack on the first subcluster

To upgrade the SFCFSHA stack on the first subcluster

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

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

```
# ./installmr node01 node02
```

where `<node01>` and `<node02>` are the nodes on the first subcluster.

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

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

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

Preparing the second subcluster

To prepare the second subcluster

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

```
# mount | grep vxfs
```

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

```
# fuser -c /mount_point
```

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

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

```
# umount /mount_point
```

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

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

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

```
# hagrps -offline group_name -sys node03 node04
```

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

```
# hagrps -state group_name
```

- 6 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```

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

```
# hastop -local
```

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

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

- 9 If the cluster-wide attribute `UseFence` is set to `SCSI3`, reset the value to `NONE` in the `/etc/VRTSvcs/conf/config/main.cf` file, in second half of the cluster.
- 10 On the second half on cluster, stop the following SFCFSHA modules: VCS, VxFEN, ODM, GAB, and LLT. Enter the following:

```
# /etc/init.d/vxglm stop
# /etc/init.d/vxodm stop
# /etc/init.d/vxgms stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

- 11** On each node in the first half of the cluster, enable fencing. Replace the `/etc/vxfemode` file with your previous `vxfenmode` file. Take the `scsi3_dmp` file as an example:

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

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

Activating the first subcluster

To activate the first subcluster

- 1** Run the installer to start SFCFSHA:

```
# /opt/VRTS/install/installsfcfsha621 -start node01 node02
```

- 2** Start LLT and GAB on the first subcluster:

```
# /etc/init.d/llt start
# /etc/init.d/gab start
```

- 3 Force gab to form a cluster in the first half of the cluster.

```
# /sbin/gabconfig -x
```

GAB port a appears in `gabconfig -a` command output.

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

```
# hagrps -online group_name -sys node_name
```

After you bring the CVM service group ONLINE, all the GAB ports u, v, w and f come ONLINE and all the CFS mounts service groups also come ONLINE automatically.

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

Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting `LLT_START = 0`.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the second subcluster

To upgrade the second subcluster

- ◆ Enter the following:

```
# ./installmr node03 node04
```

Completing the phased upgrade

To complete the phased upgrade

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

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

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

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

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

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

- 3 Start SFCFSHA using the installer:

```
# /opt/VRTS/install/installsfcfsha621 -start node03 node04
```

- 4 When second half of the nodes come up, all the GAB ports a, b, d, h, u, v, w and f are ONLINE. Also all the CFS mounts service groups come online automatically.
- 5 Manually mount the VxFS and CFS file systems that are not managed by VCS in the second half of the cluster.
- 6 Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

Performing phased upgrade of SF Oracle RAC to version 6.2.1

[Table 4-1](#) illustrates the phased upgrade process. Each column describes the steps to be performed on the corresponding subcluster and the status of the subcluster when operations are performed on the other subcluster.

Table 4-1 Summary of phased upgrade

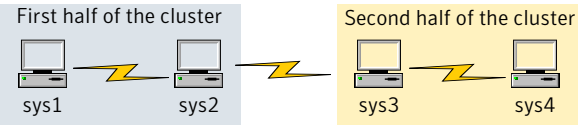





| First half of the cluster | Second half of the cluster |
|--|---|
| SF Oracle RAC cluster before the upgrade: | |
|  | |
| <p>STEP 1: Perform the following pre-upgrade steps:</p> <ul style="list-style-type: none"> ■ Switch failover applications. ■ Stop all parallel applications. <p>See “Step 1: Performing pre-upgrade tasks on the first half of the cluster” on page 129.</p> <p>STEP 2: Upgrade SF Oracle RAC.</p> <p>See “Step 2: Upgrading the first half of the cluster” on page 133.</p> | <p>The second half of the cluster is up and running.</p>  |

Table 4-1 Summary of phased upgrade (*continued*)

| First half of the cluster | Second half of the cluster |
|--|---|
| <p>The first half of the cluster is not running.</p>  | <p>STEP 3: Perform the following pre-upgrade steps:</p> <ul style="list-style-type: none"> ■ Stop all parallel and failover applications. ■ Stop SF Oracle RAC. <p>See “Step 3: Performing pre-upgrade tasks on the second half of the cluster” on page 133.</p> <p>The downtime starts now.</p> |
| <p>STEP 4: Perform the following post-upgrade steps:</p> <ul style="list-style-type: none"> ■ Start SF Oracle RAC. ■ Start all applications. <p>See “Step 4: Performing post-upgrade tasks on the first half of the cluster” on page 136.</p> <p>The downtime ends here.</p> | <p>The second half of the cluster is not running.</p>  |
| <p>The first half of the cluster is up and running.</p>  | <p>STEP 5: Upgrade SF Oracle RAC.</p> <p>See “Step 5: Upgrading the second half of the cluster” on page 137.</p> <p>STEP 6: Perform the following post-upgrade steps:</p> <ul style="list-style-type: none"> ■ Start SF Oracle RAC. ■ Start all applications. <p>See “Step 6: Performing post-upgrade tasks on the second half of the cluster” on page 138.</p> |
| <p>The phased upgrade is complete and both the first and the second half of the cluster are running.</p>  | |

Step 1: Performing pre-upgrade tasks on the first half of the cluster

Perform the following pre-upgrade steps on the first half of the cluster.

To perform the pre-upgrade tasks on the first half of the cluster

- 1 Back up the following configuration files: `main.cf`, `types.cf`, `CVMTTypes.cf`, `CFSTypes.cf`, `OracleTypes.cf`, `OracleASMTTypes.cf`, `PrivNIC.cf`, `MultiPrivNIC.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmodemain.cf`, `types.cf`, `CVMTTypes.cf`, `CFSTypes.cf`, `SybaseTypes.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmode`

For example:

```
# cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.save
# cp /etc/VRTSvcs/conf/config/types.cf \
/etc/VRTSvcs/conf/config/types.cf.save
# cp /etc/VRTSvcs/conf/config/OracleTypes.cf \
/etc/VRTSvcs/conf/config/OracleTypes.cf.save
# cp /etc/VRTSvcs/conf/config/PrivNIC.cf \
/etc/VRTSvcs/conf/config/PrivNIC.cf.save
# cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf \
/etc/VRTSvcs/conf/config/MultiPrivNIC.cf.save

# cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.save
# cp /etc/VRTSvcs/conf/config/types.cf \
/etc/VRTSvcs/conf/config/types.cf.save
# cp /etc/VRTSvcs/conf/config/SybaseTypes.cf \
/etc/VRTSvcs/conf/config/SybaseTypes.cf.save
```

- 2 Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.

If not, a warning message will be displayed after installmr upgrade prechecks.

Warning: Backup `/etc/vx/cbr/bk` directory.

- 3 If you plan to continue using Storage Checkpoint or storage tiering policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, complete the following preparatory step before migrating the SFDB repository database to 6.1.1.

See [“Pre-upgrade tasks for migrating the SFDB repository database”](#) on page 43.

- 4 Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.
- 5 Stop the applications configured under VCS. Stop the Oracle RAC database:

- If the Oracle RAC instance is managed by VCS:

```
# hagrpl -offline oracle_group -sys node01
# hagrpl -offline oracle_group -sys node02
```

- If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the first half of the cluster and shut down the instances:

For Oracle RAC 12c:

```
$ srvctl stop instance -db db_name \
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \
-i instance_name
```

- 6 ■ If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts:

```
# haconf -makerw
# hagrpl -modify oracle_group AutoStart 0
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to manual:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

- 7 Unmount the CFS file systems that are not managed by VCS.
 - Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:


```
# mount | grep vxfs | grep cluster
```

```
# fuser -cu /mount_point
```
 - Unmount the non-system CFS file system:


```
# umount /mount_point
```

- 8 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:


```
# sfcache offline cache_area
```

- 9 Stop the parallel service groups and switch over failover service groups on each of the nodes in the first half of the cluster:


```
# hastop -local -evacuate
```

- 10 Unmount the VxFS file systems that are not managed by VCS.
 - Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:


```
# mount | grep vxfs
```

```
# fuser -cu /mount_point
```
 - Unmount the non-system VxFS file system:


```
# umount /mount_point
```

- 11 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.
- 12 If you plan to upgrade the operating system, stop all ports.


```
# /opt/VRTS/install/installsfrac -stop node01 node02
```

Step 2: Upgrading the first half of the cluster

Perform the following steps to upgrade the first half of the cluster.

To upgrade the first half of the cluster

- 1 If you plan to upgrade the operating system, rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

- 2 Upgrade the operating system, if required.
For instructions, see the operating system documentation.

- 3 If you upgraded the operating system, restart the nodes:

```
# shutdown -r now
```

- 4 Rename the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

- 5 Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

- 6 Upgrade SF Oracle RAC. On the first half of the cluster, upgrade SFRAC by using the `installmr` script. For example use the `installmr` script as shown below:

```
# ./installmr node01 node02
```

```
# ./installsfsybasece -upgrade node01 node02
```

Note: After you complete the upgrade of the first half of the cluster, no GAB ports will be shown in the output when you run the `gabconfig -a` command.

Step 3: Performing pre-upgrade tasks on the second half of the cluster

Perform the following pre-upgrade steps on the second half of the cluster.

To perform the pre-upgrade tasks on the second half of the cluster

- 1 Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.

Note: The downtime starts now.

- 2 If you plan to continue using Storage Checkpoint or storage tiering policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, complete the following preparatory step before migrating the SFDB repository database to 6.2.1.

See [“Pre-upgrade tasks for migrating the SFDB repository database”](#) on page 43.

- 3 Stop all applications that are configured under VCS. Stop the Oracle RAC database:

- If the Oracle RAC instance is managed by VCS:

```
# hagrps -offline oracle_group -sys node03
# hagrps -offline oracle_group -sys node04
```

- If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the second half of the cluster and shut down the instances:

For Oracle RAC 12c:

```
# srvctl stop instance -db db_name \
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \
-i instance_name
```

- 4 Unmount the CFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

```
# mount | grep vxfs | grep cluster
# fuser -cu /mount_point
```

- Unmount the non-system VxFS file system:

```
# umount /mount_point
```

- 5 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```

- 6 Stop VCS on each of the nodes in the second half of the cluster:

```
# hastop -local
```

- 7 Unmount the VxFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

```
# mount | grep vxfs
# fuser -cu /mount_point
```

- Unmount the non-system VxFS file system:

```
# umount /mount_point
```

- 8 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.

9 Stop all ports.

```
# /opt/VRTS/install/installsfrac -stop node03 node04
```

10 Stop all ports.

While upgrading from 5.0 or later:

```
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

Step 4: Performing post-upgrade tasks on the first half of the cluster

Perform the following post-upgrade steps on the first half of the cluster.

To perform the post-upgrade tasks on the first half of the cluster

1 On any one node on the first half of the cluster, force GAB to form a cluster.

```
# /etc/init.d/llt start
# /etc/init.d/gab start

# gabconfig -x
```

2 On the first half of the cluster, start SF Oracle RAC:

```
# cd /opt/VRTS/install

# ./installsfrac621 -start node01 node02
```

3 On the first half of the cluster, manually mount the VxFS or CFS file systems that are not managed by VCS.

4 Relink the SF Oracle RAC libraries with Oracle.

- 5 Bring the Oracle database service group online.

If the Oracle database is managed by VCS:

```
# hagrps -online oracle_group -sys node_name
```

If the Oracle database is not managed by VCS:

For Oracle RAC 12c:

```
$ srvctl start instance -db db_name \
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl start instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl start instance -d db_name \
-i instance_name
```

Note: The downtime ends here.

- 6 On the first half of the cluster, start all applications that are not managed by VCS. Use native application commands to start the applications.

Step 5: Upgrading the second half of the cluster

Perform the following steps to upgrade the second half of the cluster.

To upgrade the second half of the cluster

- 1 If you plan to upgrade the operating system, rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

- 2 Upgrade the operating system, if required.

For instructions, see the operating system documentation.

- 3 If you upgraded the operating system, restart the nodes:

```
# shutdown -r now
```

- 4 Rename the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

- 5 Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the first subcluster without requests for a password.
- 6 On the second half of the cluster, upgrade SF Oracle RAC. Navigate to the product directory on the installation media.

Upgrade SFRAC by using the `installmr` script. For example use the `installmr` script as shown below:

```
# ./installmr node03 node04
```

Step 6: Performing post-upgrade tasks on the second half of the cluster

Perform the following post-upgrade steps on the second half of the cluster.

To perform the post-upgrade tasks on the second half of the cluster

- 1 Manually mount the VxFS and CFS file systems that are not managed by VCS.
- 2 On the second half of the cluster, start SF Oracle RAC:

```
# cd /opt/VRTS/install
```

```
# ./installsfrac621 -start node03 node04
```

- 3 Relink the SF Oracle RAC libraries with Oracle.

4 Upgrade VxVM disk group version.

All Veritas Volume Manager disk groups have an associated version number. Each VxVM release supports a specific set of disk group versions and can import and perform tasks on disk groups with those versions. Some new features and tasks work only on disk groups with the current disk group version. Before you can perform the tasks, you need to upgrade existing disk group version to 180.

Check the existing disk group version:

```
# vxpdg list dg_name | grep -i version
```

If the disk group version is not 180, run the following command on the master node to upgrade the version:

```
# vxpdg -T 180 upgrade dg_name
```

5 Upgrade disk layout version.

In this release, you can create and mount only file systems with disk layout Version 7, 8, and 9. You can only local mount disk layout Version 6 only to upgrade to a later disk layout version.

Disk layout Version 6 has been deprecated and you cannot cluster mount an existing file system that has disk layout Version 6. To upgrade a cluster file system with disk layout Version 6, you must local mount the file system and then upgrade the file system using the `vxupgrade` utility to a later version.

See the `vxupgrade(1M)` manual page.

Support for disk layout Version 4 and 5 has been removed. You must upgrade any existing file systems with disk layout Version 4 or 5 to disk layout Version 7 or later using the `vxfsconvert` command.

See the `vxfsconvert(1M)` manual page.

Note: Symantec recommends that you upgrade existing file systems to the highest supported disk layout version prior to upgrading to this release.

You can check which disk layout version your file system has by using the following command:

```
# fstyp -v /dev/vx/dsk/dg1/vol1 | grep -i version
```

For more information about disk layout versions, see the *Symantec™ Storage Foundation Administrator's Guide*.

6 Bring the Oracle database service group online.

If the Oracle database is managed by VCS:

```
# hagrps -online oracle_group -sys node03
# hagrps -online oracle_group -sys node04
```

If the Oracle database is not managed by VCS:

For Oracle RAC 12c:

```
$ srvctl start instance -db db_name \
node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl start instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl start instance -d db_name \
-i instance_name
```

- 7** ■ If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrps -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

- 8** Start all applications that are not managed by VCS. Use native application commands to start the applications.

9 Set or change the product license level, if required.

10 Migrate the SFDB repository database.

As root, dump out the old Sybase Adaptive Server Anywhere (Sybase ASA) repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.

```
# /opt/VRTSdbed/migrate/sfua_rept_migrate
```

Upgrading to 6.2.1 on a system that has encapsulated boot disk

You can use this procedure to upgrade to 6.2.1 on a system that has encapsulated boot disk.

Note: Upgrading with encapsulated boot disk from 6.2 to 6.2.1 requires reboot.

To upgrade to 6.2.1 on a system that has encapsulated boot disk

1 If you have VxVM or VxFS cache on your system, offline the cache.

```
# sfcache offline cache_area
```

2 Manually unmount file systems and stop open volumes.

3 Upgrade to 6.2.1 using `installmr` command.

4 After upgrading, reboot the system to have the new VM drivers take effect.

5 If the mirror of boot disk is split during upgrading, re-join the mirrors manually when systems reboot after upgrading to 6.2.1.

Performing a rolling upgrade using the installer

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

- [About rolling upgrades](#)
- [Prerequisites for a rolling upgrade](#)
- [Performing a rolling upgrade on kernel packages for VCS, SFHA and SFCFSA: phase 1](#)

- [Performing a rolling upgrade on non-kernel packages for VCS, SFHA and SFCFSHA: phase 2](#)
- [Performing a rolling upgrade on kernel packages for SF Oracle RAC: phase 1](#)
- [Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2](#)

About rolling upgrades

You can use rolling upgrades to upgrade one product from a release to the next. Rolling upgrades require less downtime.

Rolling upgrades take two discrete phases. In the first, you upgrade the kernel packages with exception of VCS packages and agent packages. In the second, you upgrade the non-kernel packages, which are VCS packages and agents packages.

You can perform a rolling upgrade for the following products:

- Symantec Cluster Server
- Storage Foundation and High Availability
- Storage Foundation Cluster File System High Availability
- Storage Foundation for Oracle RAC

Prerequisites for a rolling upgrade

Meet the following prerequisites before performing a rolling upgrade:

- Make sure that the product you want to upgrade supports rolling upgrades.
- Make a plan on splitting up your clusters into sub-clusters for the purpose of upgrade. A sub-cluster can include one or more nodes. This division helps to keep service groups running during the upgrade.
- Make sure you are logged in as superuser.
- VCS must be running before performing the rolling upgrade.
- Make sure you have downloaded the latest software required for the upgrade.

Limitation: During VCS and agents upgrade, you must bring down the application High Availability (HA) for several minutes. This does not affect the application running on the cluster. You can restore the application's high availability after VCS and the agent packages are upgraded.

Performing a rolling upgrade using the installer

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

Performing a rolling upgrade on kernel packages for VCS, SFHA and SFCFSA: phase 1

Note that in the following instructions a sub-cluster can represent one or more nodes in a full cluster, but is represented by nodeA as subcluster1 and nodeB as subcluster2.

To perform the rolling upgrade on kernel packages: phase 1

- 1 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```

- 2 On the first sub-cluster, start the installer for the rolling upgrade with the `-rollingupgrade_phase1` option.

```
# ./installmr -rollingupgrade_phase1 nodeA
```

You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, start the web-based installer with the `./webinstaller start` command, select **Rolling Upgrade** from the task list, make sure the **Phase-1: Upgrade Kernel packages** radio button is checked, and then click **Next**.

- 3 Note that if the boot-disk is encapsulated, then you do not need to perform an unencapsulation for upgrades.
- 4 The installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel patches.

If you are using the web-based installer, input one node of the cluster. The web-based installer detects the whole cluster, and then recommend some nodes (NodeA) as the subcluster to run the rolling upgrade phase 1. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel packages.

- 5 The installer loads new kernel modules and starts all the relevant processes and brings all the service groups online.
- 6 If the boot disk is encapsulated, reboot the first sub-cluster's system. Otherwise go to step 7.

- 7** After rolling upgrade phase 1 is completed on nodeA, the following message displays:

It is recommended to perform rolling upgrade phase 1 on the systems nodeB in the next step.

Would you like to perform rolling upgrade phase 1 on the systems?
 [y,n,q] (y)

If you choose *y*, it continues to run rolling upgrade phase 1 by itself on nodeB.

If you choose *n* or *q*, you need to complete step 2 to step 5 on nodeB.

- 8** After rolling upgrade phase 1 of the cluster, the following message displays:

Would you like to perform rolling upgrade phase 2 on the cluster?
 [y,n,q] (y)

- If you choose *y*, it continues to run rolling upgrade phase 2 of the cluster by itself. You don't need to run phase 2:

After phase 2 upgrade, verify the cluster's status:

```
# hastatus -sum
```

- If you choose *n* or *q*, you need to use the following steps to finish rolling upgrade phase 2 of the cluster:

Performing a rolling upgrade on non-kernel packages for VCS, SFHA and SFCFSA: phase 2

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

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

- 1 Start the installer for the rolling upgrade with the `-rollingupgrade_phase2` option. Specify all the nodes in the cluster:

```
# ./installmr -rollingupgrade_phase2 nodeA nodeB nodeC nodeD
```

You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, select **Rolling Upgrade** from the task list, make sure the **Phase-2: Upgrade non Kernel packages** radio button is checked, and then click **Next**.

- 2 The installer checks system communications, patch versions, product versions, and completes prechecks. It upgrades non-kernel patches. It also verifies completion of phase 1.

If you are using the web-based installer, input one node of the cluster, the web-based installer detects the whole cluster to run the rolling upgrade phase 2. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.

- 3 Installer will start HA daemon (had) on all nodes, HA will be available once HA daemon is up.
- 4 Verify the cluster's status:

```
# hastatus -sum
```

- 5 If you want to upgrade CP server systems that use VCS or SFHA to 6.2, make sure that you upgraded all application clusters to version 6.2. Then, upgrade VCS or SFHA on the CP server systems.

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

Performing a rolling upgrade on kernel packages for SF Oracle RAC: phase 1

Note that in the following instructions that a subcluster can represent one or more nodes in a full cluster, but is represented by nodeA, nodeB as subcluster1 and nodeC, nodeD as subcluster2.

To perform the rolling upgrade on kernel: phase 1

- 1 Log in as superuser to one of the nodes in the cluster.
- 2 Back up the following configuration files on your system: `main.cf`, `types.cf`, `CVMTTypes.cf`, `CFSTypes.cf`, `OracleTypes.cf`, `OracleASMTTypes.cf`, `PrivNIC.cf`, `MultiPrivNIC.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmode`.

For example:

```
# cp /etc/VRTSvcs/conf/config/main.cf \
    /etc/VRTSvcs/conf/config/main.cf.save
```

- 3
 - If the Oracle database is managed by VCS, set the `AutoStart` value to 0 to prevent the database service group from starting automatically when VCS starts. Failing to perform this step results in the database attempting to come online after the upgrade; the attempt fails due to the presence of old libraries on the system.

```
# haconf -makerw
# hagrpl -modify oracle_group AutoStart 0
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to manual:

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

- 4 Stop the applications that use VxFS or VxVM disk groups on each node, whether local or CFS.

If the applications are under VCS control:

```
# hagrpl -offline grp_name -sys node_name
```

If the applications are not under VCS control:

Use native application commands to stop the application.

- 5 Stop the Oracle RAC resources on each node.

- If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:

```
# hagrps -offline oracle_group -sys nodeA
# hagrps -offline oracle_group -sys nodeB
```

- If the database instances are not managed by VCS, then run the following on one node:

For Oracle RAC 12 c:

```
$ srvctl stop instance -db db_name -node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \
-i instance_name
```

- 6 Switch over all failover service groups to the other nodes in the cluster:

```
# hagrps -switch grp_name -to node_name
```

- 7 Take all the VCS service groups offline:

```
# hagrps -offline grp_name -sys node_name
```

- 8 Unmount all the VxFS file system which is not under VCS control.

```
# mount |grep vxfs
# fuser -m /mount_point
# umount /mount_point
```

Make sure that no processes are running which make use of mounted shared file system or shared volumes.

```
# fuser -cu /mount_point
```

Note: Installer will automatically stop all the applications, database instances, filesystems and volumes which are under VCS control on nodes, while using the `rollingupgrade_phase1` option.

- 9 On the sub-cluster, start the installer for the rolling upgrade with the `-rollingupgrade_phase1` option.

```
# ./installmr -rollingupgrade_phase1 nodeA nodeB
```

You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, start the web-based installer with the `./webinstaller start` command, select **Rolling Upgrade** from the task list, make sure the **Phase-1: Upgrade Kernel packages** radio button is checked, and then click **Next**.

- 10 Note that if the boot-disk is encapsulated, you do not need to perform an unencapsulation for upgrades.
- 11 The installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel patches.

If you are using the web-based installer, input one node of the cluster. The web-based installer detects the whole cluster, and then recommend some nodes (NodeA) as the subcluster to run the rolling upgrade phase 1. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel.

- 12 Relink the SF Oracle RAC libraries with Oracle:

Choose the option **Relink Oracle Database Binary** from the program menu.

- 13 When prompted, choose the option " Continue Rolling Upgrade " from the menu:

```
1) Relink Oracle Database Binary
   2) Continue Rolling Upgrade
```

```
Choose option: [1-2,q] (1) 2
```

- 14 If the boot disk is encapsulated, the installer strongly recommends a reboot of the nodes. Reboot the nodes as prompted by the installer.
- 15 For minimal down time, bring the oracle groups and database up manually on subcluster on which phase 1 is completed:

- If the database instances are managed by VCS, take the corresponding VCS service groups online. As superuser, enter:

```
# hagrps -online oracle_group -sys nodeA
```

```
# hagrps -online oracle_group -sys nodeB
```

- If the database instances are not managed by VCS, then run the following on one node:

For Oracle RAC 12c:

```
# srvctl start instance -db db_name \  
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
# $ srvctl start instance -d db_name \  
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
# $ srvctl start instance -d db_name \  
-i instance_name
```

16 Manually mount the VxFS and CFS file systems that are not managed by VCS.

17 Bring the Oracle database service group online.

- If VCS manages the Oracle database:

```
# hagrps -online oracle_group -sys node_name
```

- If VCS does not manage the Oracle database:

For Oracle RAC 12c:

```
$ srvctl start instance -db db_name \  
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl start instance -d db_name \  
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl start instance -d db_name \  
-i instance_name
```

18 Start all applications that are not managed by VCS. Use native application commands to start the applications.

19 After rolling upgrade phase 1 is completed on nodeA and nodeB, the following message displays:

It is recommended to perform rolling upgrade phase 1 on the systems nodeC and nodeD in the next step.

Would you like to perform rolling upgrade phase 1 on the systems?
 [y,n,q] (y)

- If you choose `y`, first complete step 4 to step 8 on the remaining subcluster. Then it continues to run rolling upgrade phase 1 on nodeC and nodeD by itself.
- If you choose `n` or `q`, go to step 15.

20 After rolling upgrade phase 1 of the cluster, the following message displays:

Would you like to perform rolling upgrade phase 2 on the cluster?
 [y,n,q] (y)

- If you choose `y`, it continues to run rolling upgrade phase 2 of the cluster by itself. You don't need to run phase 2: See ["Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2"](#) on page 151. After rolling upgrade phase 2, complete step 19 to step 22 (except step 21) verify the cluster's status:

```
# hastatus -sum
```

- If you choose `n` or `q`, you need to complete step 19 to step 22 and run rolling upgrade phase 2: See ["Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2"](#) on page 151.

21 Before you proceed to phase 2, complete step 4 to 18 on the remaining subcluster.

22 Perform one of the following steps:

- If VCS manages the Oracle database, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrps -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If the VCS does not manage the Oracle database, change the management policy for the database to automatic:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2

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

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

- 1 Start the installer for the rolling upgrade with the `-rollingupgrade_phase2` option. Specify all the nodes in the cluster:

```
./installmr -rollingupgrade_phase2 nodeA nodeB nodeC nodeD
```

You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, select **Rolling Upgrade** from the task list, make sure the **Phase-2: Upgrade non Kernel packages** radio button is checked, and then click **Next**.

- 2 The installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.
If you are using the web-based installer, input one node of the cluster, the web-based installer detects the whole cluster to run the rolling upgrade phase 2. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.
- 3 Installer will start HA daemon (had) on all nodes, HA will be available once HA daemon is up.
- 4 Verify the cluster's status:

```
# hastatus -sum
```

Upgrading the operating system

This section describes how to upgrade the operating system on a Symantec Storage Foundation and High Availability Solutions (SFHA) node where you plan to upgrade to 6.2.1 for Red Hat Enterprise Linux (RHEL) 6, RHEL 7, RHEL 7.1, SUSE Linux Enterprise (SLES) 11, Oracle Linux (OL) 6, and OL 7.

Preparing for OS upgrades

- 1 Rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

- 2 Upgrade the operating system on all nodes in the cluster.
For instructions, see the operating system documentation.

Note: If required, restart the nodes with the `shutdown -r now` command.

- 3 After the system restarts, restore the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

To upgrade the operating system to a later version

- 1 Stop Storage Foundation.
- 2 Upgrade to the latest operating system.
- 3 Upgrade to 6.2.1.
- 4 Start Storage Foundation.

Upgrading SFHA with the Veritas Web-based installer

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

To perform a full upgrade for SFHA

- 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.
- 3 On the **Select a task and a product** page, select **Install 6.2.1** from the **Task** drop-down list, and click **Next**. Or select **Rolling Upgrade** to perform a rolling upgrade via the webinstaller
- 4 Stop all applications accessing the file system. Unmount all mounted filesystems before installation.

- 5 Indicate the systems on which to upgrade. Enter one or more system names, separated by spaces. Click **Next**.

The installer detects the product that is installed on the specified system.

- 6 The installer stops the processes. Choose to restore and reuse the previous configuration on all systems. Click **Next** to start the processes.

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

To perform a rolling upgrade with Veritas Web-based installer, refer to 6.2 Installation Guides for your products.

Verifying software versions

To list the Symantec RPMs installed on your system, enter the following command:

```
# rpm -qa | grep VRTS
```

The output version for 6.2.1 is 6.2.1.000, and the VRTSperl version is 5.16.1.27.

Removing Symantec Storage Foundation and High Availability Solutions

This chapter includes the following topics:

- [About removing Symantec Storage Foundation and High Availability Solutions 6.2.1](#)
- [Uninstalling Symantec Storage Foundation Cluster File System High Availability 6.2.1](#)
- [Uninstalling Symantec Storage Foundation for Oracle RAC 6.2.1](#)

About removing Symantec Storage Foundation and High Availability Solutions 6.2.1

Symantec recommends that you follow the steps in the following sections to remove all the installed Symantec software, and then perform a complete reinstallation of the previous release.

For extensive uninstallation and reinstallation procedures, refer to the appropriate product's Installation Guide.

Uninstalling Symantec Storage Foundation Cluster File System High Availability 6.2.1

This section provides procedures for uninstalling Symantec Storage Foundation Cluster File System High Availability (SFCFSHA). You must complete the preparatory tasks before you uninstall SFCFS.

Preparing to uninstall Symantec Storage Foundation Cluster File System High Availability

The following procedure prepares your system for uninstalling Symantec Storage Foundation Cluster File System High Availability (SFCFSHA).

To prepare to uninstall Symantec Storage Foundation Cluster File System High Availability

- 1 Log in as the root user on any node in the cluster.
- 2 Verify that the following directories are set in your `PATH` environment variable:

```
/opt/VRTS/bin
/opt/VRTSvcs/bin
```

- 3 Back up the following configuration files:

```
# mv /etc/llttab /etc/llttab.`date +%m-%d-%y_%H-%M-%S`
# mv /etc/llthosts /etc/llthosts.`date +%m-%d-%y_%H-%M-%S`
# mv /etc/gabtab /etc/gabtab.`date +%m-%d-%y_%H-%M-%S`
# mv /etc/vxfenmode /etc/vxfenmode.`date +%m-%d-%y_%H-%M-%S`
```

- 4 Determine if each node's root disk is under VxVM control and proceed as follows.
 - Check if each node's root disk is under VxVM control:

```
# df -v /
```

The root disk is under VxVM control if `/dev/vx/dsk/rootvol` is listed as being mounted as the root (`/`) file system. If so, unmirror and unencapsulate the root disk as described in the following steps:

- If the encapsulated root disk is mirrored, use the `vxrootadm` command to split the mirror.

For example, the following command removes a root disk mirror from the current root disk group:

```
# vxrootadm -Yv rmmirror rootdg_01-s0
```

- Enter the following command to convert all the encapsulated volumes in the root disk back to being accessible directly through disk partitions instead of through volume devices.

```
# /etc/vx/bin/vxunroot
```

Following the removal of encapsulation, the system is rebooted from the unencapsulated root disk.

- 5 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the `vxrvrg stop` command to stop each RVG individually:

```
# vxrvrg -g diskgroup stop rvg_name
```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

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

- 6 Check if any VxFS file systems or Storage Checkpoints are mounted:

```
# df -T | grep vxfs
```

- 7 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint1
```

```
# umount /filesystem1
```

If file system is mounted in a cluster, then use `cfsumount` command.

- 8 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g dg1 stopall
```

To verify that no volumes are open:

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

- 9 Stop VCS:

```
# hastop -all
```

Uninstalling Symantec Storage Foundation Cluster File System High Availability

The following procedure uninstalls Symantec Storage Foundation Cluster File System High Availability (SFCFSHA).

To uninstall Symantec Storage Foundation Cluster File System High Availability

- 1 Log in as the root user on any node in the cluster.
- 2 Navigate to the directory that contains the uninstallation program:

```
# cd /opt/VRTS/install
```

- 3 Run the uninstallation program while specifying each node in the cluster:

```
# ./uninstallsfcfsha62 node01 node02
```

- 4 Confirm the uninstallation:

```
Are you sure you want to uninstall SFCFSHA [y,n,q] (y)
```

The installer stops the Symantec Storage Foundation Cluster File System High Availability processes and uninstalls the packages.

After uninstalling the Symantec Storage Foundation Cluster File System High Availability, refer to the *Symantec™ Storage Foundation Cluster File System High Availability 6.2.1 Installation Guide* to reinstall the 6.2.1 software.

Uninstalling Symantec Storage Foundation for Oracle RAC 6.2.1

The following procedure uninstalls Symantec Storage Foundation for Oracle RAC (SFRAC).

Note: This procedure will remove the complete SFRAC stack from all nodes.

To uninstall Symantec Storage Foundation for Oracle RAC

- 1 On each node, take the Oracle resources in the VCS configuration file (`main.cf`) offline.

```
# hagrps -offline oracle_group -sys node_name
```

If the database is not managed by VCS, stop the Oracle database as follows:

```
$ srvctl stop database -d db_name
```

- 2 If Oracle Clusterware is not under VCS Control, then enter the following command on each node of the cluster to stop Oracle Clusterware.

- For 11gR2 and 12c:

```
# /etc/init.d/ohasd stop
```

- 3 Stop the applications that use CVM or CFS that are not under VCS control

- Using native application commands, stop the applications that use CVM or CFS on all nodes.
- Verify that no processes use the CFS mount point:

```
# fuser -c /mount_point
```

- 4 Unmount CFS file systems that are not under VCS control

- Determine the file systems that need to be unmounted by checking the output of mount command.

```
# mount -v | grep vxfs | grep cluster
```

- Unmount each file system that is not controlled by VCS on each node:

```
# umount /mount_point
```

- 5 If you have VxVM or VxFS cache on your system, offline the cache before uninstallation:

```
# sfcache offline cache_area
```

- 6 Stop VCS to take the service groups on all nodes offline
 On any one node execute following command to stop VCS:

```
# hastop -all
```

- 7 Stopping the applications that use VxVM or VxFS that are not under VCS control

- Using native application commands, stop the applications that use VxVM or VxFS.
- Verify that no processes use the VxFS mount point:

```
# fuser -c /mount_point
```

- 8 Unmounting VxFS file systems that are not under VCS control.

- Determine the file systems that need to be unmounted by checking the output of mount command.

```
# mount -v | grep vxfs
```

Unmount each file system that is not controlled by VCS on each node:

```
# umount /mount_point
```

- 9 Remove SF for Oracle RAC.

- On any one node, navigate to the directory that contains the uninstallsfrac program:

```
# cd /opt/VRTS/install
```

- Start the uninstallsfrac program:

```
# ./uninstallsfrac62
```

- 10 After uninstalling the SF Oracle RAC, refer to the chapter of *Installing the products for the first time* in this document to reinstall the SF Oracle RAC 6.2.1 software.

About the installation script

This appendix includes the following topics:

- [About the installation script](#)

About the installation script

Symantec™ Storage Foundation and High Availability Solutions 6.2.1 provides an installation and upgrade script. To install or upgrade the patches that are included in this release, you can use the `installmr` script. The `installmr` script lets you install or upgrade all the patches that are associated with the packages installed.

For more information regarding installation,

Symantec has introduced a new Install Bundles feature to help you install or upgrade directly to maintenance level with one execution. You can use the `-base_path` option to install or upgrade base and maintenance bundles. There are a few prerequisites for using Install Bundles feature for installation and upgrade of 6.2.1 mentioned below:

The installmr script options

The following table lists the command line options for the `installmr` and upgrade script:

Table A-1 The command line options for the product `installmr` script

| Command Line Option | Function |
|---------------------------------|---|
| <code>system1 system2...</code> | Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name. |

Table A-1 The command line options for the product installmr script
(continued)

| Command Line Option | Function |
|---------------------|---|
| -base_path | The <i>-base_path</i> option is used to define the path of a base level release to be integrated with a maintenance level release in order for the two releases to be simultaneously installed. |
| -patch_path | Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |
| -patch2_path | Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |
| -patch3_path | Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |
| -patch4_path | Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |
| -patch5_path | Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |
| -precheck | Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product. |
| -postcheck | Checks any issues after installation or upgrading on the system. |

Table A-1 The command line options for the product `installmr` script
(continued)

| Command Line Option | Function |
|--|---|
| <code>-responsefile response_file</code> | Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The <code>response_file</code> must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. |
| <code>-logpath log_path</code> | Specifies a directory other than <code>/opt/VRTS/install/logs</code> as the location where installer log files, summary files, and response files are saved. |
| <code>-tmppath tmp_path</code> | Specifies a directory other than <code>/var/tmp</code> as the working directory for the installation scripts. This destination is where initial logging is performed and where RPMs are copied on remote systems before installation. |
| <code>-timeout timeout_value</code> | The <code>-timeout</code> option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the <code>-timeout</code> option overrides the default value of 1200 seconds. Setting the <code>-timeout</code> option to 0 will prevent the script from timing out. The <code>-timeout</code> option does not work with the <code>-serial</code> option. |
| <code>-keyfile ssh_key_file</code> | Specifies a key file for secure shell (SSH) installs. This option passes <code>-i ssh_key_file</code> to every SSH invocation. |
| <code>-hostfile full_path_to_file</code> | Specifies the location of a file that contains a list of hostnames on which to install. |

Table A-1 The command line options for the product installmr script
(continued)

| Command Line Option | Function |
|---|--|
| <code>-kickstart <i>dir_path</i></code> | Produces a kickstart configuration file for installing with Linux RHEL Kickstart. The file contains the list of Symantec RPMs in the correct order for installing, in a format that can be used for Kickstart installations. The <i>dir_path</i> indicates the path to the directory in which to create the file. |
| <code>-yumgroupxml</code> | The <code>-yumgroupxml</code> option is used to generate a yum group definition XML file. The <code>createrepo</code> command can use the file on Redhat Linux to create a yum group for automated installation of all rpms for a product. An available location to store the XML file should be specified as a complete path. The <code>-yumgroupxml</code> option is supported on Redhat Linux only. |
| <code>-require</code> | The <code>-require</code> option is used to specify a installer hot fix file. |
| <code>-serial</code> | Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems. |
| <code>-rsh</code> | Specifies this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP. |
| <code>-redirect</code> | Displays progress details without showing the progress bar. |
| <code>-pkgset</code> | Discovers and displays the RPM group (minimum, recommended, all) and RPMs that are installed on the specified systems. |
| <code>-pkgtable</code> | Displays product's RPMs in correct installation order by group. |
| <code>-listpatches</code> | The <code>-listpatches</code> option displays product patches in correct installation order. |

Table A-1 The command line options for the product `installmr` script
(continued)

| Command Line Option | Function |
|-------------------------------------|---|
| <code>-makeresponsefile</code> | Use the <code>-makeresponsefile</code> option only to generate response files. No actual software installation occurs when you use this option. |
| <code>-comcleanup</code> | The <code>-comcleanup</code> option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated. |
| <code>-version</code> | Checks and reports the installed products and their versions. Identifies the installed and missed RPMs and patches where applicable for the product. Provides a summary that includes the count of the installed and any missed RPMs and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available. |
| <code>-nolic</code> | Allows installation of product RPMs without entering a license key. Licensed features cannot be configured, started, or used when this option is specified. |
| <code>-rolling_upgrade</code> | Starts a rolling upgrade. Using this option, the installer detects the rolling upgrade status on cluster systems automatically without the need to specify rolling upgrade phase 1 or phase 2 explicitly. |
| <code>-rollingupgrade_phase1</code> | The <code>-rollingupgrade_phase1</code> option is used to perform rolling upgrade Phase-I. In the phase, the product kernel RPMs get upgraded to the latest version |

Table A-1 The command line options for the product installmr script
(continued)

| Command Line Option | Function |
|-----------------------------|--|
| -rollingupgrade_phase2 | The <code>-rollingupgrade_phase2</code> option is used to perform rolling upgrade Phase-II. In the phase, VCS and other agent RPMs upgrade to the latest version. Product kernel drivers are rolling-upgraded to the latest protocol version." |
| -disable_dmp_native_support | Disables Dynamic multi-pathing support for native the LVM volume groups/ZFS pools during an upgrade. Retaining Dynamic multi-pathing support for the native LVM volume groups/ZFS pools during an upgrade increases package upgrade time depending on the number of LUNs and native LVM volume groups/ZFS pools configured on the system. The <code>-disable_dmp_native_support</code> option is supported in upgrade scenario only. |
| -noipc | Disables the installer from making outbound networking calls to Symantec Operations Readiness Tool (SORT) in order to automatically obtain hot fixes and release information updates. |

Installing and configuring SFSYBASECE on RHEL 6

- [Chapter 6. Installation overview and planning](#)
- [Chapter 7. Preparing to install SF Sybase CE](#)
- [Chapter 8. Installation of SF Sybase ASE CE using the script-based installer](#)
- [Chapter 9. Managing your Symantec deployments](#)
- [Chapter 10. Post-installation tasks](#)
- [Chapter 11. Installing and configuring Sybase ASE CE](#)
- [Chapter 12. Automated installation using response files](#)
- [Chapter 13. Adding and removing nodes](#)
- [Chapter 14. Configuration of disaster recovery environments](#)
- [Chapter 15. Uninstallation of Sybase ASE CE](#)
- [Appendix B. SF Sybase CE installation RPMs](#)
- [Appendix C. Installation scripts](#)
- [Appendix D. Sample installation and configuration values](#)

- [Appendix E. Tunable files for installation](#)
- [Appendix F. Configuration files](#)
- [Appendix G. Configuring the secure shell or the remote shell for communications](#)
- [Appendix H. High availability agent information](#)
- [Appendix I. Compatibility issues when installing Storage Foundation for Sybase ASE CE with other products](#)

Installation overview and planning

This chapter includes the following topics:

- [Introducing SF Sybase ASE CE](#)
- [System requirements](#)
- [Planning to install SF Sybase ASE CE](#)
- [Licensing SF Sybase ASE CE](#)

Introducing SF Sybase ASE CE

About Symantec Storage Foundation for Sybase ASE CE

Symantec Storage Foundation™ for Sybase® Adaptive Server Enterprise Cluster Edition (SF Sybase CE) by Symantec leverages proprietary storage management and high availability technologies to enable robust, manageable, and scalable deployment of Sybase ASE CE on UNIX and Linux platforms. The solution uses cluster file system technology that provides the dual advantage of easy file system management as well as the use of familiar operating system tools and utilities in managing databases.

SF Sybase CE integrates existing Symantec storage management and clustering technologies into a flexible solution which administrators can use to:

- Create a standard toward application and database management in data centers. SF Sybase CE provides flexible support for many types of applications and databases.

- Set up an infrastructure for Sybase ASE CE that simplifies database management while fully integrating with Sybase ASE CE clustering solution.
- Apply existing expertise of Symantec technologies toward this product.

The solution stack comprises the Symantec Cluster Server (VCS), Veritas Cluster Volume Manager (CVM), Veritas Cluster File System (CFS), and Symantec Storage Foundation, which includes the base Veritas Volume Manager (VxVM) and Veritas File System (VxFS).

Note: SF Sybase ASE CE 6.2.1 doesn't support upgrading from previous releases on RHEL 6.

Benefits of SF Sybase CE

SF Sybase CE provides the following benefits:

- Use of a generic clustered file system (CFS) technology or a local file system (VxFS) technology for storing and managing SF Sybase CE installation binaries.
- Support for file system-based management. SF Sybase CE provides a generic clustered file system technology for storing and managing Sybase ASE CE data files as well as other application data.
- Use of Cluster File System (CFS) for the Sybase ASE CE quorum device.
- Support for a standardized approach toward application and database management. A single-vendor solution for the complete SF Sybase CE software stack lets you devise a standardized approach toward application and database management. Further, administrators can apply existing expertise of Veritas technologies toward SF Sybase CE.
- Easy administration and monitoring of SF Sybase CE clusters using Veritas Operations Manager.
- Enhanced scalability and availability with access to multiple Sybase ASE CE instances per database in a cluster.
- Prevention of data corruption in split-brain scenarios with robust SCSI-3 Persistent Reservation (PR) based I/O fencing.
- Support for sharing all types of files, in addition to Sybase ASE CE database files, across nodes.
- Increased availability and performance using Symantec Dynamic Multi-Pathing (DMP). DMP provides wide storage array support for protection from failures and performance bottlenecks in the Host Bus Adapters (HBAs) and Storage Area Network (SAN) switches.

- Fast disaster recovery with minimal downtime and interruption to users. Users can transition from a local high availability site to a wide-area disaster recovery environment with primary and secondary sites. If a node fails, clients that are attached to the failed node can reconnect to a surviving node and resume access to the shared database. Recovery after failure in the SF Sybase CE environment is far quicker than recovery for a failover database.
- Support for block-level replication using VVR.

About SF Sybase CE components

SF Sybase CE manages database instances running in parallel on multiple nodes using the following architecture and communication mechanisms to provide the infrastructure for SF Sybase CE.

Table 6-1 SF Sybase CE component products

| Component product | Description |
|-------------------------------|--|
| Cluster Volume Manager (CVM) | Enables simultaneous access to shared volumes based on technology from Veritas Volume Manager (VxVM). |
| Cluster File System (CFS) | Enables simultaneous access to shared file systems based on technology from Veritas File System (VxFS). |
| Symantec Cluster Server (VCS) | Uses technology from Symantec Cluster Server to manage SF Sybase CE databases and infrastructure components. |
| VXFEN | The VCS module prevents cluster corruption through the use of SCSI3 I/O fencing, where the vxfen mode is set to sybase. |
| VXFEND | The VXFEN daemon communicates directly with VCMP and relays membership modification messages. |
| VCMP | VCMP provides interface between Sybase cluster and the SF Sybase CE components. |
| QRMUTIL | QRMUTIL provides Sybase instance status. |
| Sybase agent | The VCS agent is responsible for bringing Sybase ASE online, taking it offline, and monitoring it.. It obtains status by checking for processes, performing SQL queries on a running database, and interacting with QRMUTIL. |

About SF Sybase ASE CE optional features

You can configure the following optional features in an SF Sybase ASE CE cluster:

- VCS notifications
- Global clusters
See [“About global clusters”](#) on page 171.
- Symantec Replicator Option
See [“About Symantec Replicator Option”](#) on page 171.
- I/O fencing
See [“About I/O fencing”](#) on page 172.

Note: I/O fencing is mandatory in SF Sybase ASE CE installations. All other features are optional and may be configured to suit your business needs.

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 *Symantec Cluster Server Administrator’s Guide* for details on configuring these notifications.

About global clusters

Global clusters provide the ability to fail over applications between geographically distributed clusters when disaster occurs. This type of clustering involves migrating applications between clusters over a considerable distance. You can set up HA/DR using software-based replication technologies.

You are required to have a separate license to configure global clusters. You may add this license during the installation or at any time after the installation completes.

About Symantec Replicator Option

Symantec Replicator Option is an optional, separately-licensable feature.

Volume Replicator (VVR) replicates data to remote locations over any standard IP network to provide continuous data availability. It is a fully integrated component of Veritas Volume Manager (VxVM).

VVR replicates the application writes on the volumes at the source location to one or more remote locations across any distance. It provides a consistent copy of application data at the remote locations. If a disaster occurs at the source location, you can use the copy of the application data at the remote location and restart the application at the remote location. The host at the source location on which the application is running is known as the Primary host. The host at the target location is known as the Secondary host. You can have up to 32 Secondary hosts in a VVR environment. VVR provides several methods to initialize the application data between the primary location and the remote location. Some of the methods include using the network, using the tape backup, and moving the disks physically.

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, part of VRTSvxfen RPM, when you install SF Sybase CE. To protect data on shared disks, you must configure I/O fencing after you install and configure SF Sybase CE.

With disk-based I/O fencing, coordination points can be coordinator disks only.

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

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

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

See the *Symantec Storage Foundation and High Availability Administrator's Guide* for more details.

About Cluster Manager (Java Console)

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

See *Symantec Cluster Server Administrator's Guide*.

You can download the console from <http://www.symantec.com/operations-manager/support>.

About Veritas Operations Manager

Veritas Operations Manager provides a centralized management console for Symantec Storage Foundation and High Availability products. You can use Veritas Operations Manager to monitor, visualize, and manage storage resources and generate reports.

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

You can download Veritas Operations Manager from <http://go.symantec.com/vom>.

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

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

If you want to manage a single cluster using Cluster Manager (Java Console), a version is available for download from <http://www.symantec.com/operations-manager/support>. You cannot manage the new features of this release using the Java Console. Symantec Cluster Server Management Console is deprecated.

About Symantec Operations Readiness Tools

[Symantec Operations Readiness Tools \(SORT\)](#) is a website that automates and simplifies some of the most time-consuming administrative tasks. It helps you identify risks in your datacenters and improve operational efficiency, enabling you to manage the complexity that is associated with datacenter architectures and scale.

Table 6-2 lists three major datacenter tasks and the SORT tools that can help you accomplish them.

Table 6-2 Datacenter tasks and the SORT tools

| Task | SORT tools |
|--|--|
| Prepare for installations and upgrades | <ul style="list-style-type: none"> ■ Installation and Upgrade checklists Display system requirements including memory, disk space, and architecture. ■ Installation and Upgrade custom reports Create reports that determine if you're ready to install or upgrade a Symantec enterprise product. ■ Array-specific Module Finder List the latest Array Support Libraries (ASLs) and Array Policy Modules (APMs) for UNIX servers, and Device Driver Installers (DDIs) and Device Discovery Layers (DDLs) for Windows servers. ■ High Availability Agents table Find and download the agents for applications, databases, replication, and Symantec partners. |
| Identify risks and get server-specific recommendations | <ul style="list-style-type: none"> ■ Patch notifications Receive automatic email notifications about patch updates. (Sign in required.) ■ Risk Assessment check lists Display configuration recommendations based on your Symantec product and platform. ■ Risk Assessment custom reports Create reports that analyze your system and give you recommendations about system availability, storage use, performance, and best practices. ■ Error code descriptions and solutions Display detailed information on thousands of Symantec error codes. |

Table 6-2 Datacenter tasks and the SORT tools (*continued*)

| Task | SORT tools |
|--------------------|--|
| Improve efficiency | <ul style="list-style-type: none"> <li data-bbox="673 326 1220 413">■ Patch Finder List and download patches for your Symantec enterprise products. <li data-bbox="673 421 1220 534">■ License/Deployment custom reports Create custom reports that list your installed Symantec products and license keys. Display licenses by product, platform, server tier, and system. <li data-bbox="673 543 1220 630">■ Symantec Performance Value Unit (SPVU) Calculator Use the calculator to assist you with the pricing meter transition. <li data-bbox="673 638 1220 751">■ Documentation List and download Symantec product documentation, including manual pages, product guides, and support articles. <li data-bbox="673 760 1220 847">■ Related links Display links to Symantec product support, forums, customer care, and vendor information on a single page. |

SORT is available at no additional charge.

To access SORT, go to:

<https://sort.symantec.com>

SF Sybase CE cluster setup models

SF Sybase CE supports a variety of cluster configurations.

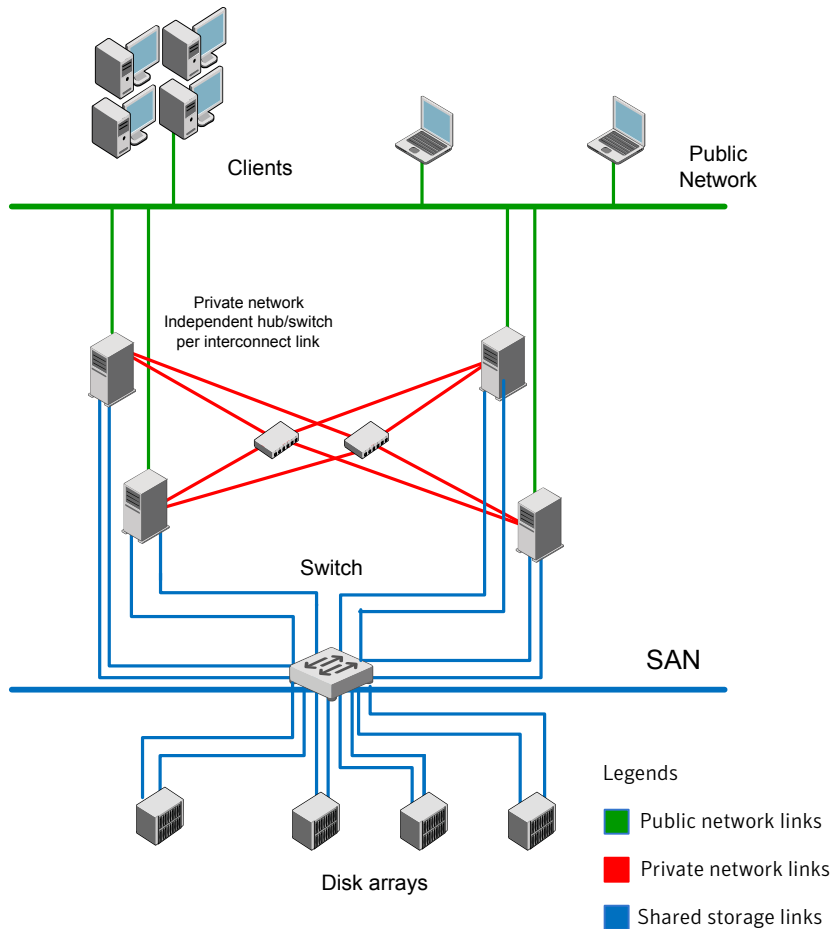
Depending on your business needs, you may choose from the following setup models:

- Basic setup
- Secure setup
- Central management setup
- Global cluster setup

Typical configuration of four-node SF Sybase CE cluster

[Figure 6-1](#) depicts a high-level view of a basic SF Sybase CE configuration for a four-node cluster.

Figure 6-1 Sample four-node SF Sybase CE cluster



A basic topology has the following layout and characteristics:

- Multiple client applications that access nodes in the cluster over a public network.
- Nodes that are connected by at least two private network links (also called cluster interconnects) using 100BaseT or gigabit Ethernet controllers on each system, using similar network devices and matching port numbers.
 For example, if you use net1 on one end of a link, it is recommended that you use net1 on the other end too.
 If the private links are on a single switch, isolate them using VLAN.
- Nodes that are connected to iSCSI or Fibre Channel shared storage devices over SAN.

All shared storage must support SCSI-3 PR.

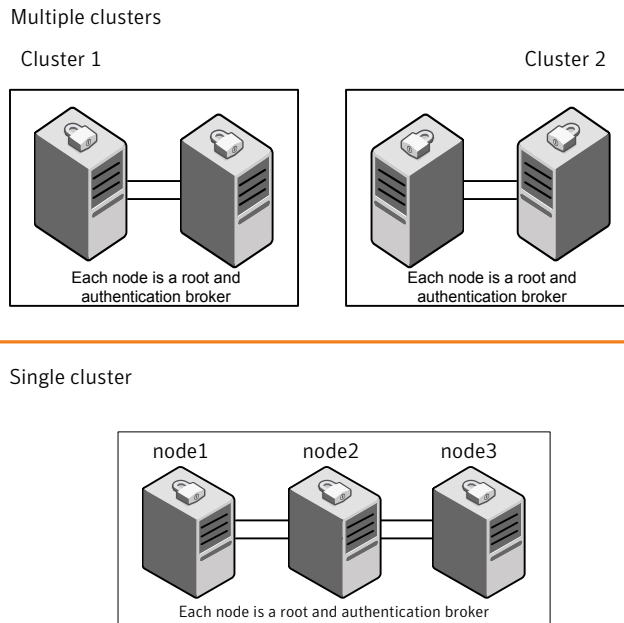
- The quorum and Sybase datafile disks configured on the shared storage that is available to each node.
 Disks for Sybase ASE CE binary can be configured either on shared storage or on local storage.
 For shared storage:
See [Preparing for shared mount point on CFS for Sybase ASE CE binary installation](#) in this document.
 For local storage:
See [Preparing for local mount point on VxFS for Sybase ASE CE binary installation](#) in this document.
- VCS manages the resources that are required by Sybase ASE CE. The resources must run in parallel on each node.

Typical configuration of SF Sybase CE clusters in secure mode

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

[Figure 6-2](#) illustrates typical configuration of SF Sybase CE clusters in secure mode.

Figure 6-2 Typical configuration of SF Sybase CE clusters in secure mode

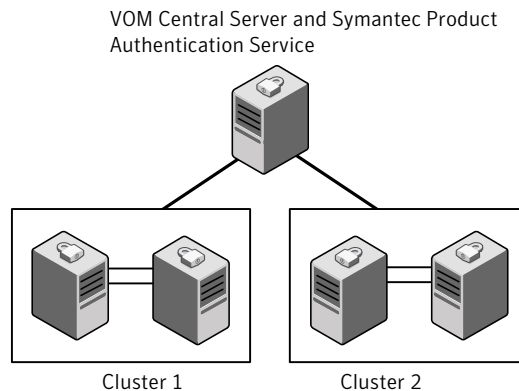


Typical configuration of VOM-managed SF Sybase CE clusters

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

Figure 6-3 illustrates a typical setup of SF Sybase CE clusters that are centrally managed using Veritas Operations Manager.

Figure 6-3 Typical configuration of VOM-managed clusters

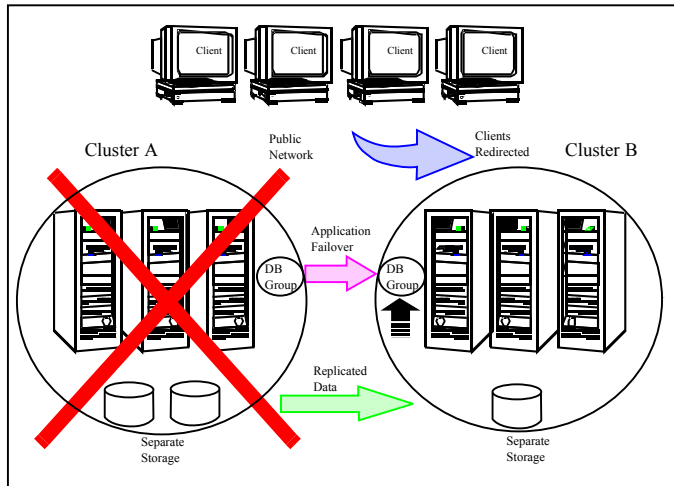


Typical configuration of SF Sybase CE global clusters for disaster recovery

SF Sybase CE leverages the global clustering feature of VCS to enable high availability and disaster recovery (HA/DR) for businesses that span wide geographical areas. Global clusters provide protection against outages caused by large-scale disasters such as major floods, hurricanes, and earthquakes. An entire cluster can be affected by such disasters. This type of clustering involves migrating applications between clusters over a considerable distance.

You can set up HA/DR using software-based replication technologies.

Figure 6-4 Global clusters



To understand how global clusters work, review the example of an Sybase ASE CE database configured using global clustering. Sybase ASE CE is installed and configured in cluster A and cluster B. Sybase ASE CE database is located on shared disks within each cluster and is replicated across clusters to ensure data concurrency. The VCS service groups for Sybase ASE CE are online on cluster A and are configured to fail over to cluster B.

Note: You must have an SF Sybase CE HA/DR license to configure global clusters. If you use VVR for replication, you must also have a VVR license. You may configure a basic cluster initially and add the HA/DR and VVR licenses at a later time or you may add the licenses during the SF Sybase CE installation.

For information on supported replication technologies:

Supported replication technologies

SF Sybase CE supports software-based replication technologies.

Veritas Volume Replicator (VVR) replicates data to remote sites over any standard IP network. You can have up to 32 secondary hosts in a VVR environment.

The supported software-based replication technologies are as follows:

- Veritas Volume Replicator (VVR)
 - A VVR environment supports up to 32 secondary hosts.

System requirements

Release notes

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

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

<https://sort.symantec.com/documents>

Important preinstallation information for SF Sybase CE

Before you install SF Sybase CE, make sure that you have reviewed the following information:

- Preinstallation checklist for your configuration. Go to [the SORT installation checklist tool](#). From the drop-down lists, select the information for the Symantec product you want to install, and click **Generate Checklist**.
- Hardware compatibility list for information about supported hardware: <http://www.symantec.com/docs/TECH211575>
- For important updates regarding this release, review the Late-Breaking News Technote on the Symantec Technical Support website: <http://www.symantec.com/docs/TECH211540>
- Sybase documentation for additional requirements pertaining to your version of Sybase.

Hardware requirements

[Table 6-3](#) lists the hardware requirements for SF Sybase CE.

Table 6-3 Hardware requirements for basic clusters

| Item | Description |
|----------------------|--|
| SF Sybase CE systems | Two to four systems with two or more CPUs. For details on the additional requirements for Sybase, see the Sybase documentation. |
| DVD drive | A DVD drive on one of the nodes in the cluster. |

Table 6-3 Hardware requirements for basic clusters (*continued*)

| Item | Description |
|---|--|
| Disks | <p>SF Sybase CE requires that all shared storage disks support SCSI-3 Persistent Reservations (PR).</p> <p>Note: The coordinator disk does not store data, so configure the disk as the smallest possible LUN on a disk array to avoid wasting space. The minimum size required for a coordinator disk is 128 MB.</p> |
| Disk space | <p>You can evaluate your systems for available disk space by running the product installation program. Navigate to the product directory on the product disc and run the following command:</p> <pre data-bbox="559 621 982 647"># ./installmr -precheck node_name</pre> <p>For details on the additional space that is required for Sybase, see the Sybase documentation.</p> |
| RAM | <p>Each SF Sybase CE system requires at least 8 GB.</p> |
| Network | <p>Two or more private links and one public link.</p> <p>Links must be 100BaseT or gigabit Ethernet directly linking each node to the other node to form a private network that handles direct inter-system communication. These links must be of the same type; you cannot mix 100BaseT and gigabit.</p> <p>Symantec recommends gigabit Ethernet using enterprise-class switches for the private links.</p> |
| Fiber Channel or SCSI host bus adapters | <p>At least one additional SCSI or Fibre Channel Host Bus Adapter per system for shared data disks.</p> |

Supported operating systems

For information on supported operating systems for various components of SF Sybase CE, see the *Symantec Storage Foundation and High Availability Solutions Release Notes*.

Coordinator disk requirements for I/O fencing

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

- For disk-based I/O fencing, you must have at least three coordinator disks or there must be odd number of coordinator disks.
- The coordinator disks must be DMP 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.
- Coordinator devices can be attached over iSCSI protocol but they must be DMP devices and 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.
- The coordinator disk size must be at least 128 MB.

Supported Sybase ASE CE releases

SF Sybase CE supports Sybase ASE CE 15.7 only at the time of publication.

For the latest information on the supported Sybase ASE CE database versions, see the following Technical Support TechNote:

<http://www.symantec.com/docs/DOC4848>

See the Sybase ASE CE documentation for more information.

Supported SF Sybase CE configurations

The following Sybase configuration options are required in an SF Sybase CE environment:

- Set SF Sybase CE fencing to "sybase" mode.
- Configure Sybase private networks on LLT links
- Set Sybase cluster membership to "vcs" mode.
- Configure Sybase instances under VCS control.

Supported replication technologies for global clusters

SF Sybase CE supports the software replication technology Veritas Volume Replicator (VVR) for global cluster configurations.

Software-based replication ■ Volume Replicator

Checking installed product versions and downloading maintenance releases and patches

Symantec provides a means to check the Symantec RPMs you have installed, and download any needed maintenance releases and patches.

Use the `installmr` command with the `-version` option to determine what is installed on your system, and download any needed maintenance releases or patches. After you have installed the current version of the product, you can use the `showversion` script in the `/opt/VRTS/install` directory to find product information.

The `version` option or the `showversion` script checks the specified systems and discovers the following:

- SF Sybase CE product versions that are installed on the system
- All the required RPMs and the optional Symantec RPMs installed on the system
- Any required or optional RPMs (if applicable) that are not present
- Installed patches
- Available base releases (major or minor)
- Available maintenance releases
- Available patch releases

To check your systems and download maintenance releases and patches

- 1 Mount the media, or navigate to the installation directory.
- 2 Start the installer with the `-version` option.

```
# ./installmr -version sys1 sys2
```

For each system, the installer lists all of the installed base releases, maintenance releases, and patches, followed by the lists of available downloads.

- 3 If you have Internet access, follow the prompts to download the available maintenance releases and patches to the local system.
- 4 If you do not have Internet access, you can download any needed maintenance releases and patches from the Symantec Operations Readiness Tools (SORT) Patch Finder page at:

<https://sort.symantec.com/patch/finder>

You can obtain installer patches automatically or manually.

Downloading maintenance releases and patches requires the installer to make outbound networking calls. You can also disable external network connection attempts.

Obtaining installer patches

Symantec occasionally finds issues with the Symantec Storage Foundation and High Availability Solutions installer, and posts public installer patches on the Symantec Operations Readiness Tools (SORT) website's Patch Finder page at:

<https://sort.symantec.com/patch/finder>

You can access installer patches automatically or manually.

To download installer patches automatically

- ◆ Starting with Symantec Storage Foundation and High Availability Solutions version 6.1, installer patches are downloaded automatically. No action is needed on your part.

If you are running Symantec Storage Foundation and High Availability Solutions version 6.1 or later, and your system has Internet access, the installer automatically imports any needed installer patch, and begins using it.

Automatically downloading installer patches requires the installer to make outbound networking calls. You can also disable external network connection attempts.

If your system does not have Internet access, you can download installer patches manually.

To download installer patches manually

- 1 Go to the Symantec Operations Readiness Tools (SORT) website's Patch Finder page, and save the most current Symantec patch on your local system.
- 2 Navigate to the directory where you want to unzip the file you downloaded in step 1.
- 3 Unzip the patch tar file. For example, run the following command:

```
# gunzip cpi-6.2P2-patches.tar.gz
```

- 4 Untar the file. For example, enter the following:

```
# tar -xvf cpi-6.2P2-patches.tar
patches/
patches/CPI62P2.pl
README
```

- 5 Navigate to the installation media or to the installation directory.
- 6 To start using the patch, run the `installer` command with the `-require` option. For example, enter the following:

```
# ./installmr -require /target_directory/patches/CPI62P2.pl
```


Disabling external network connection attempts

When you execute the `installmr` command, the installer attempts to make an outbound networking call to get information about release updates and installer patches. If you know your systems are behind a firewall, or do not want the installer to make outbound networking calls, you can disable external network connection attempts by the installer.

To disable external network connection attempts

- ◆ Disable inter-process communication (IPC).

To disable IPC, run the installer with the `-noipc` option.

For example, to disable IPC for system1 (sys1) and system2 (sys2) enter the following:

```
# ./installmr -noipc sys1 sys2
```

Planning to install SF Sybase ASE CE

Planning your network configuration

The following practices are recommended for a resilient network setup:

- Configure the private cluster interconnect over multiple dedicated gigabit Ethernet links. All single point of failures such as network interface cards (NIC), switches, and interconnects should be eliminated.
- The NICs used for the private cluster interconnect should have the same characteristics regarding speed, MTU, and full duplex on all nodes. Do not allow the NICs and switch ports to auto-negotiate speed.
- Configure non-routable IP addresses for private cluster interconnects.
- The default value for LLT peer inactivity timeout is 16 seconds.

Planning the public network configuration for Sybase ASE CE

Public interconnects are used by the clients to connect to Sybase ASE CE database. The public networks must be physically separated from the private networks.

See Sybase ASE CE documentation for more information on recommendations for public network configurations.

Planning the private network configuration for Sybase ASE CE

Private interconnect is an essential component of a shared disk cluster installation. It is a physical connection that allows inter-node communication. Symantec recommends that these interconnects and LLT links must be the same. You must have the IP addresses configured on these interconnects, persistent after reboot. You must use solutions specific to the operating System.

See Sybase ASE CE documentation for more information on recommendations for private network configurations.

Planning the storage

SF Sybase CE provides the following options for shared storage:

- CVM
 CVM provides native naming (OSN) as well as enclosure-based naming (EBN). Use enclosure-based naming for easy administration of storage. Enclosure-based naming guarantees that the same name is given to a shared LUN on all the nodes, irrespective of the operating system name for the LUN.

- CFS

The following recommendations ensure better performance and availability of storage.

- Use multiple storage arrays, if possible, to ensure protection against array failures. The minimum recommended configuration is to have two HBAs for each host and two switches.
- Design the storage layout keeping in mind performance and high availability requirements. Use technologies such as striping and mirroring.
- Use appropriate stripe width and depth to optimize I/O performance.
- Use SCSI-3 persistent reservations (PR) compliant storage.
- Provide multiple access paths to disks with HBA/switch combinations to allow DMP to provide high availability against storage link failures and to provide load balancing.

Planning the storage for SF Sybase CE

[Table 6-4](#) lists the type of storage required for SF Sybase CE.

Table 6-4 Type of storage required for SF Sybase CE

| SF Sybase CE files | Type of storage |
|-----------------------|-----------------|
| SF Sybase CE binaries | Local |

Table 6-4 Type of storage required for SF Sybase CE (*continued*)

| SF Sybase CE files | Type of storage |
|---|-----------------|
| SF Sybase CE fencing coordinator disks | Shared |
| SF Sybase CE database storage management repository | Shared |

Planning the storage for Sybase ASE CE

Review the storage options and guidelines for Sybase ASE CE:

- Storage options for Sybase ASE CE binaries
 See [“Planning the storage for Sybase ASE CE binaries”](#) on page 187.
- Storage options for Sybase ASE CE datafiles and quorum device
 See [“Planning the storage for Sybase ASE CE data files and quorum device”](#) on page 188.

Note: Symantec strongly recommends retaining the default setting (global) for the CVM diskgroup disk detach policy, for Sybase ASE CE binaries, datafiles, and quorum device. For other disk detach policy options, see the Symantec Storage Foundation Administrator’s Guide.

Planning the storage for Sybase ASE CE binaries

The Sybase ASE CE binaries can be stored on a local or shared storage, depending on your high availability requirements.

Note: Symantec recommends that you install the Sybase ASE CE binaries on a shared storage on CFS.

Consider the following points while planning the installation:

- CFS installation provides a single Sybase ASE CE installation, regardless of the number of nodes. This scenario offers a reduction in the storage requirements and easy addition of nodes.
- Local installation provides improved protection against a single point of failure and also allows for applying the Sybase ASE CE patches in a rolling fashion.

Planning the storage for Sybase ASE CE data files and quorum device

Storage for Sybase ASE CE datafiles and quorum device has to be configured on shared storage on CFS.

Table 6-5 Type of storage required for Sybase ASE CE

| Sybase ASE CE files | Type of storage |
|-------------------------|-----------------|
| Sybase ASE CE binaries | Shared or local |
| Sybase ASE CE datafiles | Shared |
| Quorum device | Shared |

Note: Refer to the Sybase ASE CE documentation for Sybase's recommendation on the required disk space for Sybase ASE CE binaries, Sybase ASE CE datafiles and quorum device.

Planning volume layout

The following recommendations ensure optimal layout of VxVM/CVM volumes:

- Mirror the volumes across two or more storage arrays, if using VxVM mirrors. Keep the Fast Mirror Resync regionsize equal to the database block size to reduce the copy-on-write (COW) overhead. Reducing the regionsize increases the amount of Cache Object allocations leading to performance overheads.
- Distribute the I/O load uniformly on all Cache Objects when you create multiple Cache Objects.
- Implement zoning on SAN switch to control access to shared storage. Be aware that physical disks may be shared by multiple servers or applications and must therefore be protected from accidental access.
- Choose DMP I/O policy based on the storage network topology and the application I/O pattern.
- Exploit thin provisioning for better return on investment.

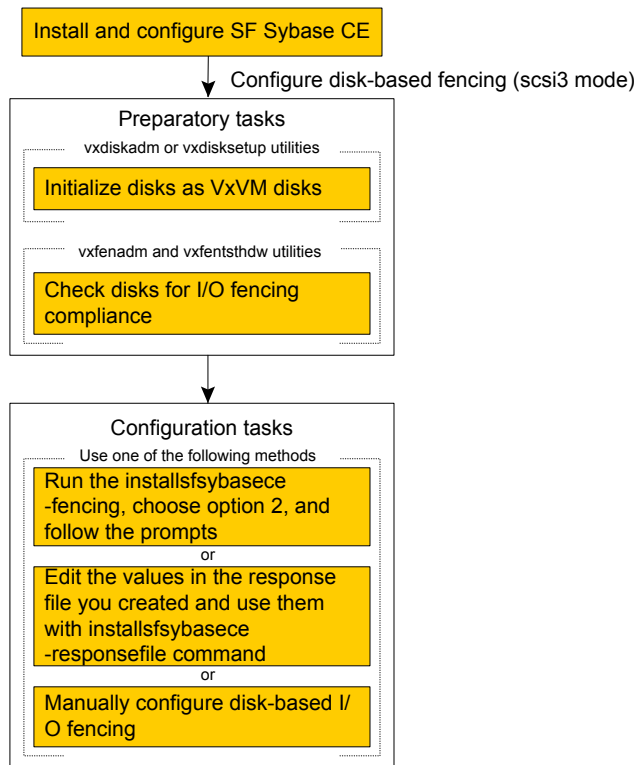
About planning to configure I/O fencing

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

You can configure disk-based I/O fencing.

[Figure 6-5](#) illustrates a high-level flowchart to configure I/O fencing for the SF Sybase CE cluster.

Figure 6-5 Workflow to configure I/O fencing



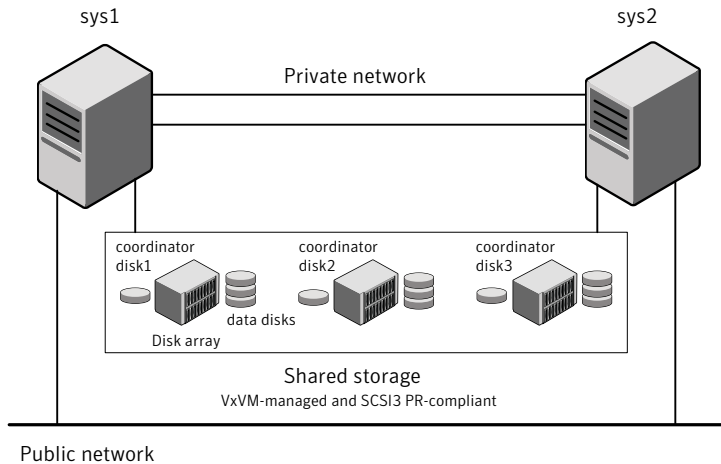
After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:

- Using the installmr See [“Setting up disk-based I/O fencing using installsybasece”](#) on page 229.
- Using response files
- Manually editing configuration files

Typical SF Sybase CE cluster configuration with disk-based I/O fencing

Figure 6-6 displays a typical VCS configuration with two nodes and shared storage. The configuration uses three coordinator disks for I/O fencing.

Figure 6-6 Typical SF Sybase CE cluster configuration with disk-based I/O fencing



Planning for cluster management

Table 6-6 lists the various agents supported in SF Sybase CE installations for effective cluster management.

Table 6-6 List of agents

| Agent | Description |
|-----------------------------|---|
| VCS agent for Sybase | Sybase database management The VCS Sybase agent is recommended for managing Sybase databases. VCS controls the Sybase database in this configuration. In the basic monitoring mode, the agent detects an application failure if a configured Sybase server process is not running. |
| VCS agents for CVM | Volume management An SF Sybase CE installation automatically configures the CVMCluster resource and the CVMVxconfigd resource. You must configure the CVMVolDg agent for each shared disk group. |
| VCS agents for CFS | File system management If the database uses cluster file systems, configure the CFSSMount agent for each volume in the disk group. |
| VCS process agent for vxfsd | vxfsd process/daemon management |

Licensing SF Sybase ASE CE

About Symantec product licensing

You have the option to install Symantec 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.

http://www.symantec.com/products-solutions/licensing/activating-software/detail.jsp?detail_id=licensing_portal

The 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 systems with a management server. If you do not comply with the above terms, continuing to use the Symantec product is a violation of your End User License Agreement, and results in warning messages
For more information about keyless licensing, see the following URL:
<http://go.symantec.com/sfhakeyless>

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

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.

See the `vxkeyless(1m)` manual page.

- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.

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

About SF Sybase CE licenses

[Table 6-7](#) lists the various SF Sybase CE license levels in keyless licensing and the corresponding features.

Table 6-7 SF Sybase CE license levels (keyless licensing)

| License | Description | Features enabled |
|----------------|--|--|
| SFSYBASECE | SF Sybase CE Enterprise Edition | The license enables the following features: <ul style="list-style-type: none"> ■ Veritas Volume Manager ■ Veritas File System ■ Symantec Cluster Server ■ Veritas Mapping Services |
| SFSYBASECE_VR | SF Sybase CE Enterprise Edition with VR (Symantec Replicator Option) | The license enables the following features: <ul style="list-style-type: none"> ■ Veritas Volume Manager Volume Replicator is enabled. ■ Veritas File System ■ Symantec Cluster Server ■ Veritas Mapping Services |
| SFSYBASECE_VFR | SF Sybase CE Enterprise Edition with VFR (Symantec File Replicator) | The license enables the following features: <ul style="list-style-type: none"> ■ Veritas Volume Manager Volume Replicator is enabled. ■ Veritas File System ■ Symantec Cluster Server ■ Veritas Mapping Services |

Table 6-7 SF Sybase CE license levels (keyless licensing) (continued)

| License | Description | Features enabled |
|--------------------|--|--|
| SFSYBASECE_GCO | SF Sybase CE Enterprise Edition with GCO (Global Cluster Option) | The license enables the following features: <ul style="list-style-type: none"> Veritas Volume Manager Veritas File System Symantec Cluster Server Global Cluster Option is enabled. Veritas Mapping Services |
| SFSYBASECE_VR_GCO | SF Sybase CE Enterprise Edition with VR and GCO | The license enables the following features: <ul style="list-style-type: none"> Veritas Volume Manager Volume Replicator is enabled. Veritas File System Symantec Cluster Server Global Cluster Option is enabled. Veritas Mapping Services |
| SFSYBASECE_VFR_GCO | SF Sybase CE Enterprise Edition with VFR and GCO | The license enables the following features: <ul style="list-style-type: none"> Veritas Volume Manager Volume Replicator is enabled. Veritas File System Symantec Cluster Server Global Cluster Option is enabled. Veritas Mapping Services |

Setting or changing the product level for keyless licensing

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

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

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

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

When you upgrade from a previous release, the product installer prompts you to update the `vxkeyless` license product level to the current release level. If you update the `vxkeyless` license product level during the upgrade process, no further action is required. If you do not update the `vxkeyless` license product level, the output

you see when you run the `vxkeyless display` command includes the previous release's `vxkeyless` license product level. Each `vxkeyless` license product level name includes the suffix `_previous_release_version`. For example, `DMP_6.0`, or `SFENT_VR_5.1SP1`, or `VCS_GCO_5.1`. If there is no suffix, it is the current release version.

You would see the suffix `_previous_release_version` if you did not update the `vxkeyless` product level when prompted by the product installer. Symantec highly recommends that you always use the current release version of the product levels. To do so, use the `vxkeyless set` command with the desired product levels. If you see `SFENT_60`, `VCS_60`, use the `vxkeyless set SFENT,VCS` command to update the product levels to the current release.

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

To set or change the product level

- 1 Change your current working directory:

```
# export PATH=$PATH:/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 Symantec products until you install a new key or set a new product level.

To clear the product license level

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

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

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

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

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

Installing Symantec product license keys

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

| | |
|------------------------|---|
| <code>vxlicinst</code> | Installs a license key for a Symantec product |
| <code>vxlicrep</code> | Displays the currently installed licenses |
| <code>vxlictest</code> | Retrieves the features and their descriptions that are 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 or change a license

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

```
# cd /opt/VRTS/bin  
  
# ./vxlicinst -k license key
```

- 2 Run the following Veritas Volume Manager (VxVM) command to recognize the new license:

```
# vxdctl license init
```

See the `vxdctl (1M)` manual page.

If you have `vxkeyless` licensing, you can view or update the keyless product licensing levels.

Preparing to install SF Sybase CE

This chapter includes the following topics:

- [About preparing to install and configure SF Sybase CE](#)
- [Synchronizing time settings on cluster nodes](#)
- [Setting up inter-system communication](#)
- [Setting up shared storage](#)
- [Setting the environment variables for Sybase ASE CE](#)
- [Setting the kernel.panic tunable](#)
- [Configuring the I/O scheduler](#)
- [Optimizing LLT media speed settings on private NICs](#)
- [Verifying the systems before installation](#)
- [About installation and configuration methods](#)

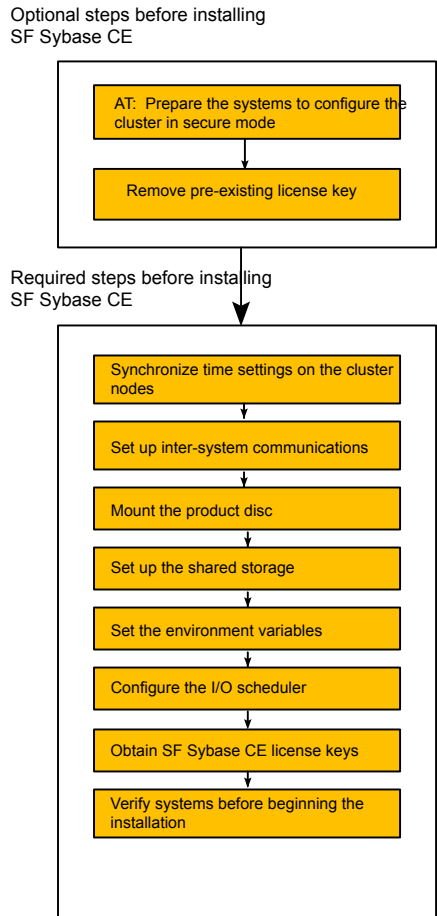
About preparing to install and configure SF Sybase CE

Before you install and configure SF Sybase CE, you need to perform some preinstallation tasks for the required and optional components of SF Sybase CE.

If you do not want to configure the optional components and features, proceed directly to the mandatory pre-installation tasks:

Figure 7-1 illustrates an overview of the mandatory and optional pre-installation steps for SF Sybase CE. The optional tasks are performed only for optional components or features that you plan to use.

Figure 7-1 SF Sybase CE pre-installation tasks



Synchronizing time settings on cluster nodes

Symantec recommends that the time settings on all cluster nodes be synchronized by running the Network Time Protocol (NTP) daemon.

The installer provides the option for automatic NTP synchronization.

Setting up inter-system communication

When you install Sybase ASE CE using the `installmr` script, make sure that communication between systems exists. By default the installer uses ssh. You must have root privileges for the system where you run the `installmr` script. This privilege facilitates 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, you have recourse.

Warning: The rsh and ssh commands to the remote systems, where Sybase ASE CE is to be installed, must not print any extraneous characters.

Setting up ssh on cluster systems

Use the Secure Shell (ssh) to install Sybase ASE CE on all systems in a cluster from a system outside of the cluster. Before you start the installation process, verify that ssh is configured correctly.

Use Secure Shell (ssh) to do the following:

- Log on to another system over a network
- Execute commands on a remote system
- Copy files from one system to another

The ssh shell provides strong authentication and secure communications over channels. It is intended to replace rlogin, rsh, and rcp.

The Remote Shell (rsh) is disabled by default to provide better security. Use ssh for remote command execution.

Configuring ssh

The procedure to configure ssh uses OpenSSH example file names and commands.

Note: You can configure ssh in other ways. Regardless of how ssh is configured, complete the last step in the example to verify the configuration.

To configure ssh

- 1 Log on to the system from which you want to install Sybase ASE CE.
- 2 Generate a DSA key pair on this system by running the following command:

```
# ssh-keygen -t dsa
```

- 3 Accept the default location of `~/.ssh/id_dsa`.
- 4 When the command prompts, enter a passphrase and confirm it.
- 5 Change the permissions of the `.ssh` directory by typing:

```
# chmod 755 ~/.ssh
```

- 6 The file `~/.ssh/id_dsa.pub` contains a line that begins with `ssh_dss` and ends with the name of the system on which it was created. Copy this line to the `/root/.ssh/authorized_keys2` file on all systems where you plan to install Sybase ASE CE.

If the local system is part of the cluster, make sure to edit the `authorized_keys2` file on that system.

- 7 Run the following commands on the system where you are installing:

```
# exec /usr/bin/ssh-agent $SHELL
# ssh-add
```

This step is shell-specific and is valid for the duration the shell is alive.

- 8 When the command prompts, enter your DSA passphrase.

To avoid running the `ssh-agent` on each shell, run the X-Window system and configure it so that you are not prompted for the passphrase. Refer to the documentation for your distribution for more information.

- 9 To verify that you can connect to the systems where you plan to install Sybase ASE CE, type:

```
# ssh -x -l root node01 ls
# ssh -x -l root node02 ifconfig
```

The commands should execute on the remote system without having to enter a passphrase or password.

Setting up shared storage

You need to set up shared storage to meet the following requirements:

- The LUNs from the shared storage must be visible to all the nodes in the cluster as seen by the following command:

```
# fdisk -l
```

For more information on setting up shared storage, see the *Symantec Cluster Server Installation Guide 6.2*.

Setting the environment variables for Sybase ASE CE

Set the MANPATH variable in the .profile file (or other appropriate shell setup file for your system) to enable viewing of manual pages.

Based on the shell you use, type one of the following:

```
For sh, ksh, or bash # export MANPATH=$MANPATH:\
/opt/VRTS/man
```

```
For csh # setenv MANPATH $MANPATH:/opt/VRTS/man
```

Some terminal programs may display garbage characters when you view the man pages. Set the environment variable LC_ALL=C to resolve this issue.

Set the PATH environment variable in the .profile file (or other appropriate shell setup file for your system) on each system to include installation and other commands.

Based on the shell you use, type one of the following:

```
For sh, ksh, or bash # PATH=/usr/sbin:/sbin:/usr/bin:\
/opt/VRTS/bin\
$PATH; export PATH
```

Setting the kernel.panic tunable

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

To set the kernel.panic tunable

- 1 Set the kernel.panic tunable to a desired value in the /etc/sysctl.conf file.

For example, kernel.panic = 10, will assign a value 10 seconds to the kernel.panic tunable. This step makes the change persistent across restarts.

- 2 Run the command:

```
sysctl -w kernel.panic=10
```

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

Configuring the I/O scheduler

Symantec recommends using the Linux 'deadline' I/O scheduler for database workloads. Configure your system to boot with the 'elevator=deadline' argument to select the 'deadline' scheduler.

To determine whether a system uses the deadline scheduler

- ◆ Look for "elevator=deadline" in /proc/cmdline.

See the operating system documentation for more information on I/O schedulers.

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 for LLT interconnects

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

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

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

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

Verifying the systems before installation

Use any of the following options to verify your systems before installation:

- Option 1: Run Symantec Operations Readiness Tools (SORT).
 For information on downloading and running SORT:
<https://sort.symantec.com>
- Option 2: Run the `installmr` script with the `"-precheck"` option as follows:
 Navigate to the directory that contains the `installmr` program.
 Start the preinstallation check:

```
# ./installmr -precheck sys1 sys2
```

where `sys1`, `sys2` are the names of the nodes in the cluster.

The program proceeds in a non-interactive mode, examining the systems for licenses, RPMs, disk space, and system-to-system communications. The program displays the results of the check and saves them in a log file. The location of the log file is displayed at the end of the precheck process.

About installation and configuration methods

You can install and configure Sybase ASE CE using Symantec installation programs or using native operating system methods.

[Table 7-1](#) shows the installation and configuration methods that Sybase ASE CE supports.

Table 7-1 Installation and configuration methods

| Method | Description |
|-------------------|--|
| Deployment Server | Using the Deployment Server, you can store multiple release images in one central location and deploy them to systems of any supported platform. |

Table 7-1 Installation and configuration methods (*continued*)

| Method | Description |
|---|---|
| <p>Silent installation using response files</p> | <p>Response files automate installation and configuration by using the information that is stored in a specified file instead of prompting you for information.</p> <p>You can use any of the above options to generate a response file. You can then customize the response file for another system. Run the product installation script with the response file option to install silently on one or more systems.</p> |
| <p>Install Bundles</p> | <p>Beginning with version 6.1, you can easily install or upgrade your systems directly to a base, maintenance, or patch level in one step using Install Bundles.</p> <p>The installer installs both releases as if they were combined in the same release image. The various scripts, RPMs, and patch components are merged, and multiple releases are installed together as if they are one combined release.</p> |

Installation of SF Sybase ASE CE using the script-based installer

This chapter includes the following topics:

- [Installing SF Sybase ASE CE](#)
- [Configuring SF Sybase ASE CE](#)
- [Setting up disk-based I/O fencing using installsfybasece](#)

Installing SF Sybase ASE CE

About the script-based installer

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

- The general product installer (`installmr`). The general product installer script provides a menu that simplifies the selection of installation and configuration options. Use the general product installer if you want to install multiple products from a disc.
See [“Installing SF Sybase CE using the Veritas script-based installation program”](#) on page 206.

[Table 8-1](#) lists all the SFHA Solutions product installation scripts. The list of product-specific installation scripts that you find on your system depends on the product that you install on your system.

Table 8-1 Product installation scripts

| Symantec product name | Script name in the media | Script name after an installation |
|---|--------------------------|-----------------------------------|
| For all SFHA Solutions products | installmr | N/A |
| Symantec ApplicationHA | N/A | installapplicationha<version> |
| Symantec Cluster Server (VCS) | N/A | installvcs<version> |
| Symantec Storage Foundation (SF) | N/A | installsf<version> |
| Symantec Storage Foundation and High Availability (SFHA) | N/A | installsfha<version> |
| Symantec Storage Foundation Cluster File System High Availability (SFCFSHA) | N/A | installsfcfsha<version> |
| Symantec Storage Foundation for Oracle RAC (SF Oracle RAC) | N/A | installsfrac<version> |
| Symantec Storage Foundation for Sybase ASE CE (SF Sybase CE) | N/A | installsfsybasece<version> |
| Symantec Dynamic Multi-pathing (DMP) | N/A | installdmp<version> |

When you configure the product after an installation, the installation scripts include the product version in the script name.

For example, for the 6.2.1 version:

```
# /opt/VRTS/install<productname>62 -configure
```

Note: The general product installer (`installmr`) script does not include the product version.

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

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

Installing SF Sybase CE using the Veritas script-based installation program

During the installation, the installer performs the following tasks:

- Verifies system readiness for installation by checking system communication, network speed, installed RPMs, operating system patches, swap space, and available volume space.

Note: If the installer reports that any of the patches are not available, install the patches on the system before proceeding with the Sybase ASE CE installation.

- Installs the SF Sybase CE 6.2.1 RPMs.

The following sample procedure installs SF Sybase CE on two systems—node01 and node02.

To install SF Sybase CE

- 1 Log in as the superuser on one of the systems.
- 2 Start the installation program:

```
Common      Navigate to the directory that contains the installation program.
product     Run the program:
installer   # ./installmr -base_path /tmp/sfha6.2/ node01 node02
```

Select SFSYBASECE from the Product selection Menu.

- 1) Symantec Dynamic Multi-Pathing (DMP)
- 2) Symantec Cluster Server (VCS)
- 3) Symantec Storage Foundation (SF)
- 4) Symantec Storage Foundation and High Availability (SFHA)
- 5) Symantec Storage Foundation Cluster File System HA (SFCFSHA)
- 6) Symantec Storage Foundation for Sybase ASE CE (SFSYBASECE)
- 7) Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)
- 8) Symantec ApplicationHA (ApplicationHA)
- b) Back to previous menu

Select a product to install: [1-8,b,q] 6

The installer displays the copyright message and specifies the directory where the running logs are created.

3 Set up the systems so that commands between systems execute without prompting for passwords or confirmations.

Would you like the installer to setup ssh or rsh communication automatically between the systems?

Superuser passwords for the systems will be asked. [y,n,q] (y)

Enter the superuser password for system node01:

- 1) Setup ssh between the systems
- 2) Setup rsh between the systems
- b) Back to previous menu

Select the communication method [1-2,b,q,?] (1)

See [“About configuring secure shell or remote shell communication modes before installing products”](#) on page 422.

4 If you had quit the installer in the process of an active installation, the installer discovers that installer process and provides the option of resuming the installation or starting a new installation. Provide a suitable response.

The installer has discovered an existing installer process.

The process exited while performing installation of SF Sybase CE on node01.

Do you want to resume this process? [y,n,q,?] (y) n

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

6 Select the type of installation—Minimal, Recommended, All. Each option displays the disk space that is required for installation.

Symantec recommends you to choose the option **Install all RPMs**.

```

1) Install minimal required RPMs
2) Install recommended RPMs
3) Install all RPMs
4) Display RPMs to be installed for each option
Select the RPMs to be installed on all systems?
[1-4,q,?] (2) 3

```

7 Enter the system names where you want to install the software.

```

Enter the system name or names and then press Enter.
Enter the system names separated by spaces:
[q,?] node01 node02

```

The installer verifies the systems for compatibility and displays the list of RPMs and patches that will be installed.

8 Select the appropriate license option.

```

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]

```

- Enter **1** if you have a valid license key. When prompted, enter the license key.

```

Enter a SF Sybase CE license key:
xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-x

```

If you plan to enable additional capabilities, enter the corresponding license keys when you are prompted for additional licenses.

```

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

```

- Enter **2** to enable keyless licensing.

Note: The keyless license option enables you to install SF Sybase CE without entering a key. However, you must still acquire a valid license to install and use SF Sybase CE. Keyless licensing requires that you manage the systems with a Management Server.

Enter **y** if you want to enable replication or configure Global Cluster Option (GCO) during the installation. Replication is configured with default values while GCO is configured with the settings you specify. You can reconfigure replication and GCO manually at any time.


```
Would you like to enable replication? [y,n,q] (y)
1) Symantec Volume Replicator
2) Symantec File Replicator Option
3) Both
Select the replication option you would like to enable [1-3,q,?] (1)
```

If you enable replication, the installer registers the corresponding license.

- 9 Verify that the installation process completed successfully. Review the output at the end of the installation and note the location of the summary and log files for future reference.
- 10 Enter **y** to configure SF Sybase CE:

```
Would you like to configure SF Sybase CE on
node01 node02 [y,n,q] (n) y
```

Note: If you had quit the installer before registering the sfsybasece license key, make sure the license key is registered on the system before starting the SF Sybase CE configuration. To register the license key, use the `installer -license` command.

- 11 Enter **y** if you want 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
```

- 12 Enter **y** if you want to view the summary file.

```
Would you like to view the summary file? [y,n,q] (n) y
```

Configuring SF Sybase ASE CE

About configuring SF Sybase CE

You need to configure SF Sybase CE when:

- You have completed installation of SF Sybase CE on your systems.
- You want to reconfigure an existing SF Sybase CE cluster.

Note: Before you reconfigure a cluster, make sure that you stop any running applications that use VxFS/CFS. Then, unmount the VxFS/CFS mounts.

SF Sybase CE configuration involves the following high-level tasks:

- Starting the product installer (if you quit the installer after installation or want to reconfigure the cluster)
- Configuring the SF Sybase CE components—VCS, CVM, and CFS
- Configuring the SF Sybase CE clusters for data integrity

During the configuration process, the installer performs the following tasks:

- Verifies the cluster information.
- Stops SF Sybase CE processes.
- Creates SF Sybase CE configuration files.
- Starts SF Sybase CE processes.
- Creates a new directory with a log file that contains any system commands executed, and their output, a response file that can be used with the `-responsefile` option of the installer, and a summary file that contains the output of the install scripts. The location of the files is indicated by the installer.

Configuring the SF Sybase CE components using the script-based installer

After installation, log in to the product installer to configure SF Sybase CE components. No configuration changes are made to the systems until all configuration questions are completed and confirmed.

Make sure that you have performed the necessary pre-configuration tasks if you want to configure the cluster in secure mode.

Start the `installsfsybasece<version>`.

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.

At the end of the configuration, the VCS, CVM, and CFS components are configured to provide a cluster-aware environment.

Note: If you want to reconfigure SF Sybase CE, 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. You must also unmount the all VxFS/CFS mounts that are not configured under VCS.

To configure the SF Sybase CE components

- 1 Log in as the superuser on any of the nodes in the cluster.
- 2 Start the configuration program.

```
SF Sybase CE installer      Run the program:

                             # cd /opt/VRTS/install

                             # ./installsybasece62 \
                             -configure sys1 sys2
```

See [“About the script-based installer”](#) on page 204.

The installer displays the copyright message and specifies the directory where the logs are created.

- 3 Enter **1** to select the option **Configure SF Sybase CE sub-components**.

```
1) Configure Cluster File System
2) Configure I/O Fencing in Sybase Mode
3) Configure Sybase ASE CE Instance in VCS
4) Exit SFSYBASECE Configuration
Choose option: [1-4,q] (1)
```

- 4 If you had quit the installer in the process of an active configuration, the installer discovers that installer process and provides the option of resuming the configuration or starting a new configuration. Provide a suitable response.

```
The installer has discovered an existing installer process.
The process exited while performing configure of
SF Sybase CE on sys1.
Do you want to resume this process? [y,n,q,?] (y) n
```

- 5 Configure the Symantec Cluster Server component to set up the SF Sybase CE cluster.

See [“Configuring the SF Sybase ASE CE cluster”](#) on page 212.

- 6 Add VCS users.

See [“Adding VCS users”](#) on page 224.

- 7 Configure SMTP email notification.
See [“Configuring SMTP email notification”](#) on page 225.
- 8 Configure SNMP trap notification.
See [“Configuring SNMP trap notification”](#) on page 227.

Configuring the SF Sybase ASE CE cluster

Configure the systems on which you installed SF Sybase ASE CE to be part of your cluster.

To configure a cluster for SF Sybase ASE CE

- 1 Log in to the installer.
See [“Configuring the SF Sybase CE components using the script-based installer”](#) on page 210.
 - 2 Select the **Configure Cluster File System** option from the main menu.
Press Return to continue.
If there are any SF Sybase ASE CE processes running, these processes are stopped. Press Return to continue.
 - 3 VCS configuration includes configuring the cluster, users, secure mode if required, and notification.
To configure a cluster:
 - Configure the cluster name.
See [“Configuring the cluster name”](#) on page 213.
 - Configure private heartbeat links.
See [“Configuring private heartbeat links”](#) on page 213.
- See [“Configuring the virtual IP of the cluster”](#) on page 218.
- See [“Configuring Symantec Storage Foundation for Sybase ASE CE in secure mode”](#) on page 219.
- See [“Configuring a secure cluster node by node”](#) on page 220.
- See [“Adding VCS users”](#) on page 224.
- See [“Configuring SMTP email notification”](#) on page 225.
- See [“Configuring SNMP trap notification”](#) on page 227.
- See [“Configuring global clusters”](#) on page 228.

Configuring the cluster name

Enter the cluster information when the installer prompts you.

To configure the cluster

- 1 Review the configuration instructions that the installer presents.
- 2 Enter a unique cluster name.

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

Configuring private heartbeat links

You now configure the private heartbeat links that LLT uses.

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

You must not configure LLT heartbeat using the links that are part of aggregated links. For example, link1, link2 can be aggregated to create an aggregated link, aggr1. You can use aggr1 as a heartbeat link, but you must not use either link1 or link2 as heartbeat links.

The following procedure helps you configure LLT heartbeat links.

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 LLT over UDP or LLT over RDMA.
 - Option 1: Configure the heartbeat links using 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: Configure the heartbeat links using 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: Configure the heartbeat links using LLT over RDMA (answer installer questions)
Make sure that each RDMA enabled NIC (RNIC) 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 RDMA. If you had not already configured IP addresses to the RNICs, the installer provides you an option to detect the IP address for a given RNIC.
Skip to step 4.
- Option 4: Automatically detect configuration for LLT over Ethernet
Allow the installer to automatically detect the heartbeat link details to configure LLT over Ethernet. The installer tries to detect all connected links between all systems.
Make sure that you activated the NICs for the installer to be able to detect and automatically configure the heartbeat links.
Skip to step 7.

Note: Option 4 is not available when the configuration is a single node configuration.

- 2 If you chose option 1, enter the network interface card details for the private heartbeat links.
The installer discovers and lists the network interface cards.
You must not enter the network interface card that is used for the public network (typically eth0.)

- 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 node01: [b,q,?] private_NIC1
Do you want to use address 192.168.0.1 for the
first private heartbeat link on node01: [y,n,q,b,?] (y)
Enter the UDP port for the first private heartbeat
link on node01: [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 node01: [b,q,?] private_NIC2
Do you want to use address 192.168.1.1 for the
second private heartbeat link on node01: [y,n,q,b,?] (y)
Enter the UDP port for the second private heartbeat
link on node01: [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 node01: [b,q,?] (private_NIC0)
Do you want to use address 192.168.3.1 for
the low priority heartbeat link on node01: [y,n,q,b,?] (y)
Enter the UDP port for the low priority heartbeat
link on node01: [b,q,?] (50004)
```

4 If you chose option 3, choose the interconnect type to configure RDMA.

- 1) Converged Ethernet (RoCE)
- 2) InfiniBand
- b) Back to previous menu

Choose the RDMA interconnect type [1-2,b,q,?] (1) 2

The system displays the details such as the required OS files, drivers required for RDMA , and the IP addresses for the NICs.

A sample output of the IP addresses assigned to the RDMA enabled NICs using InfiniBand network. Note that with RoCE, the RDMA NIC values are represented as eth0, eth1, and so on.

| System | RDMA NIC | IP Address |
|--------|----------|-------------|
| sys1 | ib0 | 192.168.0.1 |
| sys1 | ib1 | 192.168.3.1 |
| sys2 | ib0 | 192.168.0.2 |
| sys2 | ib1 | 192.168.3.2 |

- 5 If you chose option 3, enter the NIC details for the private heartbeat links. This step uses RDMA over an InfiniBand network. With RoCE as the interconnect type, RDMA NIC is represented as Ethernet (eth).

```
Enter the NIC for the first private heartbeat  
link (RDMA) on node01: [b,q,?] <ib0>
```

```
Do you want to use address 192.168.0.1 for the  
first private heartbeat link on node01: [y,n,q,b,?] (y)
```

```
Enter the port for the first private heartbeat  
link (RDMA) on node01: [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 (RDMA) on node01:  
[b,q,?] (ib1)
```

```
Do you want to use the address 192.168.3.1 for the second  
private heartbeat link on node01: [y,n,q,b,?] (y)
```

```
Enter the port for the second private heartbeat link (RDMA) on node01:  
[b,q,?] (50001)
```

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

- 6 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 node01, make sure the same NICs are available on each system. Then, enter **y** at the prompt.

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.

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

- 7 If you chose option 4, 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 or step 4 for option 3.

- 8 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)
```

- 9 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 *Symantec Cluster Server Administrator's Guide* for information on the Cluster Manager.

See the *Symantec 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 node01: eth0
Enter the NIC for Virtual IP of the Cluster to use on node01:
[b,q,?] (eth0)
```

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

Do one of the following:

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

```
Is eth0 to be the public NIC used by all systems
[y,n,q,b,?] (y)
```

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

Configuring Symantec Storage Foundation for Sybase ASE CE in secure mode

Configuring SF Sybase CE in secure mode ensures that all the communication between the systems is encrypted and users are verified against security credentials. Sybase ASE CE user names and passwords are not used when a cluster is running in secure mode.

To configure SF Sybase CE in secure mode

1 To install SF Sybase CE in secure mode, run the command:

```
# installsfybasece<version> -security
```

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

2 The installer displays the following question before the install stops the product processes:

- Do you want to grant read access to everyone? [y,n,q,?]
 - To grant read access to all authenticated users, type **y**.
 - To grant usergroup specific permissions, type **n**.
- Do you want to provide any usergroups that you would like to grant read access?[y,n,q,?]
 - To specify usergroups and grant them read access, type **y**
 - To grant read access only to root users, type **n**. The installer grants read access to the root users.

- Enter the usergroup names separated by spaces that you would like to grant read access. If you would like to grant read access to a usergroup on a specific node, enter like 'usrgrp1@node1', and if you would like to grant read access to usergroup on any cluster node, enter like 'usrgrp1'. If some usergroups are not created yet, create the usergroups after configuration if needed. [b]
- 3 To verify the cluster is in secure mode after configuration, run the command:

```
# haclus -value SecureClus
```

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

Configuring a secure cluster node by node

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

[Table 8-2](#) lists the tasks that you must perform to configure a secure cluster.

Table 8-2 Configuring a secure cluster node by node

| Task | Reference |
|---|--|
| Configure security on one node | See “Configuring the first node” on page 220. |
| Configure security on the remaining nodes | See “Configuring the remaining nodes” on page 221. |
| Complete the manual configuration steps | See “Completing the secure cluster configuration” on page 222. |

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/installsfbasece<version> -securityonnode
```

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

See [“About the script-based installer”](#) on page 204.

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

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

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

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

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

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

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

Configuring the remaining nodes

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

To configure security on each remaining node

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

```
# /opt/VRTS/install/installsfbasece<version> -securityonnode
```

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

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

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

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

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

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

```
Enter the security conf file directory: [b]
```

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

Completing the secure cluster configuration

Perform the following manual steps to complete the configuration.

To complete the secure cluster configuration

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

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

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

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

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

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

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

- 3 On all nodes, stop the CmdServer.

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

- 4 To grant access to all users, add or modify `SecureClus=1` and `DefaultGuestAccess=1` in the cluster definition.

For example:

To grant read access to everyone:

```
Cluster clus1 (  
  SecureClus=1  
  DefaultGuestAccess=1  
)
```

Or

To grant access to only root:

```
Cluster clus1 (  
  SecureClus=1  
)
```

Or

To grant read access to specific user groups, add or modify `SecureClus=1` and `GuestGroups={}` to the cluster definition.

For example:

```
cluster clus1 (  
  SecureClus=1  
  GuestGroups={staff, guest}
```

- 5 Modify `/etc/VRTSvcs/conf/config/main.cf` file on the first node, and add `-secure` to the WAC application definition if GCO is configured.

For example:

```
Application wac (  
    StartProgram = "/opt/VRTSvcs/bin/wacstart -secure"  
    StopProgram = "/opt/VRTSvcs/bin/wacstop"  
    MonitorProcesses = {" /opt/VRTSvcs/bin/wac -secure"  
    RestartLimit = 3  
)
```

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

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

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

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

- 8 On all nodes, start CmdServer.

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

- 9 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 *Symantec 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.

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

3 Provide information to configure SMTP notification.

Provide the following information:

- Enter the SMTP server's host name.

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

- Enter the email address of each recipient.

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

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

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

4 Add more SMTP recipients, if necessary.

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

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

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

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

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

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

5 Verify and confirm the SMTP notification information.

```
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 *Symantec 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.
See [“Configuring global clusters”](#) on page 228.
- 3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the SNMP trap daemon port.

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

- Enter the SNMP console system name.

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

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

```
Enter the minimum severity of events for which SNMP traps
should be sent to sys5 [I=Information, W=Warning, E=Error,
S=SevereError]: [b,q,?] E
```

4 Add more SNMP consoles, if necessary.

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

```
Would you like to add another SNMP console? [y,n,q,b] (n) y  
Enter the SNMP console system name: [b,q,?] node04  
Enter the minimum severity of events for which SNMP traps  
should be sent to node04 [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.

```
SNMP Port: 162  
Console: sys5 receives SNMP traps for Error or  
higher events  
Console: node04 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 SF Sybase CE 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 *Symantec Cluster Server Administrator's Guide* for instructions to set up SF Sybase CE global clusters.

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.

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.

- 4 Verify and confirm the configuration of the global cluster.

```
Global Cluster Option configuration verification:
```

```
NIC: eth0  
IP: 192.168.1.16  
Netmask: 255.255.240.0
```

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

For complete details for configuring your disaster recovery environment once clusters are installed and configured:

See the *Symantec Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide*.

Setting up disk-based I/O fencing using `installsfsybasece`

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

See [“Configuring disk-based I/O fencing using `installsfsybasece`”](#) on page 230.

See [“Initializing disks as VxVM disks”](#) on page 232.

See [“Identifying disks to use as coordinator disks”](#) on page 233.

See [“Checking shared disks for I/O fencing”](#) on page 233.

Configuring disk-based I/O fencing using installsfsybasece

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

To set up disk-based I/O fencing using the installsfsybasece62

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

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

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

See [“About the script-based installer”](#) on page 204.

The installsfsybasece 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 SF Sybase CE 6.2.1 is configured properly.

- 3 Review the I/O fencing configuration options that the program presents. Type **1** to configure fencing in Sybase mode.

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

- 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 `vxfcntlshdw` utility and then return to this configuration program.
See [“Checking shared disks for I/O fencing”](#) on page 233.
- 7 After you confirm the requirements, the program creates the coordinator disk group with the information you provided.
- 8 Verify and confirm the I/O fencing configuration information that the installer summarizes.
- 9 Review the output as the configuration program does the following:
- Stops VCS and I/O fencing on each node.
 - Configures disk-based I/O fencing and starts the I/O fencing process.
 - Updates the VCS configuration file `main.cf` if necessary.
 - Copies the `/etc/vxfenmode` file to a date and time suffixed file `/etc/vxfenmode-date-time`. This backup file is useful if any future fencing configuration fails.
 - Updates the I/O fencing configuration file `/etc/vxfenmode`.

- Starts VCS on each node to make sure that the SF Sybase CE is cleanly configured to use the I/O fencing feature.
- 10 Review the output as the configuration program displays the location of the log files, the summary files, and the response files.
 - 11 Configure the Coordination Point Agent.

```
Do you want to configure Coordination Point Agent on
the client cluster? [y,n,q] (y)
```

- 12 Enter a name for the service group for the Coordination Point Agent.

```
Enter a non-existing name for the service group for
Coordination Point Agent: [b] (vxfen) vxfen
```

- 13 Set the level two monitor frequency.

```
Do you want to set LevelTwoMonitorFreq? [y,n,q] (y)
```

- 14 Decide the value of the level two monitor frequency.

```
Enter the value of the LevelTwoMonitorFreq attribute: [b,q,?] (5)
```

Installer adds Coordination Point Agent and updates the main configuration file.

Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

To initialize disks as VxVM disks

- 1 # **fdisk -l**
- 2 To initialize the disks as VxVM disks, use one of the following methods:
 - Use the interactive `vxdiskadm` utility to initialize the disks as VxVM disks. For more information, see the *Symantec Storage Foundation Administrator's Guide*.
 - Use the `vxdisksetup` command to initialize a disk as a VxVM disk.

```
# vxdisksetup -i device_name
```

The example specifies the CDS format:

```
# vxdisksetup -i sdr format=cdsdisk
```


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

Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See [“Initializing disks as VxVM disks”](#) on page 232.

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 233.

Checking shared disks for I/O fencing

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

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

The `vxfststhdw` 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 *Symantec Storage Foundation and High Availability Administrator's Guide 6.2.*

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

- Verifying the Array Support Library (ASL)
See [“Verifying Array Support Library \(ASL\)”](#) on page 234.
- Verifying that nodes have access to the same disk
See [“Verifying that the nodes have access to the same disk”](#) on page 235.

- Testing the shared disks for SCSI-3
 See [“Testing the disks using vxfcntl utility”](#) on page 235.

Verifying Array Support Library (ASL)

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

To verify Array Support Library (ASL)

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

 The ASL for the supported storage device that you add is available from the disk array vendor or Symantec technical support.
- 2 Verify that the ASL for the disk array is installed on each of the nodes. Run the following command on each node and examine the output to verify the installation of ASL.

The following output is a sample:

```
# vxddladm listsupport all
```

```
LIBNAME                VID                PID
=====
libvxhitachi.so        HITACHI            DF350, DF400, DF400F,
                        DF500, DF500F
libvxxp1281024.so      HP                 All
libvxxp12k.so          HP                 All
libvxdds2a.so          DDN                S2A 9550, S2A 9900,
                        S2A 9700
libvxpurple.so         SUN                T300
libvxxiotechE5k.so    XIOTECH            ISE1400
libvxcopan.so         COPANSYS           8814, 8818
libvxibm8k.so          IBM                2107
```

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

```
# vxdisk scandisks
```

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

Verifying that the nodes have access to the same disk

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

To verify that the nodes have access to the same disk

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

```
# vxfenadm -i diskpath
```

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

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

From node A, enter:

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

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

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

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

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

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

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

Testing the disks using vxfcntlsthdw utility

This procedure uses the `/dev/sdx` disk in the steps.

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

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

```
The disk /dev/sdx is ready to be configured for I/O Fencing on
node node01
```

For more information on how to replace coordinator disks, refer to the *Symantec Storage Foundation and High Availability Administrator's Guide*.

To test the disks using vxfcntlshdw utility

- 1 Make sure system-to-system communication functions properly.
 See [“About configuring secure shell or remote shell communication modes before installing products”](#) on page 422.
- 2 From one node, start the utility.
- 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: node01
Enter the second node of the cluster: node02
```

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

- 5 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 node01.

```
The disk is now ready to be configured for I/O Fencing on node  
node01
```

```
ALL tests on the disk /dev/sdx have PASSED
```

```
The disk is now ready to be configured for I/O fencing on node  
node01
```

- 6 Run the vxfststhdw utility for each disk you intend to verify.

Note: Only dmp disk devices can be used as coordinator disks.

Managing your Symantec deployments

This chapter includes the following topics:

- [About the Deployment Server](#)
- [Deployment Server overview](#)
- [Installing the Deployment Server](#)
- [Setting up a Deployment Server](#)
- [Setting deployment preferences](#)
- [Specifying a non-default repository location](#)
- [Downloading the most recent release information](#)
- [Loading release information and patches on to your Deployment Server](#)
- [Viewing or downloading available release images](#)
- [Viewing or removing repository images stored in your repository](#)
- [Deploying Symantec product updates to your environment](#)
- [Finding out which releases you have installed, and which upgrades or updates you may need](#)
- [Defining Install Bundles](#)
- [Creating Install Templates](#)
- [Deploying Symantec releases](#)
- [Connecting the Deployment Server to SORT using a proxy server](#)

About the Deployment Server

The Deployment Server makes it easier to install or upgrade SFHA releases from a central location. The Deployment Server lets you store multiple release images and patches in one central location and deploy them to systems of any supported UNIX or Linux operating system (6.1 or later).

Note: The script-based installer for version 6.1 and higher supports installations from one operating system node onto a different operating system. Therefore, heterogeneous push installations are supported for 6.1 and higher releases only.

Push installations for product versions 5.1, 6.0, or 6.0.1 releases must be executed from a system that is running the same operating system as the target systems. In order to perform push installations for product versions 5.1, 6.0, or 6.0.1 releases on multiple platforms, you must have a separate Deployment Server for each operating system.

The Deployment Server lets you do the following as described in [Table 9-1](#).

Table 9-1 Deployment Server functionality

| Feature | Description |
|--------------------------|---|
| Manage repository images | <ul style="list-style-type: none"> ■ View available SFHA releases. ■ Download maintenance and patch release images from the Symantec Operations Readiness Tools (SORT) website into a repository. ■ Load the downloaded release image files from FileConnect and SORT into the repository. ■ View and remove the release image files that are stored in the repository. |
| Version check systems | <ul style="list-style-type: none"> ■ Discover RPMs and patches installed on your systems and informs you of the product and version installed ■ Identify base, maintenance, and patch level upgrades to your system and to download maintenance and patch releases. ■ Query SORT for the most recent updates. |

Table 9-1 Deployment Server functionality (*continued*)

| Feature | Description |
|---|---|
| Install or upgrade systems | <ul style="list-style-type: none"> ■ Install base, maintenance, or patch level releases. ■ Install SFHA from any supported UNIX or Linux operating system to any other supported UNIX or Linux operating system. ■ Automatically load the script-based installer patches that apply to that release. ■ Install or upgrade an Install Bundle that is created from the Define/Modify Install Bundles menu. ■ Install an Install Template that is created from the Create Install Templates menu. |
| Define or modify Install Bundles | Define or modify Install Bundles and save them using the Deployment Server. |
| Create Install Templates | Discover installed components on a running system that you want to replicate on to new systems. |
| Update metadata | <p>Download, load the release matrix updates, and product installer updates for systems behind a firewall.</p> <p>This process happens automatically when you connect the Deployment Server to the Internet, or it can be initiated manually. If the Deployment Server is not connected to the Internet, then the Update Metadata option is used to upload current metadata.</p> |
| Set preferences | Define or reset program settings. |
| Connecting the Deployment Server to SORT using a proxy server | Use a proxy server, a server that acts as an intermediary for requests from clients, for connecting the Deployment Server to the Symantec Operations Readiness Tools (SORT) website. |

Note: The Deployment Server is available only from the command line. The Deployment Server is not available for the web-based installer.

Note: Many of the example outputs used in this chapter are based on Red Hat Enterprise Linux.

Deployment Server overview

After obtaining and installing the Deployment Server and defining a central repository, you can begin managing your deployments from that repository. You

can load and store product images for Symantec products back to version 5.1 in your Deployment Server. The Deployment Server is a central installation server for storing and managing your product updates.

Setting up and managing your repository involves the following tasks:

- Installing the Deployment Server.
See [“Installing the Deployment Server”](#) on page 241.
- Setting up a Deployment Server.
See [“Setting up a Deployment Server”](#) on page 242.
- Finding out which products you have installed, and which upgrades or updates you may need.
See [“Viewing or downloading available release images”](#) on page 249.
- Adding release images to your Deployment Server.
See [“Viewing or removing repository images stored in your repository”](#) on page 254.
- Removing release images from your Deployment Server.
See [“Viewing or removing repository images stored in your repository”](#) on page 254.
- Defining or modifying Install Bundles to manually install or upgrade a bundle of two or more releases.
See [“Defining Install Bundles”](#) on page 259.
- Creating Install Templates to discover installed components on a system that you want to replicate to another system.
See [“Creating Install Templates”](#) on page 264.

Later, when your repository is set up, you can use it to deploy Symantec products to other systems in your environment.

See [“Deploying Symantec product updates to your environment”](#) on page 256.

See [“Deploying Symantec releases”](#) on page 266.

Installing the Deployment Server

You can obtain the Deployment Server by either:

- Installing the Deployment Server manually.
- Running the Deployment Server after installing at least one Symantec 6.2.1 product.

Note: The `VRTSper1` and the `VRTSsfcp1<version>` RPMs are included in all Storage Foundation (SF) products, so installing any Symantec 6.2.1 product lets you access the Deployment Server.

To install the Deployment Server manually without installing a Symantec 6.2.1 product

- 1 Log in as superuser.
- 2 Mount the installation media.
- 3 Move to the top-level directory on the disc.

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

where *dist* is `rhel6` and *arch* is `x86_64` for RHEL and SLES.
- 4 Navigate to the following directory:

```
# cd rpms
```
- 5 Run the following command to install the `VRTSper1` and the `VRTSsfcp1<version>` RPMs:

```
# rpm -ivh VRTSper1*.rpm VRTSsfcp1<version>*.rpm
```

To run the Deployment Server

- 1 Log in as superuser.
- 2 Navigate to the following directory:

```
# cd /opt/VRTS/install
```
- 3 Run the Deployment Server.

```
# ./deploy_sfha
```

Setting up a Deployment Server

Symantec recommends that you create a dedicated Deployment Server to manage your product updates.

A Deployment Server is useful for doing the following tasks:

- Storing release images for the latest upgrades and updates from Symantec in a central repository directory.

- Installing and updating systems directly by accessing the release images that are stored within a central repository.
- Defining or modifying Install Bundles for deploying a bundle of two or more releases.
- Discovering installed components on a system that you want to replicate to another system.
- Installing Symantec products from the Deployment Server to systems running any supported platform.
- Creating a file share on the repository directory provides a convenient, central location from which systems running any supported platform can install the latest Symantec products and updates.

Create a central repository on the Deployment Server to store and manage the following types of Symantec releases:

- Base releases. These major releases and minor releases are available for all Symantec products. They contain new features, and you can download them from FileConnect.
- Maintenance releases. These releases are available for all Symantec products. They contain bug fixes and a limited number of new features, and you can download them from the Symantec Operations Readiness Tools (SORT) website.
- Patches. These releases contain fixes for specific products, and you can download them from the SORT website.

Note: All base releases and maintenance releases can be deployed using the install scripts that are included in the release. Before version 6.0.1, patches were installed manually. From the 6.0.1 release and onwards, install scripts are included with patch releases.

You can set up a Deployment Server with or without Internet access.

- If you set up a Deployment Server that has Internet access, you can download maintenance releases and patches from Symantec directly. Then, you can deploy them to your systems.

[Setting up a Deployment Server that has Internet access](#)

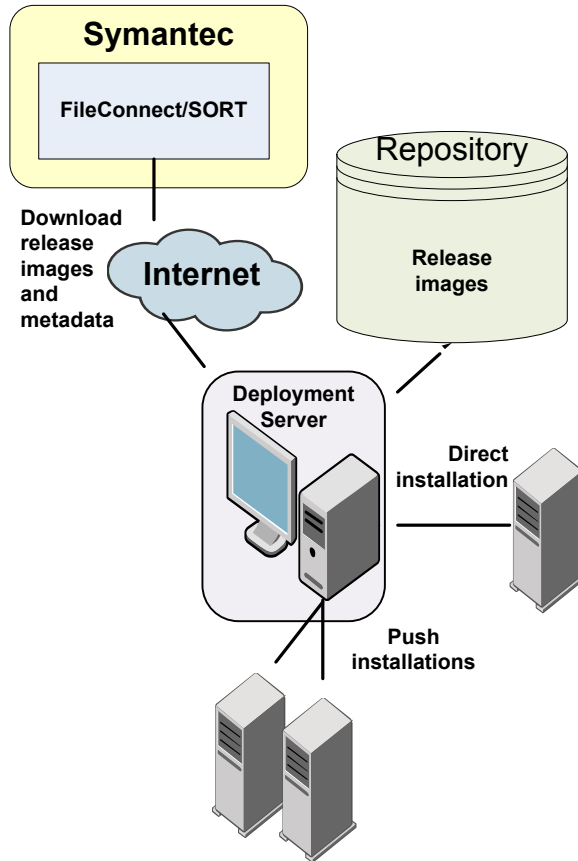
- If you set up a Deployment Server that does not have Internet access, you can download maintenance releases and patches from Symantec on another system that has Internet access. Then, you can load the images onto the Deployment Server separately.

[Setting up a Deployment Server that does not have Internet access](#)

Setting up a Deployment Server that has Internet access

Figure 9-1 shows a Deployment Server that can download product images directly from Symantec using the Deployment Server.

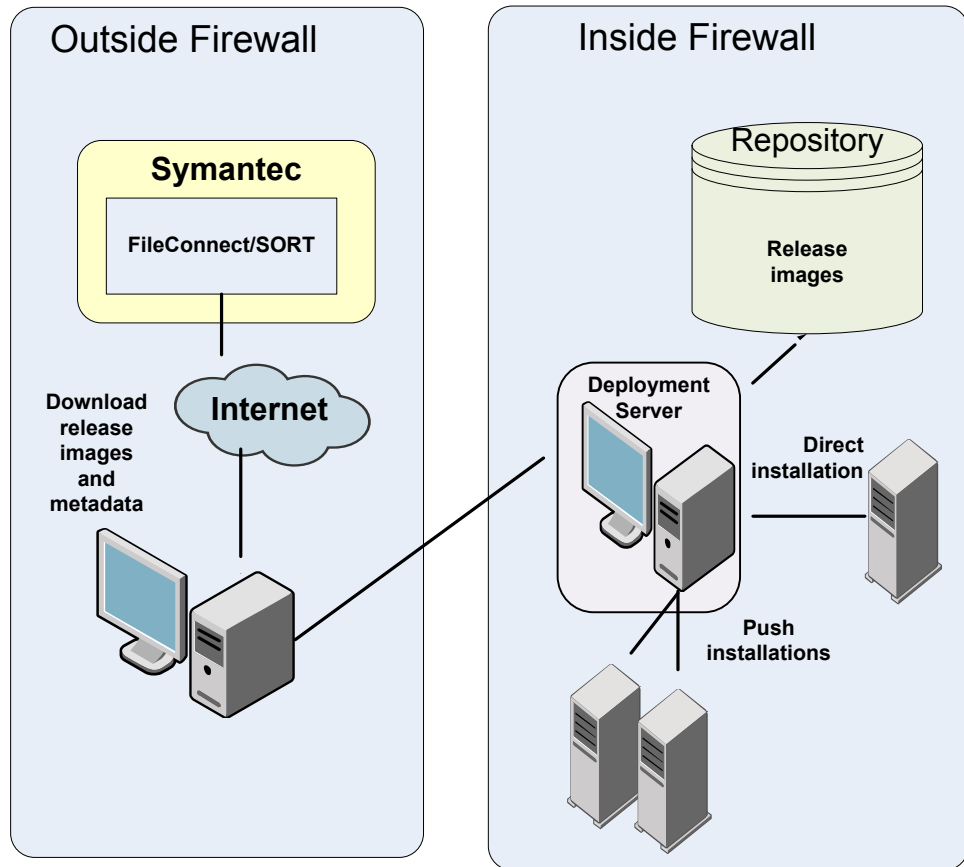
Figure 9-1 Example Deployment Server that has Internet access



Setting up a Deployment Server that does not have Internet access

Figure 9-2 shows a Deployment Server that does not have Internet access. In this scenario, release images and metadata updates are downloaded from another system. Then, they are copied to a file location available to the Deployment Server, and loaded.

Figure 9-2 Example Deployment Server that does not have Internet access



Release image files for base releases must be manually downloaded from FileConnect and loaded in a similar manner.

Setting deployment preferences

You can set preferences for managing the deployment of products dating back to version 5.1.

Note: You can select option **U (Terminology and Usage)** to obtain more information about Deployment Server terminology and usage.

To set deployment preferences

1 Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

Task Menu:

| | |
|----------------------------------|--------------------------|
| R) Manage Repository Images | M) Update Metadata |
| V) Version Check Systems | S) Set Preferences |
| I) Install/Upgrade Systems | U) Terminology and Usage |
| B) Define/Modify Install Bundles | ?) Help |
| T) Create Install Templates | Q) Quit |

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]

2 Select option **S, Set Preferences**.

You see the following output:

Current Preferences:

| | |
|--------------------|----------------------|
| Repository | /opt/VRTS/repository |
| Selected Platforms | N/A |
| Save Tar Files | N/A |

Preference List:

- 1) Repository
- 2) Selected Platforms
- 3) Save Tar Files
- b) Back to previous menu

Select a preference to set: [1-3,b,q,?]

3 Do one of the following:

- To set the default repository, enter **1**. Then enter the name of the repository in which you want to store your downloads. For example, enter the following:

```
/opt/VRTS/install/ProductDownloads
```

If the specified repository replaces a previous repository, the installer asks if you want to move all your files into the new repository. To move your files to the new repository, enter **y**.

- To add or remove a platform, enter **2**. You are provided selections for adding or deleting a platform. When a single platform is removed, it becomes **N/A**, which means that it is not defined. By default, all platforms are chosen. Once you select to add or remove a platform, the platform is added or removed in the preferences file and the preference platforms are updated. If only one platform is defined, no platform, architecture, distribution, and version selection menu is displayed.
- To set the option for saving or removing tar files, enter **3**. At the prompt, if you want to save the tar files after untarring them, enter **y**. Or, if you want to remove tar files after untarring them, enter **n**.
By default, the installer does not remove tar files after the releases have been untarred.

Specifying a non-default repository location

You can specify a repository location other than the default that has been set within the system preferences by using the command line option. The command line option is mainly used to install a release image from a different repository location. When you use the command line option, the designated repository folder is used instead of the default for the execution time of the script. Using the command line option does not override the repository preference set by the **Set Preference** menu item.

Note: When you specify a non-default repository, you are allowed only to view the repository (**View/Remove Repository**), and use the repository to install or upgrade (**Install/Upgrade Systems**) on other systems.

To use the command line option to specify a non-default repository location

- ◆ At the command line, to specify a non-default repository location, enter the following:

```
# ./deploy_sfha -repository repository_path
```

where *repository_path* is the location of the repository.

Downloading the most recent release information

Use one of the following methods to obtain a `.tar` file with the most recent release information:

- Download a copy from the SORT website.
- Run the Deployment Server from a system that has Internet access.

To obtain a data file by downloading a copy from the SORT website

- 1 Download the `.tar` file from the SORT site at:
https://sort.symantec.com/support/related_links/offline-release-updates
- 2 Click on **deploy_sfha.tar [Download]**, and save the file to your desktop.

To obtain a data file by running the Deployment Server from a system with Internet access

- 1 Run the Deployment Server. Enter the following:

```
# /opt/VRTS/install/deploy_sfha
```

- 2 Select option **M, Update Metadata**.

You see the following output:

```
The Update Metadata option is used to load release matrix updates on to systems that do not have an Internet connection with SORT (https://sort.symantec.com). Your system has a connection with SORT and is able to receive updates. No action is necessary unless you would like to create a file to update another Deployment Server system.
```

- ```
1) Download release matrix updates and installer patches
2) Load an update tar file
b) Back to previous menu
```

```
Select the option: [1-2,b,q,?]
```

- 3 Select option **1, Download release matrix updates and installer patches**.

## Loading release information and patches on to your Deployment Server

In this procedure, the Internet-enabled system is the system to which you downloaded the `deploy_sfha.tar` file.

See “[Downloading the most recent release information](#)” on page 247.



**To load release information and patches on to your Deployment Server**

- 1 On the Internet-enabled system, copy the `deploy_sfha.tar` file you downloaded to a location accessible by the Deployment Server.
- 2 On the Deployment Server, change to the installation directory. For example, enter the following:

```
cd /opt/VRTS/install/
```

- 3 Run the Deployment Server. Enter the following:

```
./deploy_sfha
```

- 4 Select option **M, Update Metadata**, and select option **2, Load an update tar file**. Enter the location of the `deploy_sfha.tar` file (the installer calls it a "meta-data tar file").

```
Enter the location of the meta-data tar file: [b]
(/opt/VRTS/install/deploy_sfha.tar)
```

For example, enter the location of the meta-data tar file:

```
/tmp/deploy_sfha.tar
```

## Viewing or downloading available release images

You can use the Deployment Server to conveniently view or download available release images to be deployed on other systems in your environment.

---

**Note:** If you have Internet access, communication with the Symantec Operations Readiness Tools (SORT) provides the latest release information. If you do not have Internet access, static release matrix files are referenced, and the most recent updates may not be included.

---

See [“Loading release information and patches on to your Deployment Server”](#) on page 248.

## To view or download available release images

### 1 Launch the Deployment Server.

```
/opt/VRTS/install/deploy_sfha
```

You see the following output:

Task Menu:

|                                  |                          |
|----------------------------------|--------------------------|
| R) Manage Repository Images      | M) Update Metadata       |
| V) Version Check Systems         | S) Set Preferences       |
| I) Install/Upgrade Systems       | U) Terminology and Usage |
| B) Define/Modify Install Bundles | ? ) Help                 |
| T) Create Install Templates      | Q) Quit                  |

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]

### 2 Select option **R**, **Manage Repository Images**.

You see the following output:

- 1) View/Download Available Releases
- 2) View/Remove Repository Images
- 3) Load a Release Image
- b) Back to previous menu

Select the option you would like to perform [1-3,b,q,?]

**3 Select option 1, View/Download Available Releases, to view or download what is currently installed on your system.**

You see a list of platforms and release levels.

To view or download available releases, the platform type and release level type must be selected.

- 1) AIX 5.3
- 2) AIX 6.1
- 3) AIX 7.1
- 4) HP-UX 11.31
- 5) RHEL5 x86\_64
- 6) RHEL6 x86\_64
- 7) RHEL7 x86\_64
- 8) SLES10 x86\_64
- 9) SLES11 x86\_64
- 10) Solaris 9 Sparc
- 11) Solaris 10 Sparc
- 12) Solaris 10 x64
- 13) Solaris 11 Sparc
- 14) Solaris 11 x64
- b) Back to previous menu

Select the platform of the release to view/download [1-14,b,q]

**4 Select the release level for which you want to get release image information. Enter the platform you want.**

You see options for the Symantec release levels.

- 1) Base
- 2) Maintenance
- 3) Patch
- b) Back to previous menu

Select the level of the <platform> releases to view/download [1-3,b,q,?]

**5 Select the number corresponding to the type of release you want to view (Base, Maintenance, or Patch).**

You see a list of releases available for download.

Available Maintenance releases for rhel6\_x86\_64:

| release_version | SORT_release_name              | DL | OBS | AI | rel_date   | size_KB |
|-----------------|--------------------------------|----|-----|----|------------|---------|
| 5.1SP1PR2RP2    | sfha-rhel6_x86_64-5.1SP1PR2RP2 | -  | Y   | Y  | 2011-09-28 | 145611  |
| 5.1SP1PR2RP3    | sfha-rhel6_x86_64-5.1SP1PR2RP3 | -  | Y   | Y  | 2012-10-02 | 153924  |
| 5.1SP1PR2RP4    | sfha-rhel6_x86_64-5.1SP1PR2RP4 | -  | -   | Y  | 2013-08-21 | 186859  |
| 5.1SP1PR3RP2    | sfha-rhel6_x86_64-5.1SP1PR3RP2 | -  | Y   | Y  | 2011-09-28 | 145611  |
| 5.1SP1PR3RP3    | sfha-rhel6_x86_64-5.1SP1PR3RP3 | -  | Y   | Y  | 2012-10-02 | 153924  |

```

5.1SP1PR3RP4 sfha-rhel6_x86_64-5.1SP1PR3RP4 - - Y 2013-08-21 186859
6.0RP1 sfha-rhel6_x86_64-6.0RP1 - - Y 2012-03-22 210076
6.0.3 sfha-rhel6_x86_64-6.0.3 - Y Y 2013-02-01 212845
6.0.5 sfha-rhel6_x86_64-6.0.5 - - Y 2014-04-15 199143
6.1.1 sfha-rhel6_x86_64-6.1.1 - - Y 2014-07-24 208028
Enter the release_version to view details about a release or press 'Enter' to continue [b,q,?]

```

The following are the descriptions for the column headers:

- **release\_version**: The version of the release.
- **SORT\_release\_name**: The name of the release, used when accessing SORT (<https://sort.symantec.com>).
- **DL**: An indicator that the release is present in your repository.
- **OBS**: An indicator that the release is obsolete by another higher release.
- **AI**: An indicator that the release has scripted install capabilities. All base and maintenance releases have auto-install capabilities. Patch releases with auto-install capabilities are available beginning with version 6.1. Otherwise the patch requires a manual installation.
- **rel\_date**: The date the release is available.
- **size\_KB**: The file size of the release in kilobytes.

**6** If you are interested in viewing more details about any release, type the release version. For example, enter the following:

```
6.0.3
```

You see the following output:

```

release_version: 6.0.3
release_name: sfha-rhel6_x86_64-6.0.3
release_type: MR
release_date: 2013-02-01
downloaded: Y
install_path: rhel6_x86_64/installmr
upload_location: ftp://ftp.veritas.com/pub/support/patchcentral
/Linux/6.0.3/sfha/sfha-rhel6_x86_64-6.0.3-patches.tar.gz
obsoletes: 6.0.1.200-fs,6.0.1.200-vm,6.0.1.300-fs
obsoleted_by: None
Would you like to download this Maintenance Release? [y,n,q] (y) n

```

Enter the release\_version to view the details about a release or press 'Enter' to continue [b,q,?]

**7** If you do not need to check detail information, you can press **Enter**.

You see the following question:

```
Would you like to download a rhel6_x86_64 Maintenance Release Image?
[y,n,q] (n) y
```

If you select a **y**, you see a menu of all releases that are not currently in the repository.

- ```
1) 5.1SP1PR2RP2
   2) 5.1SP1PR2RP3
   3) 5.1SP1PR2RP4
   4) 5.1SP1PR3RP2
   5) 5.1SP1PR3RP3
   6) 5.1SP1PR3RP4
   7) 6.0RP1
   8) 6.0.3
   9) 6.0.5
  10) 6.1.1
  11) All non-obsolete releases
  12) All releases
   b) Back to previous menu
```

```
Select the patch release to download, 'All non-obsolete releases' to
download all non-obsolete releases, or 'All releases' to download
all releases [1-5,b,q] 3
```

8 Select the number corresponding to the release that you want to download. You can download a single release, all non-obsolete releases, or all releases.

The selected release images are downloaded to the Deployment Server.

```
Downloading sfha-rhel6_x86_64-6.0RP1 from SORT - https://sort.symantec.com
Downloading 215118373 bytes (Total 215118373 bytes [205.15 MB]): 100%
Untarring sfha-rhel6_x86_64-6.0RP1 ..... Done

sfha-rhel6_x86_64-6.0RP1 has been downloaded successfully.
```

9 From the menu, select option **2, View/Remove Repository Images**, and follow the prompts to check that the release images are loaded.

See [“Viewing or downloading available release images”](#) on page 249.

Viewing or removing repository images stored in your repository

You can use the Deployment Server to conveniently view or remove the release images that are stored in your repository.

To view or remove release images stored in your repository

- 1 Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

Task Menu:

| | |
|----------------------------------|--------------------------|
| R) Manage Repository Images | M) Update Metadata |
| V) Version Check Systems | S) Set Preferences |
| I) Install/Upgrade Systems | U) Terminology and Usage |
| B) Define/Modify Install Bundles | ?) Help |
| T) Create Install Templates | Q) Quit |

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]

- 2 Select option **R, Manage Repository Images**.

You see the following output:

```
1) View/Download Available Releases
2) View/Remove Repository Images
3) Load a Release Image
b) Back to previous menu
```

Select the option you would like to perform [1-3,b,q,?]

- 3** Select option **2, View/Remove Repository Images**, to view or remove the release images currently installed on your system.

You see a list of platforms and release levels if you have downloaded the corresponding Base, Maintenance, or Patch release on that platform.

To view or remove repository images, the platform type and release level type must be selected.

- ```

1) AIX 5.3 2) AIX 6.1
3) AIX 7.1 4) HP-UX 11.31
5) RHEL5 x86_64 6) RHEL6 x86_64
7) RHEL7 x86_64 8) SLES10 x86_64
9) SLES11 x86_64 10) Solaris 9 Sparc
11) Solaris 10 Sparc 12) Solaris 10 x64
13) Solaris 11 Sparc 14) Solaris 11 x64
b) Back to previous menu

```

Select the platform of the release to view/remove [1-14,b,q]

- 4** Select the release level for which you want to get release image information. Enter the platform you want.

You see options for the Symantec release levels if you have downloaded the corresponding Base, Maintenance, or Patch release.

- ```

1)  Base
2)  Maintenance
3)  Patch
b)  Back to previous menu
    
```

Select the level of the <platform> releases to view/remove [1-3,b,q]

- 5** Select the number corresponding to the type of release you want to view or remove (Base, Maintenance, or Patch).

You see a list of releases that are stored in your repository.

Stored Repository Releases:

```

release_version SORT_release_name          OBS AI
=====
6.0RP1          sfha-rhel6_x86_64-6.0RP1  -   Y
6.0.3           sfha-rhel6_x86_64-6.0.3  -   Y
    
```

- 6 If you are interested in viewing more details about a release image that is stored in your repository, type the release version. For example, enter the following:

```
6.0.3
```

- 7 If you do not need to check detail information, you can press **Enter**. You see the following question:

```
Would you like to remove a rhel6_x86_64 Maintenance Release Image?
[y,n,q] (n) y
```

If you select a **y**, you see a menu of all the releases that are stored in your repository that match the selected platform and release level.

```
1) 6.0RP1
2) 6.0.3
b) Back to previous menu
```

```
Select the patch release to remove [1-2,b,q] 1
```

- 8 Type the number corresponding to the release version you want to remove. The release images are removed from the Deployment Server.

```
Removing sfha-rhel6_x86_64-6.0RP1-patches ..... Done
sfha-rhel6_x86_64-6.0RP1-patches has been removed successfully.
```

Deploying Symantec product updates to your environment

You can use the Deployment Server to deploy release images to the systems in your environment as follows:

- If you are not sure what to deploy, perform a version check. A version check tells you if there are any Symantec products installed on your systems. It suggests patches and maintenance releases, and gives you the option to install updates.

See [“Finding out which releases you have installed, and which upgrades or updates you may need”](#) on page 257.

- If you know which update you want to deploy on your systems, use the Install/Upgrade Systems script to deploy a specific Symantec release. See “[Deploying Symantec releases](#)” on page 266.

Finding out which releases you have installed, and which upgrades or updates you may need

Use the Version Check option to determine which Symantec product you need to deploy. The Version Check option is useful if you are not sure which releases you already have installed, or you want to know about available releases.

The Version Check option gives you the following information:

- Installed products and their versions (base, maintenance releases, and patches)
- Installed RPMs (required and optional)
- Available releases (base, maintenance releases, and patches) relative to the version which is installed on the system

To determine which Symantec product updates to deploy

- 1 Launch the Deployment Server. For example, enter the following:

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

Task Menu:

| | |
|----------------------------------|--------------------------|
| R) Manage Repository Images | M) Update Metadata |
| V) Version Check Systems | S) Set Preferences |
| I) Install/Upgrade Systems | U) Terminology and Usage |
| B) Define/Modify Install Bundles | ?) Help |
| T) Create Install Templates | Q) Quit |

```
Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

- 2 Select option **V, Version Check Systems**.

Finding out which releases you have installed, and which upgrades or updates you may need

- 3 At the prompt, enter the system names for the systems you want to check. For example, enter the following:

```
node01
```

You see output for the installed RPMs (required, optional, or missing).

You see a list of releases available for download.

Available Base Releases for Veritas Storage Foundation HA 6.0.1:

| release_version | SORT_release_name | DL | rel_date | size_KB |
|-----------------|-------------------------|----|------------|---------|
| 6.0.2 | sfha-rhel6_x86_64-6.0.2 | - | 2012-10-22 | 985909 |
| 6.1 | sfha-rhel6_x86_64-6.1 | Y | 2013-12-02 | 1047939 |

Available Maintenance Releases for Veritas Storage Foundation HA 6.0.1:

| release_version | SORT_release_name | DL | OBS | AI | rel_date | size_KB |
|-----------------|-------------------------|----|-----|----|------------|---------|
| 6.0.3 | sfha-rhel6_x86_64-6.0.3 | - | Y | - | 2013-02-01 | 212845 |
| 6.0.5 | sfha-rhel6_x86_64-6.0.5 | Y | - | - | 2014-04-15 | 199143 |
| 6.1.1 | sfha-rhel6_x86_64-6.1.1 | - | - | - | 2014-07-24 | 208028 |

Available Patches for Veritas Storage Foundation HA 6.0.1:

| release_version | SORT_release_name | DL | OBS | AI | rel_date | size_KB |
|-----------------|----------------------------|----|-----|----|------------|---------|
| 6.0.1.200-vm | vm-rhel6_x86_64-6.0.1.200 | - | Y | - | 2012-10-10 | 21359 |
| 6.0.1.300-fs | fs-rhel6_x86_64-6.0.1.300a | - | Y | - | 2012-12-20 | 7601 |

Would you like to download the available Maintenance or Patch releases that cannot be found in the repository? [y,n,q] (n)

- 4 If you want to download any of the available maintenance releases or patches, enter **y**.
- 5 If you have not set a default repository for releases you download, the installer prompts you for a directory. (You can also set the default repository in **Set Preferences**).

See [“Setting deployment preferences”](#) on page 245.

- 6 Select an option for downloading products.

The installer downloads the releases you specified and stores them in the repository.

Defining Install Bundles

You can use Install Bundles to directly install the latest base, maintenance, and patch releases on your system. Install Bundles are a combination of base, maintenance, and patch releases that can be bundled and installed or upgraded in one operation.

Note: Install Bundles can be defined only from version 6.1 or later. The exception to this rule is base releases 6.0.1, 6.0.2, or 6.0.4 or later with maintenance release 6.0.5 or later.

To define Install Bundles

- 1 Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

Task Menu:

```
R) Manage Repository Images           M) Update Metadata
V) Version Check Systems              S) Set Preferences
I) Install/Upgrade Systems           U) Terminology and Usage
B) Define/Modify Install Bundles     ?) Help
T) Create Install Templates          Q) Quit
```

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]

- 2 Select option **B, Define/Modify Install Bundles**.

You see the following output the first time you enter:

Select a Task:

```
1) Create a new Install Bundle
b) Back to previous menu
```

Select the task you would like to perform [1-1,b,q]

3 Select option 1, **Create a new Install Bundle.**

You see the following output:

```
Enter the name of the Install Bundle you would like to define:
{press [Enter] to go back)
```

For example, if you entered:

```
rhel605
```

You see the following output:

```
To create an Install Bundle, the platform type must be selected:
```

- | | |
|--------------------------|---------------------|
| 1) AIX 5.3 | 2) AIX 6.1 |
| 3) AIX 7.1 | 4) HP-UX 11.31 |
| 5) RHEL5 x86_64 | 6) RHEL6 x86_64 |
| 7) RHEL7 x86_64 | 8) SLES10 x86_64 |
| 9) SLES11 x86_64 | 10) Solaris 9 Sparc |
| 11) Solaris 10 Sparc | 12) Solaris 10 x64 |
| 13) Solaris 11 Sparc | 14) Solaris 11 x64 |
| b) Back to previous menu | |

```
Select the platform of the release for the Install Bundle rhel605:
[1-14,b,q]
```

- 4 Select the number corresponding to the platform you want to include in the Install Bundle. For example, select the number for the **RHEL5 x86_64** release, **5**.

You see the following output:

```
Details of the Install Bundle: rhel605
```

```
Install Bundle Name    rhel605
Platform              RHEL5 x86_64
Base Release          N/A
Maintenance Release   N/A
Patch Releases        N/A
```

- 1) Add a Base Release
- 2) Add a Maintenance Release
- 3) Add a Patch Release
- 4) Change Install Bundle Name
- b) Back to previous menu

```
Select an action to perform on the Install Bundle rhel605 [1-4,b,q]
```

- 5 Select option **1, Add a Base Release**.

You see the following output:

- 1) 6.0.1
- 2) 6.0.2
- 3) 6.1
- b) Back to previous menu

```
Select the Base Release version to add to the Install Bundle rhel605
[1-3,b,q]
```

6 Select option 1, 6.0.1.

You see the following output:

```
Symantec Storage Foundation and High Availability Solutions 6.2 Deployment Server Program
pilotlnx11
```

```
Details of the Install Bundle: rhel605
```

```
Install Bundle Name    rhel605
Platform              RHEL5 x86_64
Base Release          6.0.1
Maintenance Release   N/A
Patch Releases        N/A
```

- 1) Remove Base Release 6.0.1
- 2) Add a Maintenance Release
- 3) Add a Patch Release
- 4) Change Install Bundle Name
- b) Back to previous menu

```
Select an action to perform on the Install Bundle rhel605 [1-4,b,q]
```

7 Select option 2, Add a Maintenance Release.

You see the following output:

- 1) 6.0.5
- b) Back to previous menu

```
Select the Maintenance Release version to add to the Install Bundle
rhel605 [1-1,b,q]
```

8 Select option 1, 6.0.5.

You see the following output:

```
Symantec Storage Foundation and High Availability Solutions 6.2 Deployment Server Program
pilotlnx11
```

```
Details of the Install Bundle: rhel605
```

```
Install Bundle Name    rhel605
Platform              RHEL5 x86_64
Base Release          6.0.1
Maintenance Release   6.0.5
Patch Releases        N/A
```

- 1) Remove Base Release 6.0.1
- 2) Remove Maintenance Release 6.0.5
- 3) Add a Patch Release
- 4) Save Install Bundle rhel605
- 5) Change Install Bundle Name
- b) Back to previous menu

```
Select an action to perform on the Install Bundle rhel605
[1-5,b,q]
```

9 Select option 4, Save Install Bundle.

You see the following output:

```
Install Bundle rhel605 has been saved successfully
```

```
Press [Enter] to continue:
```

If there are no releases for the option you selected, you see a prompt saying that there are no releases at this time. You are prompted to continue.

After selecting the desired base, maintenance, or patch releases, you can choose to save your Install Bundle.

The specified Install Bundle is saved on your system. The specified Install Bundle is available as an installation option when using the **I) Install/Upgrade Systems** option to perform an installation or upgrade.

Creating Install Templates

You can use Install Templates to discover installed components (RPMs, patches, products, or versions) on a system that you want to replicate. Use Install Templates to automatically install those same components on to other systems.

To create Install Templates

- 1 Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

- 2 You see the following output:

```
Task Menu:
```

```
R) Manage Repository Images           M) Update Metadata
V) Version Check Systems              S) Set Preferences
I) Install/Upgrade Systems           U) Terminology and Usage
B) Define/Modify Install Bundles     ?) Help
T) Create Install Templates          Q) Quit
```

```
Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

- 3 Select option **T, Create Install Templates**.

- 4 You see the following output:

```
Select a Task:
```

```
1) Create a new Install Template
b) Back to previous menu
```

```
Select the task you would like to perform [1-1,b,q]
```


5 Select option 1, Create a new Install Template.

You see the following output:

Enter the system names separated by spaces for creating an Install Template:
 (press [Enter] to go back)

For example, if you entered `rhel89202` as the system name, you see the following output:

```
Enter the system names separated by spaces for version checking: rhel89202

Checking communication on rhel89202 ..... Done
Checking installed products on rhel89202 ..... Done

Platform of rhel89202:
    Linux RHEL 6.3 x86_64

Installed product(s) on rhel89202:
    Symantec Storage Foundation Cluster File System HA - 6.1.1 - license vxkeyless

Product:
    Symantec Storage Foundation Cluster File System HA - 6.1.1 - license vxkeyless

Packages:
    Installed Required packages for Symantec Storage Foundation Cluster File System HA 6.1.1:
        #PACKAGE      #VERSION
        VRTSsamf      6.1.1.000
        VRTSaslapm    6.1.1.000
        .....
        .....
        VRTSvxfs      6.1.1.000
        VRTSvxvm      6.1.1.000

    Installed optional packages for Symantec Storage Foundation Cluster File System HA 6.1.1:
        #PACKAGE      #VERSION
        VRTSdbed      6.1.1.000
        VRTSgms       6.1.0.000
        .....
        .....
        VRTSvcscdr    6.1.0.000
        VRTSvcsea     6.1.1.000

    Missing optional packages for Symantec Storage Foundation Cluster File System HA 6.1.1:
        #PACKAGE
```

```
VRTScps
VRTSfssdk
VRTSsvmconv
```

Summary:

Packages:

```
17 of 17 required Symantec Storage Foundation Cluster File System HA 6.1.1 packages installed
8 of 11 optional Symantec Storage Foundation Cluster File System HA 6.1.1 packages installed
```

Installed Public and Private Hot Fixes for Symantec Storage Foundation Cluster File System HA 6.1.1:

```
None
```

Would you like to generate a template file based on the above release information? [y,n,q] (y)

- 1) rhel89202
- b) Back to previous menu

Select a machine list to generate the template file [1-1,b,q]

6 Select option 1, rhel89202.

You see the following output:

```
Enter the name of the Install Template you would like to define:
(press [Enter] to go back)
```

7 Enter the name of your Install Template. For example, if you enter **MyTemplate** as the name for your Install Template, you would see the following:

```
Install Template MyTemplate has been saved successfully
```

```
Press [Enter] to continue:
```

All of the necessary information is stored in the Install Template you created.

Deploying Symantec releases

You can use the Deployment Server to deploy your licensed Symantec products dating back to version 5.1. If you know which product version you want to install, follow the steps in this section to install it.

You can use the Deployment Server to install the following:

- A single Symantec release
- Two or more releases using defined Install Bundles
 See “[Defining Install Bundles](#)” on page 259.
- Installed components on a system that you want to replicate on another system
 See “[Creating Install Templates](#)” on page 264.

To deploy a specific Symantec release

- 1 From the directory in which you installed your Symantec product (version 6.1 or later), launch the Deployment Server with the upgrade and install systems option. For example, enter the following:

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

Task Menu:

```
R) Manage Repository Images           M) Update Metadata
V) Version Check Systems              S) Set Preferences
I) Install/Upgrade Systems           U) Terminology and Usage
B) Define/Modify Install Bundles     ?) Help
T) Create Install Templates          Q) Quit
```

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]

- 2 **Select option I, Install/Upgrade Systems.**

You see the following output:

```
1) AIX 5.3
2) AIX 6.1
3) AIX 7.1
4) RHEL5 x86_64
b) Back to previous menu
```

Select the platform of the available release(s) to be upgraded/installed [1-4,b,q,?]

- 3 Select the number corresponding to the platform for the release you want to deploy. For example, select the number for the **RHEL5 x86_64** release or the **AIX 6.1** release.

You see the following output:

- ```
1) Install/Upgrade systems using a single release
2) Install/Upgrade systems using an Install Bundle
3) Install systems using an Install Template
b) Back to previous menu
```

```
Select the method by which you want to Install/Upgrade your systems
[1-3,b,q]
```

- 4 Section option **1, Install/Upgrade systems using a single release** if you want to deploy a specific Symantec release.

Select a Symantec product release.

The installation script is executed and the release is deployed on the specified server.

#### To deploy an Install Bundle

- 1 Follow Steps [1](#) - [3](#).
- 2 Select option **2, Install/Upgrade systems using an Install Bundle**.

You see the following output:

- ```
1) <NameofInstallBundle1>
2) <NameofInstallBundle2>
b) Back to previous menu
```

```
Select the bundle to be installed/upgraded [1-2,b,q]
```

You see the following output:

```
Enter the platform target system name(s) separated by spaces:
[press [Enter] to go back)
```

- 3 Enter the name of the target system for which you want to install or upgrade the Install Bundle.

The installation script for the selected Install Bundle is executed, and the Install Bundle is deployed on the specified target system.

To deploy an Install Template

- 1 Follow Steps 1 - 3.
- 2 Select option **3, Install/Upgrade systems using an Install Template**.

You see the following output:

```
1) <NameofInstallTemplate>
b) Back to previous menu
```

```
Select the template to be installed [1-1,b,q] 1
```

You see the following output:

```
Enter the platform target system name(s) separated by spaces:
[press [Enter] to go back)
```

The installation script for the selected Install Template is executed, and the Install Template is deployed on the specified target system.

Connecting the Deployment Server to SORT using a proxy server

You can use a proxy server, a server that acts as an intermediary for requests from clients, for connecting the Deployment Server to the Symantec Operations Readiness Tools (SORT) website.

To enable the proxy access, run the following commands to set the shell environment variables before you launch Deployment Server. The shell environment variables enable Deployment Server to use the proxy server myproxy.mydomain.com which connects to port 3128.

```
http_proxy="http://myproxy.mydomain.com:3128"
export http_proxy
```

```
ftp_proxy="http://myproxy.mydomain.com:3128"
export ftp_proxy
```

The lines above can be added to the user's shell profile. For the bash shell, the profile is the `~/.bash_profile` file.

Post-installation tasks

This chapter includes the following topics:

- [Verifying the installation](#)
- [Performing additional post-installation and configuration tasks](#)

Verifying the installation

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 378.

To run the postcheck command on a node

- 1 Run the installer with the `-postcheck` option.

```
# cd /opt/VRTS/install  
  
# ./installsfsybasece62 -postcheck system_name
```

- 2 Review the output for installation-related information.

Verifying SF Sybase CE installation using VCS configuration file

The configuration file, `main.cf`, is created on each node at `/etc/VRTSvcs/conf/config/`. Review the `main.cf` configuration file after the SF Sybase CE installation and before the Sybase installation.

Verify the following information in the `main.cf` file:

- The cluster definition within the `main.cf` includes the cluster information that was provided during the configuration. The cluster information includes the cluster name, cluster address, and the names of cluster users and administrators.
- The `UseFence = SCSI3` attribute is present in the file.
- If you configured the cluster in secure mode, the “`SecureClus = 1`” cluster attribute is set.

For more information on the configuration file:

Verifying LLT, GAB, and cluster operation

Verify the operation of LLT, GAB, and the cluster using the VCS commands.

To verify LLT, GAB, and cluster operation

- 1 Log in to any node in the cluster as superuser.
- 2 Make sure that the `PATH` environment variable is set to run the VCS commands.
- 3 Verify LLT operation.
- 4 Verify GAB operation.
- 5 Verify the cluster operation.

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 `node01`.
- 2 Run the `lltstat` command on the node `node01` to view the status of LLT.

```
lltstat -n
```

The output on `node01` resembles:

```
LLT node information:
Node           State      Links
*0 node01     OPEN      2
 1 node02     OPEN      2
```

Each node has two links and each node is in the OPEN state. The asterisk (*) denotes the node on which you typed the command.

If LLT does not operate, the command does not return any LLT links information: If only one network is connected, the command returns the following LLT statistics information:

```
LLT node information:
  Node           State   Links
* 0 node01      OPEN    2
  1 node02      OPEN    2
  2 sys5        OPEN    1
```

- 3 Log in as superuser on the node node02.
- 4 Run the `lltstat` command on the node node02 to view the status of LLT.

```
lltstat -n
```

The output on node02 resembles:

```
LLT node information:
  Node           State   Links
  0 node01      OPEN    2
*1 node02      OPEN    2
```

- 5 To view additional information about LLT, run the `lltstat -nvv` command on each node.

For example, run the following command on the node node01 in a two-node cluster:

```
lltstat -nvv active
```

The output on node01 resembles:

```
Node           State   Link   Status   Address
*0 node01      OPEN
                net1 UP    08:00:20:93:0E:34
                net2 UP    08:00:20:93:0E:38
  1 node02      OPEN
                net1 UP    08:00:20:8F:D1:F2
                net2 DOWN
```

The command reports the status on the two active nodes in the cluster, node01 and node02.

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 node02. 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 node01 in a two-node cluster:

```
lltstat -p
```

The output resembles:

```
LLT port information:
  Port  Usage      Cookie
  ---  ---
  0     gab        0x0
       opens:   0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
       connects: 0 1
  7     gab        0x7
       opens:   0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
       connects: 0 1
  31    gab        0x1F
       opens:   0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
       connects: 0 1
```

Verifying GAB

Verify the GAB operation using the `gabconfig -a` command. This command returns the GAB port membership information. The output displays the nodes that have membership with the modules you installed and configured. You can use GAB port membership as a method of determining if a specific component of the SFHA stack communicates with its peers.

[Table 10-1](#) lists the different ports that the software configures for different functions.

Table 10-1 GAB port description

| Port | Function |
|------|-------------|
| a | GAB |
| b | I/O fencing |

Table 10-1 GAB port description (*continued*)

| Port | Function |
|------|--|
| f | Cluster File System (CFS) |
| h | Symantec Cluster Server (VCS: High Availability Daemon) |
| m | Cluster Volume Manager (CVM) CVM uses port m for SmartIO VxVM cache coherency using Group Lock Manager (GLM). |
| u | Cluster Volume Manager (CVM) (to ship commands from slave node to master node) Port u in the <code>gabconfig</code> output is visible with CVM protocol version ≥ 100 . Run the <code>vxctl protocolversion</code> command to check the protocol version. |
| v | Cluster Volume Manager (CVM) |
| w | vxconfigd (module for CVM) |
| y | Cluster Volume Manager (CVM) I/O shipping |

For more information on GAB, refer to the *Symantec Cluster Server Administrator's Guide*.

To verify GAB

- ◆ To verify the GAB operation, type the following command on each node:

```
# /sbin/gabconfig -a
```

For example, the command returns the following output:

```
GAB Port Memberships
=====
Port a gen fd6a01 membership 01
Port b gen fd6a03 membership 01
Port f gen fd6a12 membership 01
Port h gen fd6a06 membership 01
Port m gen fd6a0b membership 01
Port u gen fd6a10 membership 01
Port v gen fd6a09 membership 01
Port w gen fd6a0d membership 01
Port y gen fd6a08 membership 01
```

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 *Symantec 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  node01          RUNNING      0
A  node02          RUNNING      0

-- GROUP STATE
-- Group          System      Probed  AutoDisabled  State
```

- 2 Review the command output for the following information:
 - The system state
If the value of the system state is `RUNNING`, the cluster is successfully started.

Verifying the cluster nodes

Verify the information of the cluster systems using the `hasys -display` command. The information for each node in the output should be similar.

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

Refer to the *Symantec Cluster Server Administrator's Guide* for information about the system attributes for VCS.

To verify the cluster nodes

- ◆ On one of the nodes, type the `hasys -display` command:

```
# hasys -display
```

The example in the following procedure shows the output when the command is run on the node node01. The list continues with similar information for node02 (not shown) and any other nodes in the cluster.

```

#System      Attribute          Value
node01      AgentsStopped      0
node01      AvailableCapacity  100
node01      CPUThresholdLevel  Critical 90 Warning 80 Note 70
              Info 60
node01      CPUUsage           0
node01      CPUUsageMonitoring Enabled 0 ActionThreshold 0
              ActionTimeLimit 0 Action NONE
              NotifyThreshold 0 NotifyTimeLimit 0

node01      Capacity           100
node01      ConfigBlockCount   293
node01      ConfigChecksum     37283
node01      ConfigDiskState    CURRENT
node01      ConfigFile         /etc/VRTSvcs/conf/config
node01      ConfigInfoCnt      0
node01      ConfigModDate      Mon Sep 03 07:14:23 CDT 2012
node01      ConnectorState     Up
node01      CurrentLimits
node01      DiskHbStatus
node01      DynamicLoad        0
node01      EngineRestarted    0
node01      EngineVersion      6.2.00.0
node01      FencingWeight      0
node01      Frozen             0
node01      GUIIPAddr
    
```

```

node01      HostUtilization      CPU 0 Swap 0
node01      LLTNodeId                  0
node01      LicenseType                PERMANENT_SITE
node01      Limits
node01      LinkHbStatus               net1 UP net2 UP
node01      LoadTimeCounter            0
node01      LoadTimeThreshold          600
node01      LoadWarningLevel           80
node01      NoAutoDisable              0
node01      NodeId                     0
node01      OnGrpCnt                   7
node01      PhysicalServer
node01      ShutdownTimeout            600
node01      SourceFile                  ./main.cf
node01      SwapThresholdLevel         Critical 90 Warning 80 Note 70
                                Info 60
node01      SysName                     node01
node01      SysState                    RUNNING
node01      SystemLocation
node01      SystemOwner
node01      SystemRecipients
node01      TFrozen                     0
node01      TRSE                        0
node01      UpDownState                 Up
node01      UserInt                     0
node01      UserStr
node01      VCSFeatures                 DR

```

```
node01      VCSMode      VCS
            VCS_RAC
            VCS_CFS_VRTS
```

Performing additional post-installation and configuration tasks

About enabling LDAP authentication for clusters that run in secure mode

Symantec Product Authentication Service (AT) supports LDAP (Lightweight Directory Access Protocol) user authentication through a plug-in for the authentication broker. AT supports all common LDAP distributions such as OpenLDAP and Windows Active Directory.

For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain.

See the *Symantec Cluster Server Installation Guide* for more information.

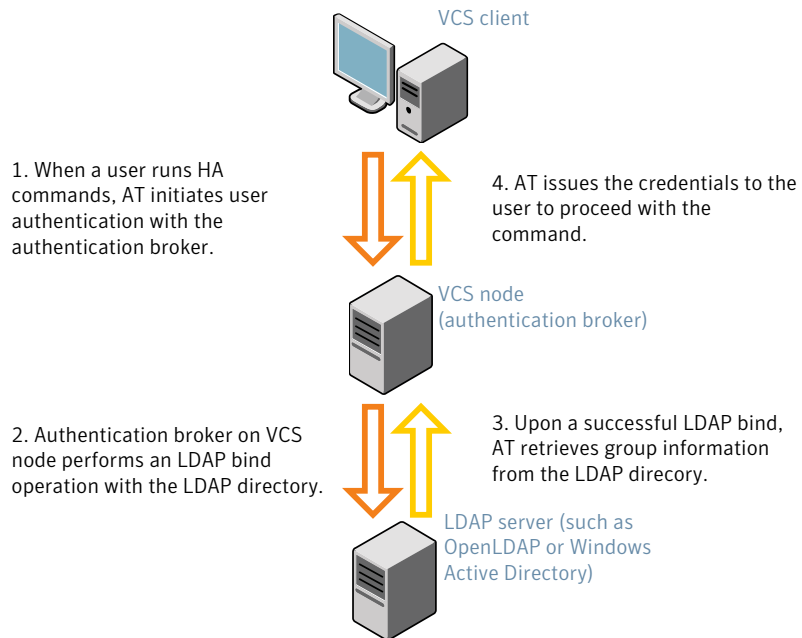
See [“Enabling LDAP authentication for clusters that run in secure mode”](#) on page 280.

If you have not already added VCS users during installation, you can add the users later.

See the *Symantec Cluster Server Administrator's Guide* for instructions to add VCS users.

[Figure 10-1](#) depicts the SF Sybase CE cluster communication with the LDAP servers when clusters run in secure mode.

Figure 10-1 Client communication with LDAP servers



The LDAP schema and syntax for LDAP commands (such as `ldapadd`, `ldapmodify`, and `ldapsearch`) vary based on your LDAP implementation.

Before adding the LDAP domain in Symantec Product Authentication Service, note the following information about your LDAP environment:

- The type of LDAP schema used (the default is RFC 2307)
 - UserObjectClass (the default is `posixAccount`)
 - UserObject Attribute (the default is `uid`)
 - User Group Attribute (the default is `gidNumber`)
 - Group Object Class (the default is `posixGroup`)
 - GroupObject Attribute (the default is `cn`)
 - Group GID Attribute (the default is `gidNumber`)
 - Group Membership Attribute (the default is `memberUid`)
- URL to the LDAP Directory
- Distinguished name for the user container (for example, `UserBaseDN=ou=people,dc=comp,dc=com`)

- Distinguished name for the group container (for example, GroupBaseDN=ou=group,dc=comp,dc=com)

Enabling LDAP authentication for clusters that run in secure mode

The following procedure shows how to enable the plug-in module for LDAP authentication. This section provides examples for OpenLDAP and Windows Active Directory LDAP distributions.

Before you enable the LDAP authentication, complete the following steps:

- Make sure that the cluster runs in secure mode.

```
# haclus -value SecureClus
```

The output must return the value as 1.

- Make sure that the AT version is 6.1.6.0 or later.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showversion
vssat version: 6.1.12.0
```

See the `vssat.1m` and the `atldapconf.1m` manual pages.

To enable OpenLDAP authentication for clusters that run in secure mode

- 1 Run the LDAP configuration tool `atldapconf` using the `-d` option. The `-d` option discovers and retrieves an LDAP properties file which is a prioritized attribute list.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
-d -s domain_controller_name_or_ipaddress -u domain_user

Attribute list file name not provided, using AttributeList.txt

Attribute file created.
```

You can use the `catatldapconf` command to view the entries in the attributes file.

- 2 Run the LDAP configuration tool using the `-c` option. The `-c` option creates a CLI file to add the LDAP domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
-c -d LDAP_domain_name

Attribute list file not provided, using default AttributeList.txt

CLI file name not provided, using default CLI.txt

CLI for addldapdomain generated.
```

- 3 Run the LDAP configuration tool `atldapconf` using the `-x` option. The `-x` option reads the CLI file and executes the commands to add a domain to the AT.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf -x

Using default broker port 14149

CLI file not provided, using default CLI.txt

Looking for AT installation...

AT found installed at ./vssat

Successfully added LDAP domain.
```

- 4 Check the AT version and list the LDAP domains to verify that the Windows Active Directory server integration is complete.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showversion
vssat version: 6.1.12.8

# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat listldapdomains
Domain Name : mydomain.com
Server URL : ldap://192.168.20.32:389
SSL Enabled : No
User Base DN : CN=people,DC=mydomain,DC=com
User Object Class : account
User Attribute : cn
User GID Attribute : gidNumber
Group Base DN : CN=group,DC=symantecdomain,DC=com
Group Object Class : group
Group Attribute : cn
Group GID Attribute : cn
Auth Type : FLAT
Admin User :
Admin User Password :
Search Scope : SUB
```

- 5 Check the other domains in the cluster.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showdomains -p vx
```

The command output lists the number of domains that are found, with the domain names and domain types.

6 Generate credentials for the user.

```
# unset EAT_LOG

# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat authenticate \
-d ldap:LDAP_domain_name -p user_name -s user_password -b \
localhost:14149
```

7 Add non-root users as applicable.

```
# useradd user1

# passwd pw1

Changing password for "user1"
user1's New password:

Re-enter user1's new password:

# su user1

# bash

# id

uid=204(user1) gid=1(staff)

# pwd

# mkdir /home/user1

# chown user1 /home/ user1
```

8 Add the non-root user to the VCS configuration.

```
# haconf -makerw
# hauser -add user1
# haconf -dump -makero
```

9 Log in as non-root user and run VCS commands as LDAP user.

```
# cd /home/user1

# ls

# cat .vcspwd

101 localhost mpise LDAP_SERVER ldap

# unset VCS_DOMAINTYPE

# unset VCS_DOMAIN

# /opt/VRTSvcs/bin/hasys -state

#System      Attribute      Value
cluster1:sysA  SysState      FAULTED
cluster1:sysB  SysState      FAULTED
cluster2:sysC  SysState      RUNNING
cluster2:sysD  SysState      RUNNING
```

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 \  
-s domain_controller_name_or_ipaddress \  
-u domain_user -g domain_group
```

For example:

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \  
-d -s 192.168.20.32 -u Administrator -g "Domain Admins"  
Search User provided is invalid or Authentication is required to  
proceed further.  
Please provide authentication information for LDAP server.
```

```
Username/Common Name: symantecdomain\administrator  
Password:
```

Attribute file created.

- 2** Run the LDAP configuration tool `atldapconf` using the `-c` option. The `-c` option creates a CLI file to add the LDAP domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \  
-c -d windows_domain_name
```

For example:

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \  
-c -d symantecdomain.com  
Attribute list file not provided, using default AttributeList.txt.  
CLI file name not provided, using default CLI.txt.
```

CLI for `addldapdomain` generated.

- 3** Run the LDAP configuration tool `atldapconf` using the `-x` option. The `-x` option reads the CLI file and executes the commands to add a domain to the AT.

```
# /opt/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
```

```
Domain Name :          symantecdomain.com
Server URL :          ldap://192.168.20.32:389
SSL Enabled :          No
User Base DN :          CN=people,DC=symantecdomain,DC=com
User Object Class :    account
User Attribute :       cn
User GID Attribute :   gidNumber
Group Base DN :        CN=group,DC=symantecdomain,DC=com
Group Object Class :   group
Group Attribute :      cn
Group GID Attribute :  cn
Auth Type :            FLAT
Admin User :
Admin User Password :
Search Scope :         SUB
```

- 5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh) or 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

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System      Attribute    Value
node01       Attribute    RUNNING
node02       Attribute    RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the SF Sybase CE 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.

Configuring Volume Replicator

Perform this step only if you have not already configured VVR during the installation.

By default, the installer installs the required VVR configuration files irrespective of whether or not you choose to enable VVR. To configure VVR manually in SF Sybase CE, simply start VVR using the `vxstart_vvr` command . The command starts the VVR daemons and configures the ports. You may change the default settings at any time.

For instructions on changing the default settings, see the *Volume Replicator Administrator's Guide*.

To configure VVR

- 1 Log into each node in the cluster as the root user.
- 2 Start VVR:

```
# vxstart_vvr start
VxVM VVR INFO V-5-2-3935 Using following ports:
heartbeat: 4145
vradmind: 8199
vxrsyncd: 8989
data: Anonymous-Ports
To change, see vrport(1M) command
VxVM VVR V-5-2-5942 Starting Communication daemon: [OK]
```

Running SORT Data Collector to collect configuration information

SORT Data Collector now supersedes the VRTExplorer utility. Run the Data Collector with the `VxExplorer` option to gather information about the system.

Visit the SORT Website and download the UNIX Data Collector appropriate for your operating system.

<https://sort.symantec.com>

For more information:

<https://sort.symantec.com/public/help/wwhelp/wwimpl/js/html/wwhelp.htm>

Installing and configuring Sybase ASE CE

This chapter includes the following topics:

- [Before installing Sybase ASE CE](#)
- [Preparing for local mount point on VxFS for Sybase ASE CE binary installation](#)
- [Preparing for shared mount point on CFS for Sybase ASE CE binary installation](#)
- [Installing Sybase ASE CE software](#)
- [Preparing to create a Sybase ASE CE cluster](#)
- [Creating the Sybase ASE CE cluster](#)
- [Preparing to configure the Sybase instances under VCS control](#)
- [Configuring a Sybase CE cluster under VCS control using the SF Sybase CE installer](#)

Before installing Sybase ASE CE

Before you install Sybase ASE CE, make sure that you perform the following tasks:

- Install SF Sybase CE
- Configure SF Sybase CE
- Set I/O fencing to Sybase mode

The high level flow for installing Sybase ASE CE in an SF Sybase CE environment:

- Create the Sybase user and groups. See Sybase ASE CE documentation.

- Create local or shared disk group, volume, and mount point for Sybase binary installation
- Install Sybase ASE CE
- Create a disk group, volume, and mount point for the Sybase quorum device
- Create a disk group, volume, and mount point for the Sybase datafiles
- Create the Sybase ASE CE cluster
- Configure Sybase ASE CE instances under VCS control

Preparing for local mount point on VxFS for Sybase ASE CE binary installation

The following procedure provides instructions for setting up the disk groups, volume, and mount point for installing Sybase ASE CE binaries for local mount point on VxFS.

To create the disk group, volume and mount point for Sybase binaries

- 1 Initialize the disk.

For example:

```
# vxdisksetup -i Disk_1 format=cddisk
```

- 2 Create a diskgroup.

For example:

```
# vxdg init sybbin_dg Disk_1 Disk_2
```

- 3 Create a mirrored volume in the group:

```
# vxassist -g sybbin_dg make sybbin_vol  
12G layout=mirrored nmirrors=2
```

- 4 Create a VxFS file system on which to install the Sybase binaries:

```
# mkfs -t vxfs /dev/vx/rdisk/sybbin_dg/sybbin_vol
```

For a binary installation on a local file system, run the command on each node.

- 5 Create the sybase home (\$SYBASE) directory on the node:

```
# mkdir /sybase
```

- 6 Mount the directory:

```
# mount -t vxfs /dev/vx/dsk/sybbin_dg/sybbin_vol /sybase
```

- 7 Repeat the above steps on all other cluster nodes.
- 8 On each system, change permission of the directory to sybase.

```
# chown -R sybase:sybase /sybase
```

Preparing for shared mount point on CFS for Sybase ASE CE binary installation

The following procedure provides instructions for setting up the disk groups, volume, and mount point for installing Sybase ASE CE binaries for shared mount point on CFS.

To create the disk group, volume and mount point for Sybase binaries

- 1 Initialize the disk.

For example:

```
# vxdisksetup -i Disk_1 format=cddisk
```

- 2 Create a CVM diskgroup.

For example:

```
# vxdg -s init sybbin_dg Disk_1 Disk_2
```

- 3 Create a mirrored volume in the group:

```
# vxassist -g sybbin_dg make sybbin_vol  
12G layout=mirrored nmirrors=2
```

- 4 Create a VxFS file system on which to install the Sybase binaries:

```
# mkfs -t vxfs -o largefiles /dev/vx/rdisk/sybbin_dg/sybbin_vol
```

For a binary installation on a shared file system, you may run the command on any one node.

- 5 Create a Sybase ASE CHome directory (\$SYBASE) on all nodes:

```
# mkdir /sybase
```

- 6 Mount the directory:

```
# mount -t vxfs -o cluster /dev/vx/dsk/sybbin_dg/sybbin_vol /sybase
```

- 7 On each system, change permission of the directory to sybase.

```
# chown -R sybase:sybase /sybase
```

Installing Sybase ASE CE software

For information on installing Sybase ASE CE software, see the Sybase ASE CE product documentation.

Requirements for the Sybase ASE CE configuration:

- Use the CFS mount points you created in the previous section for installing the binaries

Preparing to create a Sybase ASE CE cluster

The following procedure provides instructions for creating a file system for the quorum device.

To create the disk group, volume and mount point for a quorum device

- 1 Initialize the disk.

For example:

```
# vxdisksetup -i Disk_3 format=cddisk  
# vxdisksetup -i Disk_4 format=cddisk
```

- 2 As root user, from the CVM master, create a shared VxVM diskgroup for the quorum device.

```
# vxdg -s init quorum_dg Disk_3 Disk_4
```

- 3 As root user, from the CVM master, create a mirrored volume, *quorum_vol*:

```
# vxassist -g quorum_dg make quorum_vol  
1G layout=mirrored \  
nmirrors=2
```

- 4 As root user, from the CVM master, create a filesystem with the volume, *quorum_vol*.

```
# mkfs -t vxfs /dev/vx/rdisk/quorum_dg/quorum_vol
```

- 5 On each system, create a directory, */quorum*:

```
# mkdir /quorum
```

- 6 On each system, mount */quorum*

```
# mount -t vxfs -o cluster /dev/vx/dsk/quorum_dg/quorum_vol  
/quorum
```

- 7 As root user, from any system, change permissions on */quorum*

```
# chown -R sybase:sybase /quorum
```

To create the disk group, volume and mount point for the datafiles

- 1 Initialize the disk.

For example:

```
# vxdisksetup -i Disk_5 format=cdsdisk  
# vxdisksetup -i Disk_6 format=cdsdisk
```

- 2 As root user, create a shared VxVM diskgroup for the datafiles.

```
# vxdg -s init dbdata_dg Disk_5 Disk_6
```

- 3 As root user, create a mirrored volume, *sybvol*:

```
# vxassist -g dbdata_dg make sybvol 1G layout=mirrored \  
nmirrors=2
```

- 4 As root user, create a filesystem with the volume, *sybvol*.

```
# mkfs -t vxfs /dev/vx/rdisk/dbdata_dg/sybvol
```

- 5 On each system, create a directory, */sybdata*:

```
# mkdir /sybdata
```

6 On each system, mount */sybdata*

```
# mount -t vxfs -o cluster /dev/vx/dsk/dbdata_dg/sybvol  
/sybdata
```

7 As root user, from any system, change permissions on */sybdata*

```
# chown -R sybase:sybase /sybdata
```

Creating the Sybase ASE CE cluster

For information on creating a Sybase ASE CE cluster, see the Sybase ASE CE product documentation. Follow the normal process.

Requirements for the Sybase ASE CE configuration:

- When you choose the private interconnect, set them on LLT links
- SF Sybase CE supports only one instance per node
- You can create a VCS cluster in local mode. Ignore the message "If you want to create a VCS cluster, specify "Shared" mode.", if it appears.
- Put the quorum device on the mount point created for the quorum device.
- Put the datafiles on the mount point created in for the datafiles.

Preparing to configure the Sybase instances under VCS control

Before putting the Sybase instances under VCS control, you may need to perform the following tasks:

- [Language settings for the Sybase agent](#)
- [Configuring Sybase for detail monitoring](#)
- [Encrypting passwords for Sybase](#)
- [About setting up detail monitoring for the agent for Sybase](#)

Language settings for the Sybase agent

For the VCS agent for Sybase to function with the desired locale, make sure that the Sybase installation has the correct localization files. For example, if the Sybase

server requires 'LANG=en_US.UTF-8' environment variable, verify that the localization files corresponding to language 'en_US.UTF-8' are installed with Sybase.

Also, edit the file `$VCS_HOME/bin/vcsenv` to contain the following:

```
LANG=en_US.UTF-8
export LANG

LC_CTYPE=en_US.UTF-8
export LC_CTYPE

LC_ALL=en_US.UTF-8
export LC_ALL
```

This change affects all the agents that are configured on the nodes.

Configuring Sybase for detail monitoring

This section describes the tasks to be performed to configure a Sybase server for detail monitoring.

See [“About setting up detail monitoring for the agent for Sybase”](#) on page 297.

Note: The steps that are described here are specific to the sample script, `SqlTest.pl`, provided with the agent. If you use a custom script for detail monitoring, you must configure the Sybase database accordingly.

Perform these steps only once in a Sybase cluster.

To configure Sybase for detail monitoring

- 1 Source the `SYBASE.sh` file or `SYBASE.csh` file (depending on the user shell) to set the `$SYBASE` and `$SYBASE_ASE` environment variables.

- 2 Start the Sybase server.

```
# startserver -f ./SYBASE/$SYBASE_ASE/install/RUN_server_name
```

- 3 Start the Sybase client on any cluster node.

```
# isql -Usa -SSYBASE_SERVER_NAME
```

Enter the administrator password when prompted to do so.

- 4 Connect to the master database.

```
# use master
# go
```

5 Create a Sybase user account.

```
# sp_addlogin user_name, password  
# go
```

The detail monitor script should use this account to make transactions on the database.

6 Create a database.

```
# create database database_name  
# go
```

The detail monitor script should make transactions on this database.

7 If required, restrict the size of the log file for the database.

```
# sp_dboption database_name, "trunc log on chkpt", true  
# go
```

8 Connect to the database that is created in step 6.

```
# use database_name  
# go
```

9 Associate the user created in step 5 with the database created in step 6.

```
# sp_adduser user_name  
# go
```

10 Change the user to the one created in step 5.

```
# setuser "user_name"  
# go
```

11 Create a table in the database.

```
# create table table_name (lastupd datetime)  
# go
```

The detail monitor script should make transactions on this table.

If you use the SqlTest.pl for detail monitoring, make sure you create a table with a lastupd field of type datetime.

- 12 Verify the configuration by adding an initial value to the table.

```
# insert into table_name (lastupd) values (getdate())  
# go
```

- 13 Exit the database.

```
# exit
```

Encrypting passwords for Sybase

VCS provides a utility *vcscrypt* to encrypt user passwords. Encrypt passwords before specifying them for Sybase and SybaseBk resource type definition.

The *vcscrypt* utility also allows you to encrypt the agent passwords using a security key. The security key supports AES (Advanced Encryption Standard) encryption which creates a secure password for the agent. See the *Symantec Cluster Server Administrator's Guide* for more information.

To encrypt passwords

- 1 From the path `$VCS_HOME/bin/`, run the *vcscrypt* utility.
- 2 Type the following command.

```
# vcscrypt -agent
```

The utility prompts you to enter the password twice. Enter the password and press Return.

```
Enter Password:  
Enter Again:
```

- 3 The utility encrypts the password and displays the encrypted password.
- 4 Enter this encrypted password as the value for the attribute.

Save the encrypted password for future reference.

About setting up detail monitoring for the agent for Sybase

The VCS agent for Sybase provides two levels of application monitoring: basic and detail. In basic monitoring, Sybase resource monitors the Sybase dataserver processes to verify that they are continuously active.

To activate detail monitoring, the `LevelTwoMonitorFreq` attribute must be set to a positive integer and `User`, `UPword`, `Db`, and `Table` attributes must not be empty ("").

The attribute `Monscript`, which contains the path of the detail monitor script, must also exist and must have execute permissions for the root.

Enabling detail monitoring for the agent for Sybase

Perform the following steps to enable detail monitoring on a database.

Note: All Sybase resources in the cluster gets modified when you enable detail monitoring for agents.

To enable detail monitoring

- 1 Make sure the Sybase server is configured for detail monitoring.
- 2 Make the VCS configuration writable.

```
# haconf -makerw
```

- 3 Enable detail monitoring for Sybase.

```
# hatype -modify Sybase LevelTwoMonitorFreq <value>
# hares -modify Sybase_resource User user_name
# hares -modify Sybase_resource UPword encrypted-password
# hares -modify Sybase_resource Db database_name
# hares -modify Sybase_resource Table table_name
# hares -modify Sybase_resource Monscript
"/opt/VRTSagents/ha/bin/Sybase/SqlTest.pl"
```

Note: To enable detail monitoring, the `LevelTwoMonitorFreq` attribute must be set to a positive value. You can also override the value of this attribute at the resource level.

- 4 Save the configuration.

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

Note: If detail monitoring is configured and the database is full, the SQL queries take considerable time to commit the results. In such a case, the monitor routine for the agent fails and attempts to fail over the service group. This issue is not encountered if detail monitoring is not configured.

Configuring a Sybase CE cluster under VCS control using the SF Sybase CE installer

A VCS service group is a collection of resources working together to provide application services to clients. A VCS service group typically includes multiple resources that are both hardware and software based. For example, a resource maybe a physical component such as a disk or network interface card, or a software component such as Sybase or a Web server, or a configuration component such as an IP address or mounted file system.

For an example configuration file:

The SF Sybase CE installer enables you to configure VCS service groups for putting a basic Sybase ASE CE cluster under VCS control. For examples of the VCS service group dependencies for SF Sybase CE see the following diagrams.

[Figure 11-1](#) displays the service group dependencies for an SF Sybase CE configuration on local disk group with VxFS.

Figure 11-1 Service group dependencies for an SF Sybase CE configuration on local disk group with VxFS

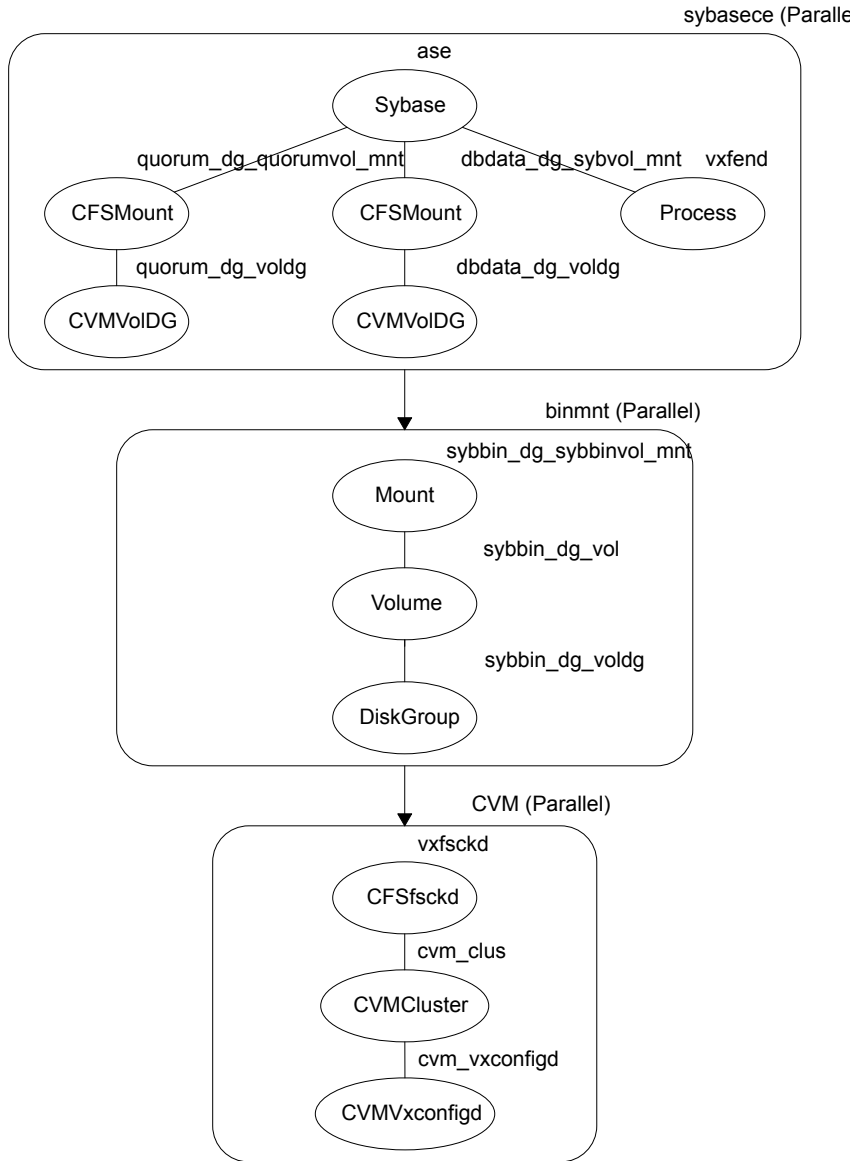
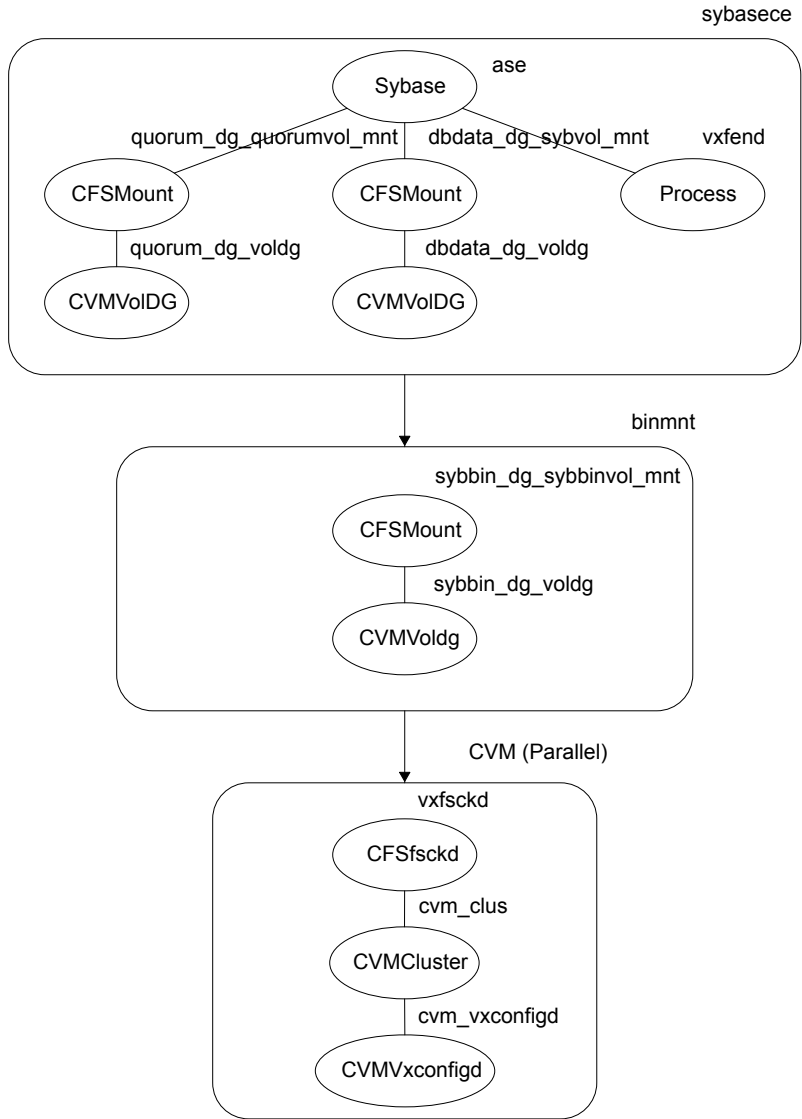


Figure 11-2 displays the service group dependencies for an SF Sybase CE configuration on shared disk group with CFS.

Figure 11-2 Service group dependencies for an SF Sybase CE configuration on shared disk group with CFS



Requirements for configuring the SF Sybase CE cluster under VCS control:

- Install SF Sybase CE.
- Configure SF Sybase CE.
- Configure I/O fencing in Sybase mode.
- Create Sybase user and group.
See Sybase documentation.
- Create a local or shared disk group, volume, and mount point for Sybase binary installation.
- Install the Sybase ASE CE software
- Create a shared disk group, volume and mount point for the Sybase ASE CE quorum device
- Create a shared disk group, volume and mount point for the Sybase ASE CE datafiles
- Create the Sybase ASE CE cluster

To put the Sybase ASE CE cluster and its resources under VCS control, the installer's configuration process will add the required resources to appropriate VCS service groups.

[Table 11-1](#) lists the required resources for configuring Sybase ASE CE under VCS control.

Table 11-1 Required resources for configuring Sybase ASE CE under VCS control

| Required resources | Example values | |
|---|---|--|
| Resources for the Sybase ASE CE binary installation: | Example values for shared mount point: | Example values for local mount point: |
| <ul style="list-style-type: none"> ■ Disk group ■ Mount point ■ Volume | <ul style="list-style-type: none"> ■ <i>sybbin_dg</i> ■ <i>/sybase</i> ■ <i>sybbin_vol</i> | <ul style="list-style-type: none"> ■ <i>sybbin_dg_voldg</i> ■ <i>/sybase</i> ■ <i>sybbin_dg_vol</i> |
| Resources for the Sybase ASE CE quorum device: | Example values for shared mount point: | |
| <ul style="list-style-type: none"> ■ Disk group ■ Mount point ■ Volume | <ul style="list-style-type: none"> ■ <i>quorum_dg</i> ■ <i>/quorum</i> ■ <i>quorum_vol</i> | |
| Resources for the Sybase ASE CE datafiles: | Example values for shared mount point: | |

Table 11-1 Required resources for configuring Sybase ASE CE under VCS control
(continued)

| Required resources | Example values |
|---|--|
| <ul style="list-style-type: none"> ■ Disk group ■ Mount point ■ Volume | <ul style="list-style-type: none"> ■ <i>dbdata_dg</i> ■ <i>/sybdata</i> ■ <i>sybvol</i> |
| Any other CFS disk group, mount point, and volume used for Sybase ASE CE resources that are required by the Sybase ASE CE cluster | As needed |
| The quorum device name | /quorum/quorum.dat |

Warning: You will not be able to proceed using the installer to configure the Sybase ASE CE cluster under VCS control without the items listed in [Table 11-1](#)

To configure VCS service groups for Sybase ASE CE

- 1 Log in to the installer if you are not currently logged in.
See [“Configuring the SF Sybase CE components using the script-based installer”](#) on page 210.
- 2 When prompted to select an option from the main menu, choose the option: **Configure Sybase ASE CE Instance in VCS.**
The installer will not be able to proceed any further unless you have the required resources available.
See [Table 11-1](#) on page 303.
- 3 To select the type of file system where Sybase ASE CE binaries reside, choose one of the options.
Symantec recommends CFS.
- 4 Configure the Sybase ASE CE binary installation resources under VCS control. These are the resources which were created while preparing to install Sybase ASE CE.
See [“Preparing for shared mount point on CFS for Sybase ASE CE binary installation”](#) on page 291. for shared mount point.
See [“Preparing for local mount point on VxFS for Sybase ASE CE binary installation”](#) on page 290. for local mount point.
To configure the Sybase resources under VCS control:

- To select a disk group used for Sybase ASE CE installation, choose one of the options.

Note: If you use Sybase ASE CE installation binaries on the local VxFS mount, you must specify the disk group for each node.

- To select the volume used for Sybase ASE CE installation, choose one of the options.
 - Enter the mount point for the selected volume.
- 5 The quorum device resources must be added into the resource group if it is under a different CFS than the Sybase database installation. These resources were created while preparing for a Sybase ASE CE cluster.

See [“Preparing to create a Sybase ASE CE cluster”](#) on page 292.

To configure the quorum device under VCS control:

- Enter **y** if the quorum device is under a different CFS than the Sybase database resources you have configured in the previous step, otherwise enter **n**.
 - If you entered **y**, select a disk group for the quorum device.
 - Select a volume for the quorum device.
 - Enter **y** if there is a CFS on the volume you selected, otherwise enter **n**. The quorum device can use either a volume which you have selected directly or a file under CFS created on the selected volume.
 - Enter the mount point for the volume.
- 6 If there are any other disk groups, volumes, or mount points used for the Sybase ASE CE cluster, such as other database files, for instance master, system, etc., which are using a different CFS, they must also be put under VCS control. To add other disk groups, volumes, and mount points to the resource group, enter **y** when prompted, otherwise enter **n**.
- 7 Verify the disk groups, volumes and mount points information when prompted.
- 8 To configure the Sybase ASE CE resources:
- Enter the Sybase instance on ASE1 and ASE2 when prompted.
 - Enter the Sybase UNIX user name.
 - Enter Sybase home directory, where the Sybase binaries reside.
 - Enter Sybase version.

- If required, enter the username and password for the Admin user. The default username is 'sa', password is".
- Enter the Sybase quorum device information.
During configuration of Sybase instance under VCS control, if the quorum device is on CFS and is not mounted, the following warning message appears on the installer screen:

```
Error: CPI WARNING V-9-0-0 The quorum file /quorum/quorum.dat
cannot be accessed now.
This may be due to a file system not being mounted.
```

This message may be safely ignored. The resource will be onlined and available when the service is completed.

- Verify the Sybase configuration information by entering **y**, otherwise enter **n**. For example:

```
Sybase configuration information verification:
```

```
Sybase Server on node01: ASE1
Sybase Server on node02: ASE2
Sybase UNIX user name: sybase
Sybase home directory where sybase binaries reside: /sybase
Sybase version: 15
Sybase sa: sa
Passwords are not displayed
Sybase quorum: /quorum/quorum.dat
```

Once you confirm the information is correct, the installer configures and onlines the VCS service groups for Sybase ASE CE. This completes the configuration of Sybase ASE CE under VCS control.

- Note the location of the configuration log files for future reference.

9 To verify the service groups have been created and are available online, enter:

```
# hagr -state
```

```
hagr -state
#Group      Attribute          System      Value
binmnt      State              system1     |ONLINE|
binmnt      State              system2     |ONLINE|
cvm         State              system1     |ONLINE|
cvm         State              system2     |ONLINE|
sybasece   State              system1     |ONLINE|
sybasece   State              system2     |ONLINE|
```

Automated installation using response files

This chapter includes the following topics:

- [About response files](#)
- [Performing an automated SF Sybase CE installation](#)
- [Performing an automated SF Sybase CE configuration](#)
- [Performing an automated I/O fencing configuration using response files](#)
- [Configuring a Sybase cluster under VCS control using a response file](#)

About response files

Use response files to standardize and automate installations on multiple clusters.

You can perform the following installation activities using a response file:

- Installing and configuring SF Sybase CE
- Uninstalling SF Sybase CE

Table 12-1 Options for obtaining a response file

| Option | Description |
|------------------------|---|
| Create a response file | Create a response file based on the sample response file. |

Table 12-1 Options for obtaining a response file (*continued*)

| Option | Description |
|--|--|
| Reuse or customize the response files generated by an installation | <p>The response file generated by the installer is located in the following directory:</p> <pre>/opt/VRTS/install/logs/installsfbasece<version>-\ installernumber/installsfbasece<version>-\ installernumber.response</pre> <p>Note: Response files are not created if the tasks terminated abruptly or if you entered q to quit the installation. To generate the response file when you plan to discontinue a task, use the Exit SF Sybase CE configuration option.</p> |

At the end of the SF Sybase CE installation, the following files are created:

- A log file that contains executed system commands and output.
- A summary file that contains the output of the installation scripts.
- Response files to be used with the `-responsefile` option of the installer.

Note: The SF Sybase CE response files also contain VCS variables used for the installation and configuration of VCS.

For the VCS variable definitions, see the *Symantec Cluster Server Installation Guide*.

Response file syntax

The Perl statement syntax that is included in the response file varies, depending on whether “Scalar” or “List” values are required by the variables.

For example,

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

or, in the case of an integer value:

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

or, in the case of a list:

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

Guidelines for creating the SF Sybase CE response file

This section provides guidelines for creating the SF Sybase CE response file. The response file variables discussed in this section are described in subsequent chapters.

1. Create a response file using one of the available options.
For various options on creating or obtaining an SF Sybase CE response file:
2. Set the following master values to 1 to enable SF Sybase CE installation and configuration.

Note: The master settings must be set to 1 to enable the installer to read dependent variable definitions. For example, if the value `$CFG{opt}{install}` is not set to 1, the other dependent installation values in the response file will be disregarded. This is true for any master setting.

The following is the list of master values that must be set for installing and configuring SF Sybase CE.

```
Installing SF Sybase CE  $CFG{opt}{install}=1;
                        $CFG{opt}{installallpkgs}=1;
```

```
Configuring SF Sybase  $CFG{opt}{configure}=1;
CE
```

3. Now, set the appropriate value in the dependent variable definitions for installing and configuring SF Sybase CE.

The set of minimum definitions for a successful installation and configuration is as follows:

```
$CFG{accepteula}=1;
$CFG{config_cfs}=1;
$CFG{lltoverudp}="0";
$CFG{opt}{configure}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{opt}{vxkeyless}=1;
$CFG{prod}="SFSYBASECE62";
$CFG{sfsybasece}{menu}=1;
$CFG{systems}=[ qw(sys1 sys2) ];
$CFG{vcs_allowcomms}=1;
```

```
$CFG{vcs_clusterid}=2455;  
$CFG{vcs_clustername}="clus1";  
$CFG{vcs_11tlink1}{sys1}="net1";  
$CFG{vcs_11tlink1}{sys2}="net1";  
$CFG{vcs_11tlink2}{sys1}="net2";  
$CFG{vcs_11tlink2}{sys2}="net2";  
$CFG{vcs_userenpw}=[ qw(gmnFmhMjnInnLvnHmk) ];  
$CFG{vcs_username}=[ qw(admin) ];  
$CFG{vcs_userpriv}=[ qw(Administrators) ];  
  
1;
```

You can add more variable definitions, as required.

Installation scenarios for response files

The chapters in this section cover the following installation scenarios using response files:

- Installing and configuring SF Sybase CE
- Configuring a SF Sybase CE instance in VCS
- Configuring I/O fencing for SF Sybase CE with a response file

Performing an automated SF Sybase CE installation

Installing SF Sybase CE using response files

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

```
# ./installmr -base_path /tmp/sfha6.2 -makeresponsefile
```

See [“About the script-based installer”](#) on page 204.

To install SF Sybase CE using response files

- 1 Make sure the systems where you want to install Sybase CE meet the installation requirements.
See [“Important preinstallation information for SF Sybase CE”](#) on page 180.
See the chapter *System Requirements*.
- 2 Make sure that the preinstallation tasks are completed.
See the chapter *Preparing to install SF Sybase CE*.
See the chapter *Preparing to install SF Sybase CE* in this document.
- 3 Create or edit a response file, as appropriate.
See [“Response file variables to install SF Sybase CE”](#) on page 312.

Note: You must replace the host names in the response file with the names of the new systems in the cluster.

For guidelines on creating a response file:

For a sample response file:

See [“Sample response files for configuring SF Sybase CE”](#) on page 326.

- 4 Edit the values of the response file variables as necessary.
See [“Response file variables to install SF Sybase CE”](#) on page 312.
- 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:

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

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

- 7 Complete the SF Sybase CE post-installation tasks.
For instructions, see the chapter *Performing post-installation and configuration tasks* in this document.

Response file variables to install SF Sybase CE

[Table 12-2](#) lists the response file variables that you can define to install SF Sybase CE.

Table 12-2 Response file variables for installing SF Sybase CE

| Variable | Description |
|--|--|
| CFG{opt}{install} | Installs SF Sybase CE RPMs. Configuration can be performed at a later time using the <code>-configure</code> option. List or scalar: scalar Optional or required: optional |
| CFG{opt}{installallpkgs} or CFG{opt}{installrecpkgs} or CFG{opt}{installminpkgs} | Instructs the installer to install SF Sybase CE RPMs based on the variable that has the value set to 1: <ul style="list-style-type: none"> ■ <code>installallpkgs</code>: Installs all RPMs ■ <code>installrecpkgs</code>: Installs recommended RPMs ■ <code>installminpkgs</code>: Installs minimum RPMs <p>Note: Set only one of these variable values to 1. In addition to setting the value of one of these variables, you must set the variable <code>CFG{opt}{install}</code> to 1.</p> List or scalar: scalar Optional or required: required |
| CFG{accepteula} | Specifies whether you agree with the EULA.pdf file on the media. List or scalar: scalar Optional or required: required |
| CFG{opt}{vxkeyless} | Installs the product with keyless license. List or scalar: scalar Optional or required: optional |
| CFG{opt}{license} | Installs the product with permanent license. List or scalar: scalar Optional or required: optional |
| CFG{keys}{hostname} | List of keys to be registered on the system if the variable <code>CFG{opt}{vxkeyless}</code> is set to 0 or if the variable <code>CFG{opt}{licence}</code> is set to 1. List or scalar: scalar Optional or required: optional |

Table 12-2 Response file variables for installing SF Sybase CE (*continued*)

| Variable | Description |
|----------------------|---|
| CFG{systems} | List of systems on which the product is to be installed or uninstalled. List or scalar: list Optional or required: required |
| CFG{prod} | Defines the product to be installed or uninstalled. List or scalar: scalar Optional or required: required |
| CFG{opt}{keyfile} | Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional |
| CFG{opt}{tmppath} | Defines the location where a working directory is created to store temporary files and the RPMs that are needed during the install. The default location is /var/tmp. List or scalar: scalar Optional or required: optional |
| CFG{opt}{updatekeys} | Updates the keyless license to the current version. List or scalar: scalar Optional or required: optional |
| CFG{opt}{rsh} | Defines that <i>rsh</i> must be used instead of <i>ssh</i> as the communication method between systems. List or scalar: scalar Optional or required: optional |
| CFG{opt}{logpath} | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. List or scalar: scalar Optional or required: optional |
| CFG{opt}{prodmode} | List of modes for product List or scalar: list Optional or required: optional |

Table 12-2 Response file variables for installing SF Sybase CE (*continued*)

| Variable | Description |
|---------------------|--|
| CFG{opt}{base_path} | <p>Defines the path of a base level release to be integrated with a maintenance level release for the two releases to be simultaneously.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p> |

Sample response file for installing SF Sybase CE

The following sample response file only installs SF Sybase CE on two nodes, node01 and node02

```
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installrecpkgs}=1;
$CFG{opt}{vr}=1;
$CFG{opt}{vxkeyless}=1;
$CFG{prod}="SFSYBASECE62";
$CFG{systems}=[ qw(node01 node02) ];
1;
```

Performing an automated SF Sybase CE configuration

Configuring SF Sybase CE using response files

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

```
# ./installsfybasece<version> -makeresponsefile -configure
```

To configure SF Sybase CE using response files

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

- 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.

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

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

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

- 5 Configure I/O fencing.

Note: Before you configure I/O fencing, make sure that you complete the required pre-configuration tasks.

For instructions on configuring I/O fencing using a response file, see the chapter *Configuring I/O fencing using a response file* in this document.

- 6 Complete the SF Sybase CE post-installation tasks.

For instructions, see the chapter *Performing post-installation and configuration tasks* in this document.

Response file variables to configure SF Sybase CE

[Table 12-3](#) lists the response file variables that you can define to configure SF Sybase CE.

Table 12-3 Response file variables specific to configuring SF Sybase CE

| Variable | List or Scalar | Description |
|---------------------|----------------|--|
| CFG{config_cfs} | Scalar | Performs the Cluster File System configuration for SF Sybase CE. (Required) Set the value to 1 to configure Cluster File System for SF Sybase CE. |
| CFG{opt}{configure} | Scalar | Performs the configuration if the RPMs are already installed. (Required) Set the value to 1 to configure SF Sybase CE. |
| CFG{config_cfs} | Scalar | Performs the Cluster File System configuration for SF Sybase CE. Set the variable to 1 to configure the SF Sybase CE components. (Required) Note: You must set the <i>CFG{opt}{configure}</i> variable to 1. |
| CFG{accepteula} | Scalar | Specifies whether you agree with EULA.pdf on the media. (Required) |
| CFG{systems} | List | List of systems on which the product is to be configured. (Required) |
| CFG{prod} | Scalar | Defines the product to be configured. The value is SFRAC62 for SFRAC. The value is SFSYBASECE62 for SFSYBASECE The value is SFCFSHA62 for SFCFSHA The value is SFHA62 for SFHA (Required) |

Table 12-3 Response file variables specific to configuring SF Sybase CE
(continued)

| Variable | List or Scalar | Description |
|----------------------|----------------|--|
| CFG{opt}{keyfile} | Scalar | Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional) |
| CFG{secusrgrps} | List | Defines the user groups which get read access to the cluster. (Optional) |
| CFG {rootsecusrgrps} | Scalar | Defines the read access to the cluster only for root and other users or usergroups which are granted explicit privileges on VCS objects. (Optional) |
| CFG{opt}{rsh} | Scalar | Defines that <i>rsh</i> must be used instead of ssh as the communication method between systems. (Optional) |
| CFG{opt}{logpath} | Scalar | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. Note: The installer copies the response files and summary files also to the specified <i>logpath</i> location. (Optional) |
| CFG{uploadlogs} | Scalar | Defines a Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec website. The value 0 indicates that the installation logs are not uploaded to the Symantec website. (Optional) |

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (csgnic, csgvip, and csgnetmask) must be defined if any are defined. The same is true for the SMTP notification (smtpserver, smtprecp, and smtpsev), the SNMP trap notification (snmpport, snmpcons, and snmpcsev), and the Global Cluster Option (gconic, gcovip, and gconetmask).

[Table 12-4](#) lists the response file variables that specify the required information to configure a basic SF Sybase CE cluster.

Table 12-4 Response file variables specific to configuring a basic SF Sybase CE cluster

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

[Table 12-5](#) lists the response file variables that specify the required information to configure LLT over Ethernet.

Table 12-5 Response file variables specific to configuring private LLT over Ethernet

| Variable | List or Scalar | Description |
|---------------------------------------|----------------|--|
| CFG{vcs_lltlink#} {"system"} | Scalar | Defines the NIC to be used for a private heartbeat link on each system. At least two LLT links are required per system (lltlink1 and lltlink2). You can configure up to four LLT links. You must enclose the system name within double quotes. (Required) |
| CFG{vcs_lltlinklowpri#} {"system"} | Scalar | Defines a low priority heartbeat link. Typically, lltlinklowpri is used on a public network link to provide an additional layer of communication. If you use different media speed for the private NICs, you can configure the NICs with lesser speed as low-priority links to enhance LLT performance. For example, lltlinklowpri1, lltlinklowpri2, and so on. You must enclose the system name within double quotes. (Optional) |

[Table 12-6](#) lists the response file variables that specify the required information to configure LLT over UDP.

Table 12-6 Response file variables specific to configuring LLT over UDP

| Variable | List or Scalar | Description |
|------------------|----------------|---|
| CFG{lltverudp}=1 | Scalar | Indicates whether to configure heartbeat link using LLT over UDP. (Required) |

Table 12-6 Response file variables specific to configuring LLT over UDP
(continued)

| Variable | List or Scalar | Description |
|---|----------------|--|
| CFG{vcs_udplink<n>_address} {<sys1>} | Scalar | Stores the IP address (IPv4 or IPv6) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required) |
| CFG {vcs_udplinklowpri<n>_address} {<sys1>} | Scalar | Stores the IP address (IPv4 or IPv6) that the low priority heartbeat link uses on node1. You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required) |
| CFG{vcs_udplink<n>_port} {<sys1>} | Scalar | Stores the UDP port (16-bit integer value) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required) |
| CFG{vcs_udplinklowpri<n>_port} {<sys1>} | Scalar | Stores the UDP port (16-bit integer value) that the low priority heartbeat link uses on node1. You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required) |

Table 12-6 Response file variables specific to configuring LLT over UDP
(continued)

| Variable | List or Scalar | Description |
|---|----------------|--|
| CFG{vcs_udplink<n>_netmask} {<sys1>} | Scalar | Stores the netmask (prefix for IPv6) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required) |
| CFG {vcs_udplinklowpri<n>_netmask} {<sys1>} | Scalar | Stores the netmask (prefix for IPv6) that the low priority heartbeat link uses on node1. You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links. (Required) |

[Table 12-7](#) lists the response file variables that specify the required information to configure virtual IP for Symantec Storage Foundation HA cluster.

Table 12-7 Response file variables specific to configuring virtual IP for SF Sybase CE cluster

| Variable | List or Scalar | Description |
|-----------------------------|----------------|--|
| CFG{vcs_csgnic} {system} | Scalar | Defines the NIC device to use on a system. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional) |
| CFG{vcs_csgvip} | Scalar | Defines the virtual IP address for the cluster. (Optional) |
| CFG{vcs_csgnetmask} | Scalar | Defines the Netmask of the virtual IP address for the cluster. (Optional) |

Table 12-8 lists the response file variables that specify the required information to configure the SF Sybase CE cluster in secure mode.

Table 12-8 Response file variables specific to configuring SF Sybase CE cluster in secure mode

| Variable | List or Scalar | Description |
|----------------------------|----------------|---|
| CFG{vcs_eat_security} | Scalar | Specifies if the cluster is in secure enabled mode or not. |
| CFG{opt}{securityonnode} | Scalar | Specifies that the securityonnode option is being used. |
| CFG{securityonnode_menu} | Scalar | Specifies the menu option to choose to configure the secure cluster one at a time. <ul style="list-style-type: none"> ■ 1—Configure the first node ■ 2—Configure the other node |
| CFG{secusrgrps} | List | Defines the user groups which get read access to the cluster. List or scalar: list Optional or required: optional |
| CFG{rootsecusrgrps} | Scalar | Defines the read access to the cluster only for root and other users or user groups which are granted explicit privileges in VCS objects. (Optional) |
| CFG{security_conf_dir} | Scalar | Specifies the directory where the configuration files are placed. |
| CFG{opt}{security} | Scalar | Specifies that the security option is being used. |
| CFG{vcs_eat_security_fips} | Scalar | Specifies that the enabled security is FIPS compliant. |

Table 12-9 lists the response file variables that specify the required information to configure VCS users.

Table 12-9 Response file variables specific to configuring VCS users

| Variable | List or Scalar | Description |
|-------------------|----------------|--|
| CFG{vcs_userenpw} | List | List of encoded passwords for VCS users The value in the list can be "Administrators Operators Guests" Note: The order of the values for the vcs_userenpw list must match the order of the values in the vcs_username list. (Optional) |
| CFG{vcs_username} | List | List of names of VCS users (Optional) |
| CFG{vcs_userpriv} | List | List of privileges for VCS users Note: The order of the values for the vcs_userpriv list must match the order of the values in the vcs_username list. (Optional) |

[Table 12-10](#) lists the response file variables that specify the required information to configure VCS notifications using SMTP.

Table 12-10 Response file variables specific to configuring VCS notifications using SMTP

| Variable | List or Scalar | Description |
|---------------------|----------------|---|
| CFG{vcs_smtpserver} | Scalar | Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for web notification. (Optional) |
| CFG{vcs_smtprecip} | List | List of full email addresses (example: user@symantecexample.com) of SMTP recipients. (Optional) |

Table 12-10 Response file variables specific to configuring VCS notifications using SMTP (*continued*)

| Variable | List or Scalar | Description |
|------------------|----------------|--|
| CFG{vcs_smtpsev} | List | Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SMTP recipients are to receive. Note that the ordering of severity levels must match that of the addresses of SMTP recipients. (Optional) |

[Table 12-11](#) lists the response file variables that specify the required information to configure VCS notifications using SNMP.

Table 12-11 Response file variables specific to configuring VCS notifications using SNMP

| Variable | List or Scalar | Description |
|-------------------|----------------|---|
| CFG{vcs_snmpport} | Scalar | Defines the SNMP trap daemon port (default=162). (Optional) |
| CFG{vcs_snmpcons} | List | List of SNMP console system names (Optional) |
| CFG{vcs_snmpsev} | List | Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names. (Optional) |

[Table 12-12](#) lists the response file variables that specify the required information to configure SF Sybase CE global clusters.

Table 12-12 Response file variables specific to configuring SF Sybase CE global clusters

| Variable | List or Scalar | Description |
|-----------------------------|----------------|---|
| CFG{vcs_gconic} {system} | Scalar | Defines the NIC for the Virtual IP that the Global Cluster Option uses. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional) |
| CFG{vcs_gcovip} | Scalar | Defines the virtual IP address to that the Global Cluster Option uses. (Optional) |
| CFG{vcs_gconetmask} | Scalar | Defines the Netmask of the virtual IP address that the Global Cluster Option uses. (Optional) |

Sample response files for configuring SF Sybase CE

The following sample response file installs and configures SF Sybase CE on two nodes, node01 and node02.

```
our %CFG;

$CFG{accepteula}=1;
$CFG{config_cfs}=1;
$CFG{fencingenabled}=0;
$CFG{lltoverudp}=0;
$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{opt}{vr}=1;
$CFG{opt}{vxkeyless}=1;
$CFG{prod}="SFSYBASECE62";
$CFG{sfsybasece}{menu}=1;
$CFG{systems}=[ qw(node01 node02) ];
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=24731;
$CFG{vcs_clustername}="clus1";
```

```
$CFG{vcs_lltlink1}{node01}="net1";  
$CFG{vcs_lltlink1}{node02}="net1";  
$CFG{vcs_lltlink2}{node01}="net2";  
$CFG{vcs_lltlink2}{node02}="net2";  
$CFG{vcs_userenpw}=[ qw(JqrJqlQnrMrrPzrLqo) ];  
$CFG{vcs_username}=[ qw(admin) ];  
$CFG{vcs_userpriv}=[ qw(Administrators) ];
```

```
1;
```

The following sample response file only configures CFS on two nodes, node01 and node02.

```
our %CFG;  
  
$CFG{config_cfs}=1;  
$CFG{fencingenabled}=0;  
$CFG{lltoverudp}=0;  
$CFG{opt}{configure}=1;  
$CFG{prod}="SFSYBASECE62";  
$CFG{sfsybasece}{menu}=1;  
$CFG{systems}=[ qw(node01 node02) ];  
$CFG{vcs_allowcomms}=1;  
$CFG{vcs_clusterid}=60037;  
$CFG{vcs_clustername}="clus1";  
$CFG{vcs_lltlink1}{node01}="net1";  
$CFG{vcs_lltlink1}{node02}="net1";  
$CFG{vcs_lltlink2}{node01}="net2";  
$CFG{vcs_lltlink2}{node02}="net2";  
$CFG{vcs_userenpw}=[ qw(bMNfMHmJNiNNlVNhMK) ];  
$CFG{vcs_username}=[ qw(admin) ];  
$CFG{vcs_userpriv}=[ qw(Administrators) ];
```

```
1;
```

Performing an automated I/O fencing configuration using response files

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 SF Sybase CE.

To configure I/O fencing using response files

- 1 Make sure that SF Sybase CE is configured.
- 2 As SF Sybase CE only supports disk based I/O fencing, make sure you have completed the preparatory tasks.

Make sure you have completed the preparatory tasks.

See “[About planning to configure I/O fencing](#)” on page 188.

- 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 331.

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

See “[Response file variables to configure disk-based I/O fencing](#)” on page 328.

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

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

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

See “[About the script-based installer](#)” on page 204.

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

[Table 12-13](#) lists the response file variables that specify the required information to configure disk-based I/O fencing for SF Sybase CE.

Table 12-13 Response file variables specific to configuring disk-based I/O fencing

| Variable | List or Scalar | Description |
|-------------------|----------------|---|
| CFG{opt}{fencing} | Scalar | Performs the I/O fencing configuration. (Required) |

Table 12-13 Response file variables specific to configuring disk-based I/O fencing
(continued)

| Variable | List or Scalar | Description |
|--------------------------|----------------|---|
| CFG{fencing_option} | Scalar | <p>Specifies the I/O fencing configuration mode.</p> <ul style="list-style-type: none"> ■ 2—Sybase Mode fencing ■ 5—Replace/Add/Remove coordination points ■ 6—Refresh keys/registrations on the existing coordination points <p>(Required)</p> |
| CFG{fencing_dgname} | Scalar | <p>Specifies the disk group for I/O fencing.</p> <p>(Optional)</p> <p>Note: You must define the <code>fencing_dgname</code> variable to use an existing disk group. If you want to create a new disk group, you must use both the <code>fencing_dgname</code> variable and the <code>fencing_newdg_disks</code> variable.</p> |
| CFG{fencing_newdg_disks} | List | <p>Specifies the disks to use to create a new disk group for I/O fencing.</p> <p>(Optional)</p> <p>Note: You must define the <code>fencing_dgname</code> variable to use an existing disk group. If you want to create a new disk group, you must use both the <code>fencing_dgname</code> variable and the <code>fencing_newdg_disks</code> variable.</p> |

Table 12-13 Response file variables specific to configuring disk-based I/O fencing
(continued)

| Variable | List or Scalar | Description |
|-----------------------------------|----------------|--|
| CFG{fencing_cpagent_monitor_freq} | Scalar | <p>Specifies the frequency at which the Coordination Point Agent monitors for any changes to the Coordinator Disk Group constitution.</p> <p>Note: Coordination Point Agent can also monitor changes to the Coordinator Disk Group constitution such as a disk being accidentally deleted from the Coordinator Disk Group. The frequency of this detailed monitoring can be tuned with the LevelTwoMonitorFreq attribute. For example, if you set this attribute to 5, the agent will monitor the Coordinator Disk Group constitution every five monitor cycles. If LevelTwoMonitorFreq attribute is not set, the agent will not monitor any changes to the Coordinator Disk Group. 0 means not to monitor the Coordinator Disk Group constitution.</p> |
| CFG {fencing_config_cpagent} | Scalar | <p>Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not.</p> <p>Enter "0" if you do not want to configure the Coordination Point agent using the installer.</p> <p>Enter "1" if you want to use the installer to configure the Coordination Point agent.</p> |
| CFG {fencing_cpagentgrp} | Scalar | <p>Name of the service group which will have the Coordination Point agent resource as part of it.</p> <p>Note: This field is obsolete if the fencing_config_cpagent field is given a value of '0'.</p> |

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 328.

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

$CFG{fencing_config_cpagent}=1;
$CFG{fencing_cpagent_monitor_freq}=5;
$CFG{fencing_cpagentgrp}="vxfen";
$CFG{fencing_dgname}="fencingdg1";
$CFG{fencing_newdg_disks}=[ qw(emc_clariion0_155
    emc_clariion0_162 emc_clariion0_163) ];
$CFG{fencing_option}=2;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{fencing_scsi3_disk_policy}="dmp";

$CFG{prod}="SFSYBASECE62";

$CFG{systems}=[ qw(node01 node02) ];
$CFG{vcs_clusterid}=32283;
$CFG{vcs_clustername}="clus1";
1;

#
# Configuration Values:
#
our %CFG;

$CFG{fencing_config_cpagent}="0";
$CFG{fencing_dgname}="fendg";
$CFG{fencing_newdg_disks}=[ qw(emc_clariion0_236
    emc_clariion0_237 emc_clariion0_238) ];
$CFG{fencing_option}=2;
$CFG{fencing_scsi3_disk_policy}="dmp";
$CFG{opt}{configure}=1;
$CFG{prod}="SFSYBASECE62";
$CFG{sfsybasece}{menu}=2;
$CFG{systems}=[ qw(sys1 sys2) ];
```

```
$CFG{vcs_clusterid}=8950;
$CFG{vcs_clustername}="clus1";

1;
```

Configuring a Sybase cluster under VCS control using a response file

Configuring a Sybase cluster under VCS control with a response file

Observe the following prerequisites prior to configuring a Sybase cluster under VCS with a response file:

- SF Sybase CE must be installed and configured on the system.
- Sybase must be installed.
- The Sybase cluster must already be created.

To configure a Sybase cluster under VCS using a response file

- ◆ Use the configuration response file to configure the product:

```
# installsfbase62 -responsefile /opt/VRTS/install/logs/\
installsf-installernumber/installsfbase-installer/\
number.response
```

The following sample response file configures SF Sybase CE under VCS control.

```
our %CFG;

$CFG{opt}{configure}=1;
$CFG{prod}="SFSYBASECE62";
$CFG{sfsybasece}{ase_home}="/sybase_home";
$CFG{sfsybasece}{ase_owner}="sybase";
$CFG{sfsybasece}{ase_quorum}="/qrmnt/newqrm1";
$CFG{sfsybasece}{ase_sa}="sa";
$CFG{sfsybasece}{ase_server}{vcslx003}{SERVER}="inst1";
$CFG{sfsybasece}{ase_server}{vcslx004}{SERVER}="inst2";
$CFG{sfsybasece}{ase_server}{vcslx005}{SERVER}="inst3";
$CFG{sfsybasece}{ase_server}{vcslx006}{SERVER}="inst4";
$CFG{sfsybasece}{ase_version}=15;
$CFG{sfsybasece}{menu}=3;
$CFG{sfsybasece}{storage_resource}{qrm304}{vol1}{mount}="/qrmnt";
```

```

$CFG{sfsybasece}{storage_resource}{qrmdg304}{vol1}{usage}="quorum device";
$CFG{sfsybasece}{storage_resource}{sybdatadg304}{vol1}{mount}="/datamnt";
$CFG{sfsybasece}{storage_resource}{sybdatadg304}{vol1}{usage}="database
devices";
$CFG{sfsybasece}{storage_resource}{sybhomedg304}{vol1}{mount}=
"/sybase_home";
$CFG{sfsybasece}{storage_resource}{sybhomedg304}{vol1}{usage}="sybase
installation";
$CFG{sybase_location}=1;
$CFG{systems}=[ qw(vcslx003 vcslx004 vcslx005 vcslx006) ];

1;

```

Response file variables to configure SF Sybase CE in VCS

[Table 12-14](#) lists the response file variables that you can define to configure SF Sybase CE in VCS.

Table 12-14 Response file variables specific to configuring SF Sybase CE in VCS

| Variable | List or Scalar | Description |
|---|----------------|---|
| CFG{sfsybasece}{ase_home} | Scalar | Defines the SF Sybase CE home directory. |
| CFG{sfsybasece}{ase_owner} | Scalar | Defines the SF Sybase CE owner name. |
| CFG{sfsybasece}{ase_quorum} | Scalar | Defines the SF Sybase CE quorum device. |
| CFG{sfsybasece}{ase_sa} | Scalar | Defines the SF Sybase CE administrator name. |
| CFG{sfsybasece}{ase_version} | Scalar | Defines the SF Sybase CE version. |
| CFG{sfsybasece}{menu}=3 | Scalar | Option for configuring SF Sybase CE under VCS. |
| CFG{sfsybasece}{storage_resource}{<diskgroupname>}{<volumename>}{usage} | Scalar | Lists the SF Sybase CE database devices that reside on the <diskgroupname> diskgroup and the <volumename> volume. |

Table 12-14 Response file variables specific to configuring SF Sybase CE in VCS
(continued)

| Variable | List or Scalar | Description |
|--|----------------|--|
| CFG{sfsybasece}{storage_resource} {master_dontuse}{mastervol} {usage} | Scalar | Lists the SF Sybase CE database devices that reside on the master_dontuse diskgroup and the mastervol volume. |
| CFG{sfsybasece}{storage_resource} {proc_dontuse}{proc01vol} {mount} | Scalar | Specifies the mount point for the proc_dontuse database device. |
| CFG{sfsybasece}{storage_resource} {proc_dontuse}{proc01vol} {usage} | Scalar | Lists the SF Sybase CE database devices that reside on the database_dontuse diskgroup and the database01vol volume. |
| CFG{sfsybasece}{storage_resource} {quorum_dontuse}{quorum_vol} {usage} | Scalar | Lists the SF Sybase CE quorum devices that reside on the quorum_dontuse diskgroup and the quorum_vol volume. |
| CFG{sfsybasece}{storage_resource} {sybase1_dontuse}{sybasevol} {mount}="/opt/sybase" | Scalar | Specifies the SF Sybase CE installation location under /opt/sybase. |
| CFG{sfsybasece}{storage_resource} {sybase1_dontuse}{sybasevol} {usage}="sybase installation" | Scalar | Specifies the SF Sybase CE installation location that resides on the sybase1_dontuse diskgroup and the sybasevol volume. |
| CFG{sybase_location} | Scalar | Specifies the SF Sybase CE location type. <ul style="list-style-type: none"> ■ 1—Location on CFS ■ 2—Location on a local VxFS file system. |

Adding and removing nodes

This chapter includes the following topics:

- [Adding a node to SF Sybase CE clusters](#)
- [Removing a node from SF Sybase CE clusters](#)

Adding a node to SF Sybase CE clusters

About adding a node to a cluster

After you install SF Sybase CE and create a cluster, you can add and remove nodes from the cluster. You can create clusters of up to 4 nodes.

You can add a node:

- Using the product installer
- Manually

The following table provides a summary of the tasks required to add a node to an existing SF Sybase CE cluster.

Table 13-1 Tasks for adding a node to a cluster

| Step | Description |
|---|--|
| Complete the prerequisites and preparatory tasks before adding a node to the cluster. | See “Before adding a node to a cluster” on page 336. |
| Add a new node to the cluster. | See “Adding the node to a cluster manually” on page 338. |
| Complete the configuration of the new node after adding it to the cluster. | |

Table 13-1 Tasks for adding a node to a cluster (*continued*)

| Step | Description |
|---|---|
| Prepare the new node for installing Sybase. | See “Adding the new instance to the Sybase ASE CE cluster” on page 349. |
| Add the node to Sybase. | See “Adding the new instance to the Sybase ASE CE cluster” on page 349. |

The example procedures describe how to add a node to an existing cluster with two nodes.

Before adding a node to a cluster

Before preparing to add the node to an existing SF Sybase CE cluster, perform the required preparations.

- Verify hardware and software requirements are met.
- Set up the hardware.
- Prepare the new node.

To verify hardware and software requirements are met

- 1 Review hardware and software requirements for SF Sybase CE.
 See [“Important preinstallation information for SF Sybase CE”](#) on page 180.
- 2 Verify the new system has the same identical operating system versions and patch levels as that of the existing cluster
- 3 Verify the existing cluster is an SF Sybase CE cluster and that SF Sybase CE is running on the cluster.
- 4 If the cluster is upgraded from the previous version, you must check the cluster protocol version to make sure it has the same version as the node to be added. If there is a protocol mismatch, the node is unable to join the existing cluster.

Check the cluster protocol version using:

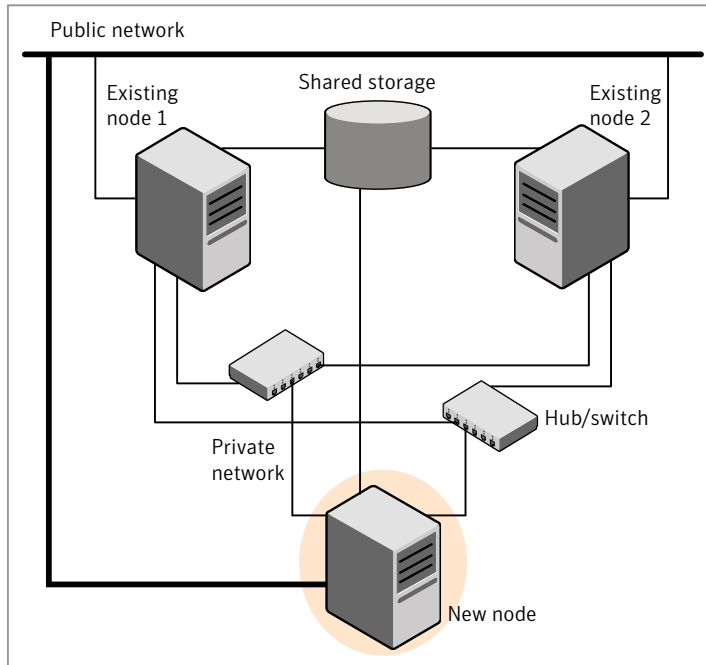
```
# vxdctl protocolversion
Cluster running at protocol 140
```

- 5 If the cluster protocol on the master node is below 130, upgrade it using:

```
# vxdctl upgrade [version]
```


Before you configure a new system on an existing cluster, you must physically add the system to the cluster as illustrated in [Figure 13-1](#).

Figure 13-1 Adding a node to a two-node cluster using two switches



To set up the hardware

1 Connect the SF Sybase CE private Ethernet controllers.

Perform the following tasks as necessary:

- When you add nodes to a cluster, use independent switches or hubs for the private network connections. You can only use crossover cables for a two-node cluster, so you might have to swap out the cable for a switch or hub.

When you add nodes to a cluster, use independent switches or hubs for the private network connections.

- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

[Figure 13-1](#) illustrates a new node being added to an existing two-node cluster using two independent hubs.

2 Make sure that you meet the following requirements:

- The node must be connected to the same shared storage devices as the existing nodes.
- The node must have private network connections to two independent switches for the cluster.
For more information, see the *Symantec Cluster Server Installation Guide*.
- The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster.

Complete the following preparatory steps on the new node before you add it to an existing SF Sybase CE cluster.

To prepare the new node

- 1 Navigate to the folder that contains the installmr program. Verify that the new node meets installation requirements. Verify that the new node meets installation requirements.

```
# ./installmr -precheck
```

You can also use the web-based installer for the precheck.

- 2 Install SF Sybase CE RPMs only without configuration on the new system. Make sure all the VRTS RPMs available on the existing nodes are also available on the new node.

```
# ./installmr -base_path /tmp/sfha6.2
```

Do not configure SF Sybase CE when prompted.

```
Would you like to configure SF Sybase CE on sys5? [y,n,q]? n
```

- 3 Restart the node if the installer asks for a reboot.

Adding the node to a cluster manually

Perform this procedure after you install SF Sybase CE only if you plan to add the node to the cluster manually.

Table 13-2 Procedures for adding a node to a cluster manually

| Step | Description |
|--|---|
| Start the Veritas Volume Manager (VxVM) on the new node. | See “Starting Veritas Volume Manager (VxVM) on the new node” on page 339. |

Table 13-2 Procedures for adding a node to a cluster manually (*continued*)

| Step | Description |
|--|---|
| Configure the cluster processes on the new node. | See “Configuring cluster processes on the new node” on page 339. |
| Configure fencing for the new node to match the fencing configuration on the existing cluster. | See “Starting fencing on the new node” on page 343. |
| Start VCS. | See “To start VCS on the new node” on page 346. |
| Configure CVM and CFS. | See “Configuring Cluster Volume Manager (CVM) and Cluster File System (CFS) on the new node” on page 344. |
| If the ClusterService group is configured on the existing cluster, add the node to the group. | See “Configuring the ClusterService group for the new node” on page 346. |

Starting Veritas Volume Manager (VxVM) on the new node

Veritas Volume Manager (VxVM) uses license keys to control access. As you run the `vxinstall` utility, answer **n** to prompts about licensing. You installed the appropriate license when you ran the `installmr` program.

To start VxVM on the new node

- 1 To start VxVM on the new node, use the `vxinstall` utility:

```
# vxinstall
```

- 2 Enter **n** when prompted to set up a system wide disk group for the system.

The installation completes.

- 3 Verify that the daemons are up and running. Enter the command:

```
# vxdisk list
```

Make sure the output displays the shared disks without errors.

Configuring cluster processes on the new node

Perform the steps in the following procedure to configure cluster processes on the new node.

Setting up the node to run in secure mode

You must follow this procedure only if you are adding a node to a cluster that is running in secure mode. If you are adding a node to a cluster that is not running in a secure mode, proceed with configuring LLT and GAB.

[Table 13-3](#) uses the following information for the following command examples.

Table 13-3 The command examples definitions

| Name | Fully-qualified host name (FQHN) | Function |
|------|----------------------------------|--|
| sys5 | sys5.nodes.example.com | The new node that you are adding to the cluster. |

Configuring the authentication broker on node sys5

To configure the authentication broker on node sys5

- 1 Extract the embedded authentication files and copy them to temporary directory:

```
# mkdir -p /var/VRTSvcs/vcsauth/bkup  
  
# cd /tmp; gunzip -c /opt/VRTSvcs/bin/VxAT.tar.gz | tar xvf -
```

- 2 Edit the setup file manually:

```
# cat /etc/vx/.uuids/clusuuid 2>&1
```

The output is a string denoting the UUID. This UUID (without { and }) is used as the ClusterName for the setup file.

```
{UUID}
```

```
# cat /tmp/eat_setup 2>&1
```

The file content must resemble the following example:

```
AcceptorMode=IP_ONLY  
  
BrokerExeName=vcsauthserver  
  
ClusterName=UUID  
  
DataDir=/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER  
  
DestDir=/opt/VRTSvcs/bin/vcsauth/vcsauthserver  
  
FipsMode=0  
  
IPPort=14149  
  
RootBrokerName=vcsroot_uuid  
  
SetToRBPlusABorNot=0  
  
SetupPDRs=1  
  
SourceDir=/tmp/VxAT/version
```

3 Set up the embedded authentication file:

```
# cd /tmp/VxAT/version/bin/edition_number; \  
./broker_setup.sh/tmp/eat_setup  
  
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssregctl -s -f \  
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER/root/.VRTSat/profile \  
/VRTSatlocal.conf -b 'Security\Authentication \  
\Authentication Broker' -k UpdatedDebugLogFileName \  
-v /var/VRTSvcs/log/vcsauthserver.log -t string
```

4 Copy the broker credentials from one node in the cluster to sys5 by copying the entire `bkup` directory.

The `bkup` directory content resembles the following example:

```
# cd /var/VRTSvcs/vcsauth/bkup/  
  
# ls  
  
CMDSERVER HAD VCS_SERVICES WAC  
  
HAD VCS_SERVICES WAC
```

5 Import the `VCS_SERVICES` domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atutil import -z \  
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER -f /var/VRTSvcs/vcsauth/bkup \  
/VCS_SERVICES -p password
```

6 Import the credentials for HAD, CMDSERVER, and WAC.

Import the credentials for HAD, CMDSERVER, and WAC.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atutil import -z \  
/var/VRTSvcs/vcsauth/data/VCS_SERVICES -f /var/VRTSvcs/vcsauth/bkup \  
/HAD -p password
```

7 Start the `vcsauthserver` process on `sys5`.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh
```

8 Perform the following tasks:

```
# mkdir /var/VRTSvcs/vcsauth/data/CLIENT
# mkdir /var/VRTSvcs/vcsauth/data/TRUST
# export EAT_DATA_DIR='/var/VRTSvcs/vcsauth/data/TRUST'
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat setuptrust -b \
localhost:14149 -s high
```

9 Create the `/etc/VRTSvcs/conf/config/.secure` file:

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

Setting up SF Sybase CE related security configuration

Perform the following steps to configure SF Sybase CE related security settings.

Setting up SF Sybase CE related security configuration

1 Start `/opt/VRTSvcs/bin/vxatd` process.

2 Create `HA_SERVICES` domain for SF Sybase CE.

```
# vssat createpd --pdrtype ab --domain HA_SERVICES
```

3 Add SF Sybase CE and webserver principal to AB on node sys5.

```
# vssat addprpl --pdrtype ab --domain HA_SERVICES --prplname \
webserver_VCS_prplname --password new_password --prpltype \
service --can_proxy
```

4 Create `/etc/VRTSvcs/conf/config/.secure` file:

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

Starting fencing on the new node

Perform the following steps to start fencing on the new node.

To start fencing on the new node

1 For disk-based fencing on at least one node, copy the following files from one of the nodes in the existing cluster to the new node:

```
/etc/sysconfig/vxfen
/etc/vxfendg
/etc/vxfenmode
```

- 2 For disk-based fencing, copy the following files from one of the nodes in the existing cluster to the new node:

```
/etc/sysconfig/vxfen
/etc/vxfendg
/etc/vxfenmode
```

- 3 Start fencing on the new node:
- 4 On the new node, verify that the GAB port memberships are a and b:

```
# gabconfig -a
GAB Port Memberships
=====
Port a gen    57c004 membership 012
Port b gen    57c019 membership 012
```

Configuring Cluster Volume Manager (CVM) and Cluster File System (CFS) on the new node

Modify the existing cluster configuration to configure Cluster Volume Manager (CVM) and Cluster File System (CFS) for the new node.

To configure CVM and CFS on the new node

- 1 Make a backup copy of the main.cf file on the existing node, if not backed up in previous procedures. For example:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.cf.2node
```

- 2 On one of the nodes in the existing cluster, set the cluster configuration to read-write mode:

```
# haconf -makerw
```

- 3 Add the new node to the VCS configuration, if not already added:

```
# hasys -add system3
```


- 4 To enable the existing cluster to recognize the new node, run the following commands on one of the existing nodes:

```
# hagrpl -modify cvm SystemList -add system3 2
# hagrpl -modify cvm AutoStartList -add system3
# hares -modify cvm_clus CVMNodeId -add system3 2
# haconf -dump -makero
# /etc/vx/bin/vxclustadm -m vcs reinit
# /etc/vx/bin/vxclustadm nidmap
```

- 5 On the remaining nodes of the existing cluster, run the following commands:

```
# /etc/vx/bin/vxclustadm -m vcs reinit
# /etc/vx/bin/vxclustadm nidmap
```

- 6 Copy the configuration files from one of the nodes in the existing cluster to the new node:

```
# rcp /etc/VRTSvcs/conf/config/main.cf \
system3:/etc/VRTSvcs/conf/config/main.cf
# rcp /etc/VRTSvcs/conf/config/CFSTypes.cf \
system3:/etc/VRTSvcs/conf/config/CFSTypes.cf
# rcp /etc/VRTSvcs/conf/config/CVMTypes.cf \
system3:/etc/VRTSvcs/conf/config/CVMTypes.cf
```

- 7 The `/etc/vx/tunefstab` file sets non-default tunables for local-mounted and cluster-mounted file systems.

If you have configured a `/etc/vx/tunefstab` file to tune cluster-mounted file systems on any of the existing cluster nodes, you may want the new node to adopt some or all of the same tunables.

To adopt some or all tunables, review the contents of the file, and copy either the file, or the portions desired, into the `/etc/vx/tunefstab` file on the new cluster node.

After adding the new node

Start VCS on the new node.

To start VCS on the new node

- 1 Start VCS on the new node:

```
# hastart
```

VCS brings the CVM group online.

- 2 Verify that the CVM group is online:

```
# hagrps -state
```

Configuring the ClusterService group for the new node

If the ClusterService group is configured on the existing cluster, add the node to the group by performing the steps in the following procedure on one of the nodes in the existing cluster.

To configure the ClusterService group for the new node

- 1 On an existing node, for example node01, write-enable the configuration:

```
# haconf -makerw
```

- 2 Add the node system3 to the existing ClusterService group.

```
# hagrps -modify ClusterService SystemList -add system3 2
```

```
# hagrps -modify ClusterService AutoStartList -add system3
```

- 3 Modify the IP address and NIC resource in the existing group for the new node.

```
# hares -modify gcoip Device eth0 -sys system3
```

```
# hares -modify gconic Device eth0 -sys system3
```

- 4 Save the configuration by running the following command from any node.

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

Adding a node to a cluster using the SF Sybase CE installer

You can add a node to a cluster using the `-addnode` option with the SF Sybase CE installer.

At the end of the process, the new node joins the SF Sybase CE cluster.

To add the node to an existing cluster using the installer

- 1 Log in as the root user on one of the nodes of the existing cluster.
- 2 Run the SF Sybase CE installer with the `-addnode` option.

```
# cd /opt/VRTS/install  
  
# ./installsfybasece<version> -addnode
```

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

See [“About the script-based installer”](#) on page 204.

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 SF Sybase CE cluster.

The installer uses the node information to identify the existing cluster.

```
Enter one node of the SF Sybase CE cluster to which  
you would like to add one or more new nodes: node01
```

```
Enter one node of the SFSYBASECE cluster to which  
you would like to add one or more new nodes: node01
```

- 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: system3
```

Confirm if the installer prompts if you want to add the node to the cluster.

The installer checks the installed products and RPMs on the nodes and discovers the network interfaces.

- 6 Enter the name of the network interface that you want to configure as the first private heartbeat link.

If there are IP addresses already configured on the interface, confirm whether you want to use the interface as the first private heartbeat link.

Note: The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster. The LLT configuration for the new node must be the same as that of the existing cluster.

```
Enter the NIC for the first private heartbeat
link on system3: [b,q,?] net1
```

```
Enter the NIC for the second private heartbeat
link on system3: [b,q,?] net2
```

Note: At least two private heartbeat links must be configured for high availability of the cluster.

- 7 Depending on the number of LLT links configured in the existing cluster, configure additional private heartbeat links for the new node.
 The installer verifies the network interface settings and displays the information.
- 8 Review and confirm the information.
- 9 If you have configured SMTP, SNMP, or the global cluster option in the existing cluster, you are prompted for the NIC information for the new node.

```
Enter the NIC for VCS to use on system3: eth3
```

The installer starts the SF Sybase CE processes and configures CVM and CFS on the new node. The new node is now part of the cluster.

To add the new node into the Sybase ASE CE cluster and database:

See [“Adding the new instance to the Sybase ASE CE cluster”](#) on page 349.

- 10 Configure the following service groups manually to include the new node in the VCS configuration:
 - The *binmnt* group which contains the Sybase binaries
 - The *Sybase* group which contains:
 - The new instance on the added node

- The database mounts where the database resides
 - The quorum mounts where the quorum device resides.
 - See [“Adding the new instance to the Sybase ASE CE cluster”](#) on page 349.
- 11 The installer prompts you with an option to mount the shared volumes on the new node. Select **y** to mount them.
- When completed, the installer confirms the volumes are mounted. The installer indicates the location of the log file, summary file, and response file with details of the actions performed.
- 12 Confirm that the new node has joined the SF Sybase CE cluster using `lltstat -n` and `gabconfig -a` commands.

Adding the new instance to the Sybase ASE CE cluster

To add a new Sybase CE instance to the cluster you must complete the following tasks:

- [Creating Sybase user and groups](#)
- [Preparing the mount point for Sybase resources on the new node](#)
- [Adding a new Sybase ASE CE instance to the Sybase ASE CE cluster](#)
- [Bringing the new Sybase ASE CE instance under VCS control](#)

Creating Sybase user and groups

To prepare the new node for a Sybase ASE CE instance, create the Sybase user and groups.

See your Sybase ASE CE documentation.

Preparing the mount point for Sybase resources on the new node

To prepare the new node for installing Sybase, you must prepare mount points on the new node for Sybase binaries, quorum device, and datafiles.

See [“Preparing for shared mount point on CFS for Sybase ASE CE binary installation”](#) on page 291.

See [“Preparing to create a Sybase ASE CE cluster”](#) on page 292.

Create the mount point for the file system with the Sybase binary files.

For example:

```
# mkdir -p /sybase
# chown -R sybase:sybase /sybase
```

Create the mount point for the file system with the Sybase quorum device.

For example:

```
# mkdir -p /quorum
# chown -R sybase:sybase /quorum
```

Create the mount point for the file system with the Sybase datafiles.

For example:

```
# mkdir -p /sybdata
# chown -R sybase:sybase /sybdata
```

Configuring CVM

As root user, execute the following procedure on the CVM master node only.

For an example main.cf files:

See [“Sample main.cf for a basic Sybase ASE CE cluster configuration under VCS control with shared mount point on CFS for Sybase binary installation”](#) on page 400.

To configure the CVM group in the main.cf file

- 1 Make a backup copy of the main.cf file.

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.cf.2node
```

- 2 On the CVM master node, execute:

```
# haconf -makerw
# hasys -add system3
# hagrps -modify cvm SystemList -add system3 2
# hagrps -modify cvm AutoStartList -add system3
# hares -modify cvm_clus CVMNodeId -add system3 2
# haconf -dump -makero
```

- 3 Verify the changes. Change directory to /etc/VRTSvcs/conf/config and run:

```
# hacf -verify .
```

- 4 Copy the new version of the main.cf to each system in the cluster including the newly added system.

```
# rcp (or scp) main.cf node02:/etc/VRTSvcs/conf/config
```

```
# rcp (or scp) main.cf system3:/etc/VRTSvcs/conf/config
```

In the example, node01 is the system where main.cf is edited; it does not need a copy.

- 5 To enable the existing cluster to recognize the new node, execute the following on each system in the existing cluster:

```
# /etc/vx/bin/vxclustadm -m vcs -t gab reinit
```

```
# /etc/vx/bin/vxclustadm nidmap
```

- 6 Start CVM on the newly added node

- Determine the node ID:

```
# cat /etc/llthosts
```

- Verify this host ID is seen by the GAB module.

```
# gabconfig -a
```

- Start the VCS engine.

- 7 Verify that the CVM group has come online on the newly added node.

```
# hastatus -sum
```

Adding a new Sybase ASE CE instance to the Sybase ASE CE cluster

For a CFS shared installation of Sybase ASE CE binaries, the new Sybase ASE CE instance on the new node can share the existing cluster's Sybase ASE CE binaries.

For a local VxFS installation of Sybase ASE CE binaries, you need to create diskgroups for binaries and install Sybase ASE CE binaries on the new node.

To configure the new node

- 1 From an existing node in the cluster, write enable the cluster configuration:

```
# haconf -makerw
```

- 2 In case of Sybase binaries on CFS, add the new node to the VCS service group for the Sybase binaries:

```
# hagrps -modify binmnt SystemList -add sys5 2
```

```
# hagrps -modify binmnt AutoStartList -add sys5
```

- 3 In case of Sybase binaries on local VxFS, add the name of the DiskGroup for the new node.

```
# hares -modify sybase_install_dg DiskGroup  
sybase_new_diskgroup -sys sys5
```

```
# hares -modify sybase_install_mnt BlockDevice  
/dev/vx/dsk/sybase_new_diskgroup/sybase_new_volume -sys sys5
```

```
# hares -modify sybase_install_vol DiskGroup  
sybase_new_diskgroup -sys sys5
```

```
# hares -modify sybase_install_vol Volume  
sybase_new_volume -sys sys5
```

- 4 Save the configuration changes.

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

- 5 Bring the VCS group for Sybase binaries group online on the new node:

```
# hagrps -online binmnt -sys sys5
```

To add the new node to the Sybase ASE CE cluster

- ◆ Follow the procedures in your Sybase ASE CE documentation.

Bringing the new Sybase ASE CE instance under VCS control

After adding a new instance to the Sybase ASE CE cluster you must bring it under VCS control.

To configure the new instance under VCS control

- 1 From an existing node in the cluster, write enable the cluster configuration:

```
# haconf -makerw
```

- 2 Add the node to the VCS service group for managing Sybase resources:

```
# hagrps -modify sybasece SystemList -add sys5 2
```

```
# hagrps -modify sybasece AutoStartList -add sys5
```

- 3 Add the new instance to the VCS resource used to manage Sybase instances:

```
# hares -modify ase Server ase3 -sys sys5
```

- 4 Save the configuration changes.

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

- 5 Bring the Sybase service group online on the new node:

```
# hagrps -online sybasece -sys sys5
```

Note: Before you bring the Sybase service group online, make sure you have manually created the Run file for the added instance on the added node, with appropriate instance information.

This completes the addition of the new node to the cluster. You now have a three node cluster.

Removing a node from SF Sybase CE clusters

About removing a node from a cluster

You can remove one or more nodes from an SF Sybase CE cluster. The following table provides a summary of the tasks required to add a node to an existing SF Sybase CE cluster.

Table 13-4 Tasks for removing a node from a cluster

| Step | Description |
|--|--|
| Prepare to remove the node: <ul style="list-style-type: none"> ■ Back up the configuration file. ■ Check the status of the nodes and the service groups. ■ Take the service groups offline and removing the database instances. | See “About removing a node from a cluster” on page 353. |
| Remove the node from the cluster. <ul style="list-style-type: none"> ■ Switch or remove any SF Sybase CE service groups on the node departing the cluster. ■ Delete the node from SF Sybase CE configuration. | See “About removing a node from a cluster” on page 353. |
| Modify the cluster configuration on remaining nodes. <ul style="list-style-type: none"> ■ Edit the /etc/llhosts file. ■ Edit the /etc/gabtab file. ■ Modify the VCS configuration to remove the node. ■ Modify the CVM configuration to remove the node. | See “Modifying the VCS configuration files on existing nodes” on page 356. See “Modifying the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node” on page 359. |
| For a cluster that is running in a secure mode, remove the security credentials from the leaving node. | See “Removing security credentials from the leaving node” on page 359. |

The Veritas product installer does not support removing a node. You must remove a node manually. The example procedures describe how to remove a node from a cluster with three nodes.

Removing a node from a cluster

Perform the following steps to remove a node from a cluster. The procedure can be done from any node remaining in the cluster or from a remote host.

To prepare to remove a node from a cluster

- 1 Take the Sybase ASE CE service group offline (if under VCS control) on the node you want to remove.

```
# hagrps -offline sybase_group -sys system3
```

- 2 Remove the Sybase ASE CE database instance from the node.
For instructions, see the Sybase ASE CE documentation.

- 3 Take the *binmnt* service group offline (if under VCS control) on the node you want to remove.

```
# hagrps -offline binmnt_group -sys system3
```

- 4 Stop the applications that use Veritas File System (VxFS) or Cluster File System (CFS) mount points and are not configured under VCS. Use native application commands to stop the applications.
- 5 Uninstall Sybase ASE CE from the node.
For instructions, see the Sybase ASE CE documentation.

To remove a node from a cluster

- 1 Unmount the VxFS/CFS file systems that are not configured under VCS.

```
# umount mount_point
```

- 2 Stop VCS on the node:

```
# hastop -local
```

- 3 Stop SF Sybase CE on the node using the SF Sybase CE installer.

```
# cd /opt/VRTS/install
```

```
# ./installsfbasece<version> -stop system3
```

The installer stops all SF Sybase CE processes.

- 4 Modify the VCS configuration files on the existing nodes to remove references to the deleted node.
See [“Modifying the VCS configuration files on existing nodes”](#) on page 356.
- 5 Modify the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node.
See [“Modifying the Cluster Volume Manager \(CVM\) configuration on the existing nodes to remove references to the deleted node”](#) on page 359.

Modifying the VCS configuration files on existing nodes

Modify the configuration files on the remaining nodes of the cluster to remove references to the deleted nodes.

Tasks for modifying the cluster configuration files:

- Edit the `/etc/llthosts` file
- Edit the `/etc/gabtab` file
- Modify the VCS configuration to remove the node

For an example `main.cf`:

To edit the `/etc/llthosts` file

- ◆ On each of the existing nodes, edit the `/etc/llthosts` file to remove lines that contain references to the removed nodes.

For example, if `system3` is the node removed from the cluster, remove the line `"2 system3"` from the file:

```
0 node01
1 node02
2 system3
```

Change to:

```
0 node01
1 node02
```

To edit the `/etc/gabtab` file

- ◆ Modify the following command in the `/etc/gabtab` file to reflect the number of systems after the node is removed:

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

where N is the number of remaining nodes in the cluster.

For example, with two nodes remaining, the file resembles:

```
/sbin/gabconfig -c -n2
```

Modify the VCS configuration file `main.cf` to remove all references to the deleted node.

Use one of the following methods to modify the configuration:

- Edit the `/etc/VRTSvcs/conf/config/main.cf` file
This method requires application down time.
- Use the command line interface
This method allows the applications to remain online on all remaining nodes.

The following procedure uses the command line interface and modifies the sample VCS configuration to remove references to the deleted node. Run the steps in the procedure from one of the existing nodes in the cluster. The procedure allows you to change the VCS configuration while applications remain online on the remaining nodes.

To modify the cluster configuration using the command line interface (CLI)

- 1 Back up the `/etc/VRTSvcs/conf/config/main.cf` file.

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

```
# cp main.cf main.cf.3node.bak
```

- 2 Change the cluster configuration to read-write mode:

```
# haconf -makerw
```

- 3 Remove the node from the `AutoStartList` attribute of the service group by specifying the remaining nodes in the desired order:

```
# hagrps -modify cvm AutoStartList node01 node02
```

- 4 Remove the deleted node from the system list of any other parent service groups to CVM that exist on the cluster before removing CVM. For example, to delete the node `system3`:

```
# hagrps -modify syb_grp SystemList -delete system3
# hagrps -modify Sybase SystemList -delete system3
# hagrps -modify cvm SystemList -delete system3
# hares -modify cvm_clus CVMNodeId -delete system3
```

- 5 If you have a local VxFS configuration, will also need to remove the diskgroup of node to be removed from `binmnt`.

```
# hares -modify sybase_install_dg DiskGroup -delete \
sybase_new_diskgroup
```

- 6 Remove the node from the SystemList attribute of the service group:

```
# hagrps -modify cvm SystemList -delete system3
```

If the system is part of the SystemList of a parent group, it must be deleted from the parent group first.

- 7 Remove the node from the CVMNodeId attribute of the service group:

```
# hares -modify cvm_clus CVMNodeId -delete system3
```

- 8 If you have the other service groups (such as the database service group or the ClusterService group) that have the removed node in their configuration, perform step 6 and step 7 for each of them.

- 9 Remove the deleted node from the NodeList attribute of all CFS mount resources:

```
# hares -modify CFSMount NodeList -delete system3
```

- 10 Remove the deleted node from the system list of any other service groups that exist on the cluster. For example, to delete the node `system3`:

```
# hagrps -modify appgrp SystemList -delete system3
# hagrps -modify crsgrp SystemList -delete system3
```

- 11 Remove the deleted node from the cluster system list:

```
# hasys -delete system3
```

- 12 Save the new configuration to disk:

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

- 13 Verify that the node is removed from the VCS configuration.

```
# grep -i system3 /etc/VRTSvcs/conf/config/main.cf
```

If the node is not removed, use the VCS commands as described in this procedure to remove the node.

Modifying the Cluster Volume Manager (CVM) configuration on the existing nodes to remove references to the deleted node

To modify the CVM configuration on the existing nodes to remove references to the deleted node

- ◆ On the remaining nodes of the existing cluster, run the following commands:

```
# /etc/vx/bin/vxclustadm -m vcs reinit  
# /etc/vx/bin/vxclustadm nidmap
```

Removing security credentials from the leaving node

If the leaving node is part of a cluster that is running in a secure mode, you must remove the security credentials from node sys5. Perform the following steps.

To remove the security credentials

- 1 Stop the AT process.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh \  
stop
```

- 2 Remove the credentials.

```
# rm -rf /var/VRTSvcs/vcsauth/data/
```

Configuration of disaster recovery environments

This chapter includes the following topics:

- [Disaster recovery options for SF Sybase CE](#)
- [About setting up a global cluster environment for SF Sybase CE](#)
- [About configuring a parallel global cluster using Volume Replicator \(VVR\) for replication](#)

Disaster recovery options for SF Sybase CE

SF Sybase CE supports configuring a disaster recovery environment using:

- Global clustering option (GCO) with replication
- Global clustering using Volume Replicator (VVR) for replication

Storage Foundation for Sybase CE supports configuring a disaster recovery environment using global clustering (GCO) using Volume Replicator (VVR) for replication.

For more about planning for disaster recovery environments:

See [“About global clusters”](#) on page 171.

See [“Supported replication technologies for global clusters”](#) on page 182.

You can install and configure clusters for your disaster recovery environment as you would for any cluster using the procedures in this installation guide.

For a high level description of the tasks for implementing disaster recovery environments:

See [“About configuring a parallel global cluster using Volume Replicator \(VVR\) for replication”](#) on page 361.

For complete details for configuring your disaster recovery environment once clusters are installed and configured:

See the *Symantec Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide*.

About setting up a global cluster environment for SF Sybase CE

Configuring a global cluster for environment with parallel clusters requires the coordination of many component setup tasks. The procedures provided here are guidelines. Refer to your product installation guide for your product installation and basic configuration for each cluster. You will need this guide to configure a global cluster environment and replication between the two configured clusters.

- Configure a SF Sybase CE cluster at the primary site
- Configure an SF Sybase CE cluster at the secondary site
- Configure a global cluster environment
- Test the HA/DR configuration

Upon successful testing, you can bring the environment into production

For global cluster configuration details:

See the *Symantec Storage Foundation and High Availability Solutions Disaster Recovery Guide*.

About configuring a parallel global cluster using Volume Replicator (VVR) for replication

Configuring a global cluster for environment with parallel clusters using Volume Replicator requires the coordination of many component setup tasks. The tasks listed below are guidelines.

Before configuring two clusters for global clustering, you must verify that:

- You have the correct installation options enabled for SF Sybase CE, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster and VVR enabled.

Review SF Sybase CE requirements and licensing information.

About configuring a parallel global cluster using Volume Replicator (VVR) for replication

- Both clusters have SF Sybase CE software installed and configured.

Note: You can install and configure both clusters at the same time, or you can configure the second cluster at a later time than the first.

You can use this guide to install and configure SF Sybase CE on each cluster. For details for configuring a global cluster environment and replication between the the clusters using VVR:

See the *Symantec Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide*.

See the *Symantec Storage Foundation for Sybase ASE CE Installation and Configuration Guide*.

With two clusters installed and configured , you are ready to configure a global cluster environment using VVR. You must perform the following tasks to modify both cluster configurations to support replication in the global cluster environment.

Table 14-1 Tasks for configuring a parallel global cluster with VVR

| Task | Description |
|--|--|
| Setting up replication on the primary site | <ul style="list-style-type: none"> ■ Create the Storage Replicator Log (SRL) in the disk group for the database. ■ Create the Replicated Volume Group (RVG) on the primary site. |
| Setting up replication on the secondary site | <ul style="list-style-type: none"> ■ Create a disk group to hold the data volume, SRL, and RVG on the storage on the secondary site. You must match the names and sizes of these volumes with the names and sizes of the volumes on the primary site. ■ Edit the <code>/etc/vx/vras/.rdg</code> file on the secondary site. ■ Use resolvable virtual IP addresses that set network RLINK connections as host names of the primary and secondary sites. ■ Create the replication objects on the secondary site. |
| Starting replication of the database. | <p>You can use either of the following methods to start replication:</p> <ul style="list-style-type: none"> ■ Automatic synchronization ■ Full synchronization with Storage Checkpoint |

Table 14-1 Tasks for configuring a parallel global cluster with VVR (*continued*)

| Task | Description |
|--|---|
| Configuring VCS for replication on clusters at both sites. | Configure Symantec Cluster Server (VCS) to provide high availability for the database: <ul style="list-style-type: none"> ■ Modify the VCS configuration on the primary site ■ Modify the VCS configuration on the secondary site |

Once the global clusters and replication with VVR are configured, the following replication use cases are supported for it:

- Migration of the role of the primary site to the remote site
- Takeover of the primary site role by the secondary site
- Migrate the role of primary site to the secondary site
- Migrate the role of new primary site back to the original primary site
- Take over after an outage
- Resynchronize after an outage
- Update the rlink to reflect changes

For details on the replication use cases:

See the *Symantec Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide*.

Uninstallation of Sybase ASE CE

This chapter includes the following topics:

- [Preparing to uninstall SF Sybase CE from a cluster](#)
- [Uninstalling SF Sybase CE with the script-based installer](#)
- [Performing an automated uninstallation of SF Sybase CE using response files](#)

Preparing to uninstall SF Sybase CE from a cluster

Perform the steps in the following procedure before you uninstall SF Sybase CE from a cluster.

To prepare to uninstall SF Sybase CE from a cluster

- 1 Stop applications that use the Sybase ASE CE database.
- 2 Stop Sybase instances.
- 3 Back up the Sybase database.
- 4 Uninstalling Sybase ASE CE (optional)
- 5 Stop the applications that use CFS (outside of VCS control).
- 6 Stop VCS.
- 7 Stop the applications that use VxFS (outside of VCS control).
- 8 Unmount VxFS file systems (outside of VCS control).

Uninstalling SF Sybase CE with the script-based installer

Perform the steps in the following procedure to remove SF Sybase CE from a cluster.

To remove SF Sybase CE from a cluster

- 1 Remove the SF Sybase CE RPMs. You can remove the RPMs using the uninstallation program or using the response file.

Using the uninstallation program:

```
# cd /opt/VRTS/install  
./uninstallsfsybasece<version>
```

Using the response file:

```
# ./uninstallsfsybasece<version> -responsefile /tmp/response_file
```

- 2 Remove other configuration files (optional).
- 3 Reboot the nodes.

```
# shutdown -r now
```

Performing an automated uninstallation of SF Sybase CE using response files

Uninstalling SF Sybase CE using a response file

Perform the steps in the following procedure to uninstall SF Sybase CE using a response file.

To uninstall SF Sybase CE using a response file

- 1 Make sure that you have completed the pre-uninstallation tasks.
See [“Preparing to uninstall SF Sybase CE from a cluster”](#) on page 364.
- 2 Create a response file using one of the available options.
For information on various options available for creating a response file:

Note: You must replace the host names in the response file with that of the systems from which you want to uninstall SF Sybase CE.

For a sample response file:

- 3 Navigate to the directory containing the SF Sybase CE uninstallation program:

```
# cd /opt/VRTS/install
```

- 4 Start the uninstallation:

```
# ./uninstallsfsybasece<version> -responsefile /tmp/response_file
```

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

Where */tmp/response_file* is the full path name of the response file.

- 5 Optionally, remove residual configuration files, if any.

Response file variables to uninstall SF Sybase CE

[Table 15-1](#) lists the response file variables that you can define to configure SF Sybase CE.

Table 15-1 Response file variables for uninstalling SF Sybase CE

| Variable | Description |
|--------------|---|
| CFG{systems} | List of systems on which the product is to be installed or uninstalled. List or scalar: list Optional or required: required |
| CFG{prod} | Defines the product to be installed or uninstalled. List or scalar: scalar Optional or required: required |

Table 15-1 Response file variables for uninstalling SF Sybase CE (*continued*)

| Variable | Description |
|---------------------|--|
| CFG{opt}{keyfile} | <p>Defines the location of an ssh keyfile that is used to communicate with all remote systems.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p> |
| CFG{opt}{tmppath} | <p>Defines the location where a working directory is created to store temporary files and the RPMs that are needed during the install. The default location is /var/tmp.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p> |
| CFG{opt}{logpath} | <p>Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p> |
| CFG{opt}{uninstall} | <p>Uninstalls SF Sybase CE RPMs.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p> |

Sample response file for uninstalling SF Sybase CE

The following sample response file uninstalls SF Sybase CE from nodes, node01 and node02.

```
our %CFG;

$CFG{opt}{uninstall}=1;
$CFG{prod}="SFSYBASECE62";
$CFG{systems}=[ qw(node01 node02) ];

1;
```

SF Sybase CE installation RPMs

This appendix includes the following topics:

- [SF Sybase CE installation RPMs](#)

SF Sybase CE installation RPMs

[Table B-1](#) lists the RPM name and contents for each SF Sybase CE RPM.

Table B-1 List of SF Sybase CE RPMs

| RPM | Content | Configuration |
|----------|---|---------------|
| VRTSgab | Depends on VRTSllt. Contains the binaries for Symantec Cluster Server group membership and atomic broadcast services. | Minimum |
| VRTSllt | Contains the binaries for Symantec Cluster Server low-latency transport. | Minimum |
| VRTSamf | Contains the binaries for the Veritas Asynchronous Monitoring Framework kernel driver functionality for the process and mount based agents. | Minimum |
| VRTSperl | Contains Perl for Veritas. | Minimum |
| VRTSspt | Contains the binaries for Veritas Software Support Tools. | Recommended |

Table B-1 List of SF Sybase CE RPMs (*continued*)

| RPM | Content | Configuration |
|------------|--|---------------|
| VRTSvcscs | <p>Depends on VRTSvxfen, VRTSgab, and VRTSIlt.</p> <p>Contains the following components:</p> <ul style="list-style-type: none"> ■ Contains the binaries for Symantec Cluster Server. ■ Contains the binaries for Symantec Cluster Server manual pages. ■ Contains the binaries for Symantec Cluster Server English message catalogs. ■ Contains the binaries for Symantec Cluster Server utilities. These utilities include security services. | Minimum |
| VRTSvcscag | <p>Depends on VRTSvcscs.</p> <p>Contains the binaries for Symantec Cluster Server bundled agents.</p> | Minimum |
| VRTSvcsea | <p>Required for VCS with the high availability agent for Sybase.</p> <p>VRTSvcsea contains the binaries for Veritas high availability agents for DB2, Sybase, and Oracle.</p> | Recommended |
| VRTSvlic | Contains the binaries for Symantec License Utilities. | Minimum |
| VRTSvxfen | <p>Depends on VRTSgab.</p> <p>Contains the binaries for Veritas I/O fencing.</p> | Minimum |
| VRTScavf | Symantec Cluster Server Agents for Storage Foundation Cluster File System | Minimum |
| VRTSfssdk | <p>Veritas File System Software Developer Kit</p> <p>For VxFS APIs, the RPM contains the public Software Developer Kit (SDK), which includes headers, libraries, and sample code. The SDK is required if some user programs use VxFS APIs.</p> | All |
| VRTSglm | Veritas Group Lock Manager for Storage Foundation Cluster File System | Minimum |
| VRTSob | Veritas Enterprise Administrator | Recommended |
| VRTSvxfs | Veritas File System binaries | Minimum |

Table B-1 List of SF Sybase CE RPMs (*continued*)

| RPM | Content | Configuration |
|------------|--|---------------|
| VRTSvxvm | Veritas Volume Manager binaries | Minimum |
| VRTSaslapm | Volume Manager ASL/APM | Minimum |
| VRTSsfcp62 | Symantec Storage Foundation Common Product Installer The Storage Foundation Common Product installer RPM contains the scripts that perform the following functions: installation, configuration, upgrade, uninstallation, adding nodes, and removing nodes. You can use this script to simplify the native operating system installations, configurations, and upgrades. | Minimum |
| VRTSsfmh | Symantec Storage Foundation Managed Host | Recommended |
| VRTSfsadv | Veritas File System Advanced Features by Symantec | Minimum |
| VRTSvcsdr | Veritas Cluster Server Disk Reservation Modules and Utilities by Symantec | Recommended |
| VRTSvbs | Veritas Virtual Business Service. | Recommended |

Installation scripts

This appendix includes the following topics:

- [Installation script options](#)
- [About using the postcheck option](#)

Installation script options

[Table C-1](#) shows command line options for the installation script. For an initial install or upgrade, options are not usually required. The installation script options apply to all Symantec Storage Foundation product scripts, except where otherwise noted.

See [“About the script-based installer”](#) on page 204.

Table C-1 Available command line options

| Command Line Option | Function |
|---------------------|--|
| -addnode | Adds a node to a high availability cluster. |
| -allpkgs | Displays all RPMs required for the specified product. The RPMs are listed in correct installation order. The output can be used to create scripts for command line installs, or for installations over a network. |
| -comcleanup | The <code>-comcleanup</code> option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated. |

Table C-1 Available command line options (*continued*)

| Command Line Option | Function |
|------------------------------------|---|
| -comsetup | The <code>-comsetup</code> option is used to set up the ssh or rsh communication between systems without requests for passwords or passphrases. |
| -configcps | The <code>-configcps</code> option is used to configure CP server on a running system or cluster. |
| -configure | Configures the product after installation. |
| -fencing | Configures I/O fencing in a running cluster. |
| -fips | The <code>-fips</code> option is used to enable or disable security with fips mode on a running VCS cluster. It could only be used together with <code>-security</code> or <code>-securityonnode</code> option. |
| -hostfile <i>full_path_to_file</i> | Specifies the location of a file that contains a list of hostnames on which to install. |
| -disable_dmp_native_support | Disables Dynamic Multi-pathing support for the native LVM volume groups and ZFS pools during upgrade. Retaining Dynamic Multi-pathing support for the native LVM volume groups and ZFS pools during upgrade increases RPM upgrade time depending on the number of LUNs and native LVM volume groups and ZFS pools configured on the system. |
| -online_upgrade | Used to perform online upgrade. Using this option, the installer upgrades the whole cluster and also supports customer's application zero down time during the upgrade procedure. Now this option only supports VCS and ApplicationHA. |
| -patch_path | Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed . |
| -patch2_path | Defines the path of a second patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |

Table C-1 Available command line options (*continued*)

| Command Line Option | Function |
|------------------------------|---|
| -patch3_path | Defines the path of a third patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |
| -patch4_path | Defines the path of a fourth patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |
| -patch5_path | Defines the path of a fifth patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed. |
| -installallpkgs | The <code>-installallpkgs</code> option is used to select all RPMs. |
| -installrecpkgs | The <code>-installrecpkgs</code> option is used to select the recommended RPMs set. |
| -installminpkgs | The <code>-installminpkgs</code> option is used to select the minimum RPMs set. |
| -ignorepatchreqs | The <code>-ignorepatchreqs</code> option is used to allow installation or upgrading even if the prerequisite RPMs or patches are missed on the system. |
| -keyfile <i>ssh_key_file</i> | Specifies a key file for secure shell (SSH) installs. This option passes <code>-I ssh_key_file</code> to every SSH invocation. |
| -kickstart <i>dir_path</i> | Produces a kickstart configuration file for installing with Linux RHEL Kickstart. The file contains the list of Symantec RPMs in the correct order for installing, in a format that can be used for Kickstart installations. The <i>dir_path</i> indicates the path to the directory in which to create the file. |
| -license | Registers or updates product licenses on the specified systems. |

Table C-1 Available command line options (*continued*)

| Command Line Option | Function |
|--------------------------------|--|
| <code>-logpath log_path</code> | Specifies a directory other than <code>/opt/VRTS/install/logs</code> as the location where installer log files, summary files, and response files are saved. |
| <code>-makeresponsefile</code> | Use the <code>-makeresponsefile</code> option only to generate response files. No actual software installation occurs when you use this option. |
| <code>-minpkgs</code> | Displays the minimal RPMs required for the specified product. The RPMs are listed in correct installation order. Optional RPMs are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See <code>allpkgs</code> option. |
| <code>-noipc</code> | Disables the installer from making outbound networking calls to Symantec Operations Readiness Tool (SORT) in order to automatically obtain patch and release information updates. |
| <code>-nolic</code> | Allows installation of product RPMs without entering a license key. Licensed features cannot be configured, started, or used when this option is specified. |
| <code>-pkginfo</code> | Displays a list of RPMs and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the <code>-pkginfo</code> option with the <code>installvcs</code> script to display VCS RPMs. |
| <code>-pkgset</code> | Discovers and displays the RPM group (minimum, recommended, all) and RPMs that are installed on the specified systems. |
| <code>-pkgtable</code> | Displays product's RPMs in correct installation order by group. |
| <code>-postcheck</code> | Checks for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups. |

Table C-1 Available command line options (*continued*)

| Command Line Option | Function |
|------------------------------------|--|
| -precheck | Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product. |
| -prod | Specifies the product for operations. |
| -recpkgs | Displays the recommended RPMs required for the specified product. The RPMs are listed in correct installation order. Optional RPMs are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See <code>allpkgs</code> option. |
| -redirect | Displays progress details without showing the progress bar. |
| -require | Specifies an installer patch file. |
| -requirements | The <code>-requirements</code> option displays required OS version, required RPMs and patches, file system space, and other system requirements in order to install the product. |
| -responsefile <i>response_file</i> | Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The <i>response_file</i> must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. |
| -rolling_upgrade | Starts a rolling upgrade. Using this option, the installer detects the rolling upgrade status on cluster systems automatically without the need to specify rolling upgrade phase 1 or phase 2 explicitly. |
| -rollingupgrade_phase1 | The <code>-rollingupgrade_phase1</code> option is used to perform rolling upgrade Phase-I. In the phase, the product kernel RPMs get upgraded to the latest version. |

Table C-1 Available command line options (*continued*)

| Command Line Option | Function |
|------------------------|--|
| -rollingupgrade_phase2 | The <code>-rollingupgrade_phase2</code> option is used to perform rolling upgrade Phase-II. In the phase, VCS and other agent RPMs upgrade to the latest version. Product kernel drivers are rolling-upgraded to the latest protocol version. |
| -rsh | Specify this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP. See “About configuring secure shell or remote shell communication modes before installing products” on page 422. |
| -security | The <code>-security</code> option is used to convert a running VCS cluster between secure and non-secure modes of operation. |
| -securityonenode | The <code>-securityonenode</code> option is used to configure a secure cluster node by node. |
| -securitytrust | The <code>-securitytrust</code> option is used to setup trust with another broker. |
| -serial | Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems. |
| -settunables | Specify this option when you want to set tunable parameters after you install and configure a product. You may need to restart processes of the product for the tunable parameter values to take effect. You must use this option together with the <code>-tunablesfile</code> option. |
| -start | Starts the daemons and processes for the specified product. |
| -stop | Stops the daemons and processes for the specified product. |

Table C-1 Available command line options (*continued*)

| Command Line Option | Function |
|-------------------------------------|---|
| -timeout | The <code>-timeout</code> option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the <code>-timeout</code> option overrides the default value of 1200 seconds. Setting the <code>-timeout</code> option to 0 prevents the script from timing out. The <code>-timeout</code> option does not work with the <code>-serial</code> option. |
| -tmppath <i>tmp_path</i> | Specifies a directory other than <code>/var/tmp</code> as the working directory for the installation scripts. This destination is where initial logging is performed and where RPMs are copied on remote systems before installation. |
| -tunables | Lists all supported tunables and create a tunables file template. |
| -tunables_file <i>tunables_file</i> | Specify this option when you specify a tunables file. The tunables file should include tunable parameters. |
| -upgrade | Specifies that an existing version of the product exists and you plan to upgrade it. |
| -version | Checks and reports the installed products and their versions. Identifies the installed and missing RPMs and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing RPMs and patches where applicable. Lists the installed patches, patches, and available updates for the installed product if an Internet connection is available. |
| -yumgroupxml | The <code>-yumgroupxml</code> option is used to generate a yum group definition XML file. The <code>createrepo</code> command can use the file on Redhat Linux to create a yum group for automated installation of all RPMs for a product. An available location to store the XML file should be specified as a complete path. The <code>-yumgroupxml</code> option is supported on Redhat Linux only. |

About using the postcheck option

You can use the installer's post-check to determine installation-related problems and to aid in troubleshooting.

Note: This command option requires downtime for the node.

When you use the `postcheck` option, it can help you troubleshoot the following VCS-related issues:

- The heartbeat link does not exist.
- The heartbeat link cannot communicate.
- The heartbeat link is a part of a bonded or aggregated NIC.
- A duplicated cluster ID exists (if LLT is not running at the check time).
- The VRTSllt pkg version is not consistent on the nodes.
- The llt-linkinstall value is incorrect.
- The `/etc/llthosts` and `/etc/llttab` configuration is incorrect.
- the `/etc/gabtab` file is incorrect.
- The incorrect GAB linkinstall value exists.
- The VRTSgab pkg version is not consistent on the nodes.
- The `main.cf` file or the `types.cf` file is invalid.
- The `/etc/VRTSvcs/conf/sysname` file is not consistent with the hostname.
- The cluster UUID does not exist.
- The `uuidconfig.pl` file is missing.
- The VRTSvcs pkg version is not consistent on the nodes.
- The `/etc/vxfenmode` file is missing or incorrect.
- The `/etc/vxfendg` file is invalid.
- The vxfen link-install value is incorrect.
- The VRTSvxfen pkg version is not consistent.

The `postcheck` option can help you troubleshoot the following SFHA or SFCFSHA issues:

- Volume Manager cannot start because the `/etc/vx/reconfig.d/state.d/install-db` file has not been removed.

- Volume Manager cannot start because the `volboot` file is not loaded.
- Volume Manager cannot start because no license exists.
- Cluster Volume Manager cannot start because the CVM configuration is incorrect in the `main.cf` file. For example, the `Autostartlist` value is missing on the nodes.
- Cluster Volume Manager cannot come online because the node ID in the `/etc/llthosts` file is not consistent.
- Cluster Volume Manager cannot come online because `Vxfen` is not started.
- Cluster Volume Manager cannot start because `gab` is not configured.
- Cluster Volume Manager cannot come online because of a CVM protocol mismatch.
- Cluster Volume Manager group name has changed from "cvm", which causes CVM to go offline.

You can use the installer's post-check option to perform the following checks:

General checks for all products:

- All the required RPMs are installed.
- The versions of the required RPMs are correct.
- There are no verification issues for the required RPMs.

Checks for Volume Manager (VM):

- Lists the daemons which are not running (`vxattachd`, `vxconfigbackupd`, `vxesd`, `vxrelocd` ...).
- Lists the disks which are not in 'online' or 'online shared' state (`vxdisk list`).
- Lists the diskgroups which are not in 'enabled' state (`vxdg list`).
- Lists the volumes which are not in 'enabled' state (`vxprint -g <dgname>`).
- Lists the volumes which are in 'Unstartable' state (`vxinfo -g <dgname>`).
- Lists the volumes which are not configured in `/etc/fstab`.

Checks for File System (FS):

- Lists the VxFS kernel modules which are not loaded (`vxfs/fdd/vxportal`).
- Whether all VxFS file systems present in `/etc/fstab` file are mounted.
- Whether all VxFS file systems present in `/etc/fstab` are in disk layout 6 or higher.
- Whether all mounted VxFS file systems are in disk layout 6 or higher.

Checks for Cluster File System:

- Whether FS and ODM are running at the latest protocol level.
- Whether all mounted CFS file systems are managed by VCS.
- Whether cvm service group is online.

Sample installation and configuration values

This appendix includes the following topics:

- [SF Sybase CE installation and configuration information](#)
- [SF Sybase CE worksheet](#)

SF Sybase CE installation and configuration information

The SF Sybase CE installation and configuration program prompts you for information about SF Sybase CE. It also provides default values for some information which you can choose to use. The worksheets provide sample values that you can use as examples of the information required for an SF Sybase CE installation and configuration.

Symantec recommends using the worksheets provided to record values for your systems before you begin the installation and configuration process.

SF Sybase CE worksheet

[Table D-1](#) contains the sample values that may be used when you install and configure SF Sybase CE. Enter the SF Sybase CE values for your systems in the following table:

Table D-1 SF Sybase CE worksheet

| Installation information | Sample value | Assigned value |
|---|---|----------------|
| Number of nodes in the cluster | 2 | |
| Host names for Primary cluster | node01 and node02 | |
| Host names for added or removed node | sys5 | |
| SF Sybase CE License key | License keys are in the format: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXX | |
| Required SF Sybase CE RPMs vs. all SF Sybase CE RPMs | Install only the required RPMs if you do not want to configure any optional components or features. Default option is to install all RPMs. | |
| Primary cluster name | clus1 | |
| Primary cluster ID number | 101 | |
| <p>Private network links</p> <p>You can choose a network interface card that is not part of any aggregated interface, or you can choose an aggregated interface.</p> <p>The interface names that are associated with each NIC for each network link must be the same on all nodes.</p> <p>Do not use the network interface card that is used for the public network, which is typically eth0.</p> | eth1,eth2 | |
| Cluster Manager NIC (Primary NIC) | eth0 | |
| Cluster Manager IP | 10.10.12.1, 10.10.12.2 | |
| Netmask for the virtual IP address | 255.255.240.0 | |

Table D-1 SF Sybase CE worksheet (*continued*)

| Installation information | Sample value | Assigned value |
|---|--------------------------|----------------|
| <p>Mode for Authentication Service:</p> <ul style="list-style-type: none"> ■ Automatic mode ■ Semiautomatic mode using encrypted files ■ Semiautomatic mode without using encrypted files <p>Default option is automatic mode.</p> | Automatic mode | |
| <p>User name</p> <p>Adding users is required if when using secure cluster mode. Otherwise it is optional.</p> | smith | |
| <p>User password</p> | password | |
| <p>User privilege</p> <p>VCS privilege levels include:</p> <ul style="list-style-type: none"> ■ Administrators— Can perform all operations, including configuration options on the cluster, service groups, systems, resources, and users. ■ Operators—Can perform specific operations on a cluster or a service group. ■ Guests—Can view specified objects. | admin | |
| <p>Domain-based address of the SMTP server</p> <p>The SMTP server sends notification email about the events within the cluster.</p> | smtp.symantecexample.com | |
| <p>Email address of each SMTP recipient to be notified</p> | john@symantecexample.com | |

Table D-1 SF Sybase CE worksheet (*continued*)

| Installation information | Sample value | Assigned value |
|--|---------------------------|----------------|
| <p>Minimum severity of events for SMTP email notification</p> <p>The severity levels are defined as follows:</p> <ul style="list-style-type: none"> ■ Information - Important events that exhibit normal behavior ■ Warning - Deviation from normal behavior ■ Error - A fault ■ Severe Error -Critical error that can lead to data loss or corruption | E | |
| <p>Email address of SMTP notification recipients</p> | admin@symantecexample.com | |
| <p>SNMP trap daemon port number the console</p> | 162 | |
| <p>System name for the SNMP console</p> | system2 | |
| <p>Minimum severity level of events for SMTP notification</p> <p>The severity levels are defined as follows:</p> <ul style="list-style-type: none"> ■ Information - Important events that exhibit normal behavior ■ Warning - Deviation from normal behavior ■ Error - A fault ■ Severe Error -Critical error that can lead to data loss or corruption | i | |
| <p>CVM enclosure-based naming</p> <p>Requires Dynamic Multi-pathing (DMP).</p> | yes | |

Table D-1 SF Sybase CE worksheet (*continued*)

| Installation information | Sample value | Assigned value |
|--|---|----------------|
| <p>Default disk group</p> <p>You can select the name of a default disk group of a system for running Veritas Volume Manager commands which require a disk group to be specified.</p> | <p>vxfencoordg</p> | |
| <p>The name of three disks that form the coordinator disk group.</p> | <ul style="list-style-type: none"> ■ sdd ■ sde ■ sdf | |
| <p>Vxfen disk group</p> | <p>vxfencoordg</p> | |

Tunable files for installation

This appendix includes the following topics:

- [Setting tunables for an installation, configuration, or upgrade](#)
- [Setting tunables with no other installer-related operations](#)
- [Setting tunables with an un-integrated response file](#)
- [Preparing the tunables file](#)
- [Setting parameters for the tunables file](#)
- [Tunables value parameter definitions](#)

Setting tunables for an installation, configuration, or upgrade

You can use a tunables file for installation procedures to set non-default tunables. You invoke the installation script with the `tunablesfile` option. The tunables file passes arguments to the script to set the selected tunables. You must select the tunables that you want to use from this guide.

See [“Tunables value parameter definitions”](#) on page 390.

Note: Certain tunables only take effect after a system reboot.

To set the non-default tunables for an installation, configuration, or upgrade

- 1 Prepare the tunables file.
See [“Preparing the tunables file”](#) on page 389.
- 2 Make sure the systems where you want to install SF Sybase CE meet the installation requirements.

- 3 Complete any preinstallation tasks.
- 4 Copy the tunables file to one of the systems where you want to install, configure, or upgrade the product.
- 5 Mount the product disc and navigate to the directory that contains the installation program.
- 6 Start the installer for the installation, configuration, or upgrade. For example:

```
# ./installmr -tunablesfile /tmp/tunables_file  
-setttunables [sys1 sys2 ...]
```

Where `/tmp/tunables_file` is the full path name for the tunables file.

- 7 Proceed with the operation. When prompted, accept the tunable parameters. Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.
- 8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Setting tunables with no other installer-related operations

You can use the installer to set tunable parameters without any other installer-related operations. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See [“Tunables value parameter definitions”](#) on page 390.

Note: Certain tunables only take effect after a system reboot.

To set tunables with no other installer-related operations

- 1 Prepare the tunables file.
See [“Preparing the tunables file”](#) on page 389.
- 2 Make sure the systems where you want to install SF Sybase CE meet the installation requirements.
- 3 Complete any preinstallation tasks.
- 4 Copy the tunables file to one of the systems that you want to tune.

5 Mount the product disc and navigate to the directory that contains the installation program.

6 Start the installer with the `-settunables` option.

```
# ./installmr -tunablesfile tunables_file_name -settunables [  
sys123 sys234 ...]
```

Where `/tmp/tunables_file` is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Setting tunables with an un-integrated response file

You can use the installer to set tunable parameters with an un-integrated response file. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See [“Tunables value parameter definitions”](#) on page 390.

Note: Certain tunables only take effect after a system reboot.

To set tunables with an un-integrated response file

1 Make sure the systems where you want to install SF Sybase CE meet the installation requirements.

2 Complete any preinstallation tasks.

3 Prepare the tunables file.

See [“Preparing the tunables file”](#) on page 389.

4 Copy the tunables file to one of the systems that you want to tune.

5 Mount the product disc and navigate to the directory that contains the installation program.

- 6 Start the installer with the `-responsefile` and `-tunablesfile` options.

```
# ./installmr -responsefile response_file_name -tunablesfile  
tunables_file_name
```

Where *response_file_name* is the full path name for the response file and *tunables_file_name* is the full path name for the tunables file.

- 7 Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.
- 8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

For more information on response files, see the *chapter: About response files*.

Preparing the tunables file

A tunables file is a Perl module and consists of an opening and closing statement, with the tunables defined between. Use the hash symbol at the beginning of the line to comment out the line. The tunables file opens with the line "our %TUN;" and ends with the return true "1;" line. The final return true line only needs to appear once at the end of the file. Define each tunable parameter on its own line.

You can use the installer to create a tunables file template, or manually format tunables files you create.

To create a tunables file template

- ◆ Start the installer with the `-tunables` option. Enter the following:

```
# ./installmr -tunables
```

You see a list of all supported tunables, and the location of the tunables file template.

To manually format tunables files

- ◆ Format the tunable parameter as follows:

```
$TUN{"tunable_name"}{"system_name"|"*"}=value_of_tunable;
```

For the *system_name*, use the name of the system, its IP address, or a wildcard symbol. The *value_of_tunable* depends on the type of tunable you are setting. End the line with a semicolon.

The following is an example of a tunables file.

```
#  
# Tunable Parameter Values:  
#  
our %TUN;  
  
$TUN{ "tunable1" } {"*"}=1024;  
$TUN{ "tunable3" } {"sys123"}="SHA256";  
  
1;
```

Setting parameters for the tunables file

Each tunables file defines different tunable parameters. The values that you can use are listed in the description of each parameter. Select the tunables that you want to add to the tunables file and then configure each parameter.

See [“Tunables value parameter definitions”](#) on page 390.

Each line for the parameter value starts with \$TUN. The name of the tunable is in curly brackets and double-quotes. The system name is enclosed in curly brackets and double-quotes. Finally define the value and end the line with a semicolon, for example:

```
$TUN{ "dmp_daemon_count" } {"node123"}=16;
```

In this example, you are changing the `dmp_daemon_count` value from its default of 10 to 16. You can use the wildcard symbol "*" for all systems. For example:

```
$TUN{ "dmp_daemon_count" } {"*"}=16;
```

Tunables value parameter definitions

When you create a tunables file for the installer you can only use the parameters in the following list.

Prior to making any updates to the tunables, refer to the *Symantec Storage Foundation Cluster File System High Availability Administrator's Guide* for detailed information on product tunable ranges and recommendations.

[Table E-1](#) describes the supported tunable parameters that can be specified in a tunables file.

Table E-1 Supported tunable parameters

| Tunable | Description |
|-----------------------|--|
| autoreminor | (Veritas Volume Manager) Enable reminoring in case of conflicts during disk group import. |
| autostartvolumes | (Veritas Volume Manager) Enable the automatic recovery of volumes. |
| dmp_cache_open | (Symantec Dynamic Multi-Pathing) Whether the first open on a device performed by an array support library (ASL) is cached. |
| dmp_daemon_count | (Symantec Dynamic Multi-Pathing) The number of kernel threads for DMP administrative tasks. |
| dmp_delayq_interval | (Symantec Dynamic Multi-Pathing) The time interval for which DMP delays the error processing if the device is busy. |
| dmp_fast_recovery | (Symantec Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Symantec Dynamic Multi-Pathing is started. |
| dmp_health_time | (Symantec Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy. |
| dmp_log_level | (Symantec Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed. |
| dmp_low_impact_probe | (Symantec Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. |
| dmp_lun_retry_timeout | (Symantec Dynamic Multi-Pathing) The retry period for handling transient errors. |
| dmp_monitor_fabric | (Symantec Dynamic Multi-Pathing) Whether the Event Source daemon (<code>vxesd</code>) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Symantec Dynamic Multi-Pathing is started. |

Table E-1 Supported tunable parameters (*continued*)

| Tunable | Description |
|---------------------------|---|
| dmp_monitor_osevent | (Symantec Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. |
| dmp_monitor_ownership | (Symantec Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. |
| dmp_native_support | (Symantec Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices. |
| dmp_path_age | (Symantec Dynamic Multi-Pathing) The time for which an intermittently failing path needs to be monitored before DMP marks it as healthy. |
| dmp_pathswitch_blks_shift | (Symantec Dynamic Multi-Pathing) The default number of contiguous I/O blocks sent along a DMP path to an array before switching to the next available path. |
| dmp_probe_idle_lun | (Symantec Dynamic Multi-Pathing) Whether the path restoration kernel thread probes idle LUNs. |
| dmp_probe_threshold | (Symantec Dynamic Multi-Pathing) The number of paths will be probed by the restore daemon. |
| dmp_restore_cycles | (Symantec Dynamic Multi-Pathing) The number of cycles between running the check_all policy when the restore policy is check_periodic. |
| dmp_restore_interval | (Symantec Dynamic Multi-Pathing) The time interval in seconds the restore daemon analyzes the condition of paths. |
| dmp_restore_policy | (Symantec Dynamic Multi-Pathing) The policy used by DMP path restoration thread. |
| dmp_restore_state | (Symantec Dynamic Multi-Pathing) Whether kernel thread for DMP path restoration is started. |

Table E-1 Supported tunable parameters (*continued*)

| Tunable | Description |
|----------------------|---|
| dmp_retry_count | (Symantec Dynamic Multi-Pathing) The number of times a path reports a path busy error consecutively before DMP marks the path as failed. |
| dmp_scsi_timeout | (Symantec Dynamic Multi-Pathing) The timeout value for any SCSI command sent via DMP. |
| dmp_sfg_threshold | (Symantec Dynamic Multi-Pathing) The status of the subpaths failover group (SFG) feature. |
| dmp_stat_interval | (Symantec Dynamic Multi-Pathing) The time interval between gathering DMP statistics. |
| fssmartmovethreshold | (Veritas Volume Manager) The file system usage threshold for SmartMove (percent). This tunable must be set after Veritas Volume Manager is started. |
| max_diskq | (Veritas File System) Specifies the maximum disk queue generated by a single file. The installer can only set the system default value of max_diskq. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |
| read_ahead | (Veritas File System) The 0 value disables read ahead functionality, the 1 value (default) retains traditional sequential read ahead behavior, and the 2 value enables enhanced read ahead for all reads. The installer can only set the system default value of read_ahead. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |
| read_nstream | (Veritas File System) The number of parallel read requests of size read_pref_io that can be outstanding at one time. The installer can only set the system default value of read_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |

Table E-1 Supported tunable parameters (*continued*)

| Tunable | Description |
|-------------------------------|---|
| read_pref_io | (Veritas File System) The preferred read request size. The installer can only set the system default value of read_pref_io. Refer to the tuneftab(4) manual page for setting this tunable for a specified block device. |
| reclaim_on_delete_start_time | (Veritas Volume Manager) Time of day to start reclamation for deleted volumes. This tunable must be set after Veritas Volume Manager is started. |
| reclaim_on_delete_wait_period | (Veritas Volume Manager) Days to wait before starting reclamation for deleted volumes. This tunable must be set after Veritas Volume Manager is started. |
| same_key_for_alldgs | (Veritas Volume Manager) Use the same fencing key for all disk groups. This tunable must be set after Veritas Volume Manager is started. |
| sharedminorstart | (Veritas Volume Manager) Start of range to use for minor numbers for shared disk groups. This tunable must be set after Veritas Volume Manager is started. |
| storage_connectivity | (Veritas Volume Manager) The CVM storage connectivity type. This tunable must be set after Veritas Volume Manager is started. |
| usefssmartmove | (Veritas Volume Manager) Configure SmartMove feature (all, thinonly, none). This tunable must be set after Veritas Volume Manager is started. |
| vol_checkpoint_default | (Veritas File System) Size of VxVM storage checkpoints (kBytes). This tunable requires a system reboot to take effect. |
| vol_cmpres_enabled | (Veritas Volume Manager) Allow enabling compression for Volume Replicator. |
| vol_cmpres_threads | (Veritas Volume Manager) Maximum number of compression threads for Volume Replicator. |

Table E-1 Supported tunable parameters (*continued*)

| Tunable | Description |
|------------------------|---|
| vol_default_iodelay | (Veritas Volume Manager) Time to pause between I/O requests from VxVM utilities (10ms units). This tunable requires a system reboot to take effect. |
| vol_fmr_logsz | (Veritas Volume Manager) Maximum size of bitmap Fast Mirror Resync uses to track changed blocks (KBytes). This tunable requires a system reboot to take effect. |
| vol_max_adminio_poolsz | (Veritas Volume Manager) Maximum amount of memory used by VxVM admin I/O's (bytes). This tunable requires a system reboot to take effect. |
| vol_max_nm_poolsz | (Veritas Volume Manager) Maximum name pool size (bytes). |
| vol_max_rdback_sz | (Veritas Volume Manager) Storage Record readback pool maximum (bytes). |
| vol_max_wrspool_sz | (Veritas Volume Manager) Maximum memory used in clustered version of Volume Replicator . |
| vol_maxio | (Veritas Volume Manager) Maximum size of logical VxVM I/O operations (kBytes). This tunable requires a system reboot to take effect. |
| vol_maxioctl | (Veritas Volume Manager) Maximum size of data passed into the VxVM ioctl calls (bytes). This tunable requires a system reboot to take effect. |
| vol_maxparallelio | (Veritas Volume Manager) Number of I/O operations vxconfigd can request at one time. This tunable requires a system reboot to take effect. |
| vol_maxspecialio | (Veritas Volume Manager) Maximum size of a VxVM I/O operation issued by an ioctl call (kBytes). This tunable requires a system reboot to take effect. |
| vol_min_lowmem_sz | (Veritas Volume Manager) Low water mark for memory (bytes). |

Table E-1 Supported tunable parameters (*continued*)

| Tunable | Description |
|-----------------------------|---|
| vol_nm_hb_timeout | (Veritas Volume Manager) Volume Replicator timeout value (ticks). |
| vol_rvio_maxpool_sz | (Veritas Volume Manager) Maximum memory requested by Volume Replicator (bytes). |
| vol_stats_enable | (Veritas Volume Manager) Enable VxVM I/O stat collection. |
| vol_subdisk_num | (Veritas Volume Manager) Maximum number of subdisks attached to a single VxVM plex. This tunable requires a system reboot to take effect. |
| voldrl_max_drtregs | (Veritas Volume Manager) Maximum number of dirty VxVM regions. This tunable requires a system reboot to take effect. |
| voldrl_max_seq_dirty | (Veritas Volume Manager) Maximum number of dirty regions in sequential mode. This tunable requires a system reboot to take effect. |
| voldrl_min_regionsz | (Veritas Volume Manager) Minimum size of a VxVM Dirty Region Logging (DRL) region (kBytes). This tunable requires a system reboot to take effect. |
| voldrl_volumemax_drtregs | (Veritas Volume Manager) Max per volume dirty regions in log-plex DRL. |
| voldrl_volumemax_drtregs_20 | (Veritas Volume Manager) Max per volume dirty regions in DCO version 20. |
| voldrl_dirty_regions | (Veritas Volume Manager) Number of regions cached for DCO version 30. |
| voliomem_chunk_size | (Veritas Volume Manager) Size of VxVM memory allocation requests (bytes). This tunable requires a system reboot to take effect. |
| voliomem_maxpool_sz | (Veritas Volume Manager) Maximum amount of memory used by VxVM (bytes). This tunable requires a system reboot to take effect. |

Table E-1 Supported tunable parameters (*continued*)

| Tunable | Description |
|----------------------|---|
| voliot_errbuf_dfit | (Veritas Volume Manager) Size of a VxVM error trace buffer (bytes). This tunable requires a system reboot to take effect. |
| voliot_jobuf_default | (Veritas Volume Manager) Default size of a VxVM I/O trace buffer (bytes). This tunable requires a system reboot to take effect. |
| voliot_jobuf_limit | (Veritas Volume Manager) Maximum total size of all VxVM I/O trace buffers (bytes). This tunable requires a system reboot to take effect. |
| voliot_jobuf_max | (Veritas Volume Manager) Maximum size of a VxVM I/O trace buffer (bytes). This tunable requires a system reboot to take effect. |
| voliot_max_open | (Veritas Volume Manager) Maximum number of VxVM trace channels available for vxtrace commands. This tunable requires a system reboot to take effect. |
| volpagemod_max_memsz | (Veritas Volume Manager) Maximum paging module memory used by Instant Snapshots (Kbytes). |
| volraid_rsrtransmax | (Veritas Volume Manager) Maximum number of VxVM RAID-5 transient reconstruct operations in parallel. This tunable requires a system reboot to take effect. |
| vxfs_mbuf | (Veritas File System) Maximum memory used for VxFS buffer cache. This tunable requires a system reboot to take effect. |
| vxfs_ninode | (Veritas File System) Number of entries in the VxFS inode table. This tunable requires a system reboot to take effect. |
| write_nstream | (Veritas File System) The number of parallel write requests of size write_pref_io that can be outstanding at one time. The installer can only set the system default value of write_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |

Table E-1 Supported tunable parameters (*continued*)

| Tunable | Description |
|---------------|--|
| write_pref_io | (Veritas File System) The preferred write request size. The installer can only set the system default value of write_pref_io. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device. |

Configuration files

This appendix includes the following topics:

- [About sample main.cf files](#)
- [Sample main.cf files for Sybase ASE CE configurations](#)

About sample main.cf files

You can examine the VCS configuration file, main.cf, to verify the SF Sybase CE installation and configuration.

- The main.cf file is located in the folder /etc/VRTSvcs/conf/config.
- After an SF Sybase CE installation, several sample main.cf file types can be viewed in the following directory: /etc/VRTSagents/ha/conf/Sybase
- All sample configurations assume that the Veritas High Availability Agent for Sybase binaries are installed on local disks and that they are managed by the operating system. These file systems must be specified in the file /etc/vfstab
- For the following configuration samples, please note the "cluster" definition in all of the configurations should specify UseFence=SCSI3.

Sample main.cf files for Sybase ASE CE configurations

Sample main.cf file examples are provided for the following Sybase ASE CE configurations:

- Basic cluster configuration
 - With shared mount point on CFS for Sybase binary installation
 - With local mount point on VxFS for Sybase binary installation
- Replicating data between two clusters

- For a primary site in a CVM VVR configuration
- For a secondary site in a CVM VVR configuration

Sample main.cf for a basic Sybase ASE CE cluster configuration under VCS control with shared mount point on CFS for Sybase binary installation

This sample main.cf is for a single site with a basic cluster configuration with shared mount point on CFS for Sybase binary installation.

The following are the configuration details for this Sybase ASE CE configuration sample main.cf:

- File name: sybasece_cfs_main.cf
- File location: /etc/VRTSagents/ha/conf/Sybase/

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "SybaseTypes.cf"

cluster clus1 (
    UserNames = { admin = HopHojOlpKppNxpJom }
    Administrators = { admin }
    HacliUserLevel = COMMANDROOT
    UseFence=SCSI3
)

system system1 (
)

system system2 (
)

// binmounts group for configuring CFS mounts for Sybase binaries.

group binmnt (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    AutoStartList = { system1, system2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)
```



```
CFSMount sybbin_dg_sybbin_vol_mnt (
    MountPoint = "/sybase"
    BlockDevice = "/dev/vx/dsk/sybbin_dg/sybbin_vol"
)

CVMVolDg sybbin_dg_voldg (
    CVMDiskGroup = sybbin_dg
    CVMVolume = { sybbin_vol }
    CVMActivation = sw
)

requires group cvm online local firm
sybbin_dg_sybbin_vol_mnt requires sybbin_dg_voldg

// resource dependency tree
//
// group binmnt
// {
//   CFSMount sybbin_dg_sybbin_vol_mnt
//   {
//     CVMVolDg sybbin_dg_voldg
//   }
// }

// cvm group for CVM and CFS specific agents.

group cvm (
    SystemList = { system1 = 0, system2 = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { system1, system2 }
)

CFSfsckd vxfsckd (
)

CVMCluster cvm_clus (
    CVMClustName = sfsyb_90
    CVMNodeId = { system1 = 0, system2 = 1 }
    CVMTransport = gab
    CVMTimeout = 200
```

```

    )

CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
)

ProcessOnOnly vxattachd (
    Critical = 0
    PathName = "/bin/sh"
    Arguments = "- /usr/lib/vxvm/bin/vxattachd root"
    RestartLimit = 3
)

cvm_clus requires cvm_vxconfigd
vxfsckd requires cvm_clus

// resource dependency tree
//
// group cvm
// {
//   CFSfsckd vxfsckd
//   {
//     CVMCluster cvm_clus
//     {
//       CVMVxconfigd cvm_vxconfigd
//     }
//   }
// }

// sybasece group for:
// 1. CVM volumes for Sybase database and quorum device
// 2. CFS mount for Sybase database and quorum device
// 3. Process agent for vxfsend process.
// 4. Sybase database instance.

group sybasece (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    AutoStartList = { system1, system2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120

```

```

)

CFSMount quorum_dg_quorum_vol_mnt (
    MountPoint = "/quorum"
    BlockDevice = "/dev/vx/dsk/quorum_dg/quorum_vol"
)

CFSMount dbdata_dg_sybvol_mnt (
    MountPoint = "/sybdata"
    BlockDevice = "/dev/vx/dsk/dbdata_dg/sybvol"
)

CVMVolDg quorum_dg_voldg (
    CVMDiskGroup = quorum_dg
    CVMVolume = { quorum_vol }
    CVMActivation = sw
)

CVMVolDg dbdata_dg_voldg (
    CVMDiskGroup = dbdata_dg
    CVMVolume = { sybvol }
    CVMActivation = sw
)

Process vxfsend (
    PathName = "/sbin/vxfsend"
    Arguments = "-m sybase -k /tmp/vcmp_socket"
)

Sybase ase (
    Server @system1 = ase1
    Server @system2 = ase2
    Owner = sybase
    Home = "/sybase"
    Version = 15
    SA = sa
    Quorum_dev = "/quorum/q.dat"
)

requires group binmnt online local firm
ase requires quorum_dg_quorum_vol_mnt
ase requires dbdata_dg_sybvol_mnt
ase requires vxfsend

```

```
quorum_dg_quorum_vol_mnt requires quorum_dg_voldg
dbdata_dg_sybvol_mnt requires dbdata_dg_voldg

// resource dependency tree
//
// group sybasece
// {
//   Sybase ase
//   {
//     CFSMount quorum_dg_quorum_vol_mnt
//     {
//       CVMVolDg quorum_dg_voldg
//     }
//     CFSMount dbdata_dg_sybvol_mnt
//     {
//       CVMVolDg dbdata_dg_voldg
//     }
//     Process vxfend
//   }
// }
```

Sample main.cf for a basic Sybase ASE CE cluster configuration with local mount point on VxFS for Sybase binary installation

This sample main.cf is for a single site with a basic cluster configuration with local mount point on VxFS for Sybase binary installation.

The following are the configuration details for this Sybase ASE CE configuration sample main.cf:

- File name: sybasece_vxfs_main.cf
- File location: /etc/VRTSagents/ha/conf/Sybase/

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "SybaseTypes.cf"

cluster clus1 (
    UserNames = { admin = HopHojOlpKppNxpJom }
    Administrators = { admin }
```

```

    HacliUserLevel = COMMANDROOT
    UseFence=SCSI3
)

system system1 (
)

system system2 (
)

// binmounts group for configuring VxFS mounts for Sybase binaries.

group binlocalmnt (
    SystemList = { system1 = 0, system2 = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { system1, system2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

DiskGroup sybbin_dg_voldg (
    DiskGroup = sybbindg
)

Mount sybbin_dg_sybbin_vol_mnt (
    MountPoint = "/sybase"
    BlockDevice = "/dev/vx/dsk/sybbin_dg/sybbin_vol"
    FSType = vxfs
    FsckOpt = "-y"
)

Volume sybbin_dg_vol (
    DiskGroup = sybbindg
    Volume = sybbin_vol
)

requires group cvm online local firm
sybbin_dg_sybbin_vol_mnt requires sybbin_dg_vol
sybbin_dg_vol requires sybbin_dg_voldgdg

// resource dependency tree

```

```
//  
// group binlocalmnt  
// {  
// Mount sybbin_dg_sybbin_vol_mnt  
//     {  
//         Volume sybbindg_vol  
//             {  
//                 DiskGroup sybbin_dg_voldg  
//             }  
//     }  
// }  
  
// cvm group for CVM and CFS specific agents.  
  
group cvm (  
    SystemList = { system1 = 0, system2 = 1 }  
    AutoFailOver = 0  
    Parallel = 1  
    AutoStartList = { system1, system2 }  
)  
  
CFSfsckd vxfsckd (  
    )  
  
CVMCluster cvm_clus (  
    CVMClustName = clus1  
    CVMNodeId = { system1 = 0, system2 = 1 }  
    CVMTransport = gab  
    CVMTimeout = 200  
)  
  
CVMVxconfigd cvm_vxconfigd (  
    Critical = 0  
    CVMVxconfigdArgs = { syslog }  
)  
  
ProcessOnOnly vxattachd (  
    Critical = 0  
    PathName = "/bin/sh"  
    Arguments = "- /usr/lib/vxvm/bin/vxattachd root"  
    RestartLimit = 3  
)
```

```
cvm_clus requires cvm_vxconfigd
vxfsckd requires cvm_clus

// resource dependency tree
//
// group cvm
// {
//   CFSfsckd vxfsckd
//   {
//     CVMCluster cvm_clus
//     {
//       CVMVxconfigd cvm_vxconfigd
//     }
//   }
// }

// sybasece group for:
// 1. CVM volumes for Sybase database and quorum device
// 2. CFS mount for Sybase database and quorum device
// 3. Process agent for vxfsck process.
// 4. Sybase database instance.

group sybasece (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    AutoStartList = { system1, system2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

CFSMount quorum_dg_quorum_vol_mnt (
    MountPoint = "/quorum"
    BlockDevice = "/dev/vx/dsk/quorum_dg/quorum_vol"
)

CFSMount dbdata_dg_sybvool_mnt (
    MountPoint = "/sybdata"
    BlockDevice = "/dev/vx/dsk/dbdata_dg/sybvool"
)

CVMVolDg quorum_dg_voldg (
    CVMDiskGroup = quorum_dg
```

```

    CVMVolume = { quorum_vol }
    CVMActivation = sw
)

CVMVolDg dbdata_dg_voldg (
    CVMDiskGroup = dbdata_dg
    CVMVolume = { sybvol }
    CVMActivation = sw
)

Process vxfend (
    PathName = "/sbin/vxfend"
    Arguments = "-m sybase -k /tmp/vcmp_socket"
)

Sybase ase (
    Server @system1 = ase1
    Server @system2 = ase2
    Owner = sybase
    Home = "/sybase"
    Version = 15
    SA = sa
    Quorum_dev = "/quorum/q.dat"
)

requires group binlocalmnt online local firm
ase requires quorum_dg_quorum_vol_mnt
ase requires dbdata_dg_sybvol_mnt
ase requires vxfend
quorum_dg_quorum_vol_mnt requires quorum_dg_voldg
dbdata_dg_sybvol_mnt requires dbdata_dg_voldg

// resource dependency tree
//
// group sybasece
// {
// Sybase ase
//   {
//     CFSSMount quorum_dg_quorum_vol_mnt
//       {
//         CVMVolDg quorum_dg_voldg
//       }
//     }
// }

```



```
//      CFSSMount dbdata_dg_sybvol_mnt
//      {
//          CVMVolDg dbdata_dg_voldg
//      }
//      Process vxfend
//      }
// }
```

Sample main.cf for a primary CVM VVR site

This sample main.cf is for a primary site in a CVM VVR configuration. It is one of two sample main.cfs for replicating data between two clusters.

The following are the configuration details for this Sybase ASE CE configuration sample main.cf:

- File name: sybasece_cvmvvr_primary_main.cf
- File location: /etc/VRTSagents/ha/conf/Sybase

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTTypes.cf"
include "SybaseTypes.cf"

cluster clus1 (
    UserNames = { admin = HopHojOlpKppNxpJom }
    ClusterAddress = "10.180.88.188"
    Administrators = { admin }
    HacliUserLevel = COMMANDROOT
    UseFence=SCSI3
)

remoteclass clus2 (
    ClusterAddress = "10.190.99.199"
)

heartbeat Icmp (
    ClusterList = { clus2 }
    Arguments @clus2 = { "10.190.99.199" }

)

system system1 (
```

```

)

system system2 (
)

group ClusterService (
    SystemList = { system1 = 0, system2 = 1 }
    AutoStartList = { system1, system2 }
    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 = eth0
    Address = "10.180.88.188"
    NetMask = "255.255.255.0"
)

NIC csgnic (
    Device = eth0
)

gcoip requires csgnic
wac requires gcoip

// resource dependency tree
//
//     group ClusterService
//     {
//     Application wac
//     {
//         IP gcoip
//         {
//             NIC csgnic

```

```

//          }
//          }
//          }

group RVGgroup (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    AutoStartList = { system1, system2 }
)

CVMVolDg dbdata_voldg (
    CVMDiskGroup = dbdata_dg
    CVMActivation = sw
)

RVGShared dbdata_rvg (
    RVG = syb_rvg
    DiskGroup = dbdata_dg
)

requires group binmnt online local firm
dbdata_rvg requires dbdata_voldg

group binmnt (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    AutoStartList = { system1, system2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

CFSMount sybbin_dg_sybbin_vol_mnt (
    MountPoint = "/sybase"
    BlockDevice = "/dev/vx/dsk/sybbin_dg/sybbin_vol"
)

CVMVolDg sybbin_dg_voldg (
    CVMDiskGroup = sybbin_dg
    CVMVolume = { sybbin_vol }
    CVMActivation = sw
)

```

```

requires group cvm online local firm
sybbin_dg_sybbin_vol_mnt requires sybbin_dg_voldg

group cvm (
    SystemList = { system1 = 0, system2 = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { system1, system2 }
)

CFSfsckd vxfsckd (
)

CVMCluster cvm_clus (
    CVMClustName = clus1
    CVMNodeId = { system1 = 0, system2 = 1 }
    CVMTransport = gab
    CVMTimeout = 200
)

CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
)

ProcessOnOnly vxattachd (
    Critical = 0
    PathName = "/bin/sh"
    Arguments = "- /usr/lib/vxvm/bin/vxattachd root"
    RestartLimit = 3
)

cvm_clus requires cvm_vxconfigd
vxfsckd requires cvm_clus

// resource dependency tree
//
//     group cvm
//     {
//     CFSfsckd vxfsckd
//     {

```

```

//          CVMCluster cvm_clus
//          {
//          CVMVxconfigd cvm_vxconfigd
//          }
//          }
//          }

group logowner (
    SystemList = { system1 = 0, system2 = 1 }
    AutoStartList = { system1, system2 }
)

IP logowner_ip (
    Device = eth0
    Address = "10.10.9.101"
    NetMask = "255.255.255.0"
)

NIC nic (
    Device = eth0
)

RVGLogowner rvg_logowner (
    RVG = syb_rvg
    DiskGroup = dbdata_dg
)

requires group RVGgroup online local firm
logowner requires logowner_ip
logowner_ip requires nic

// resource dependency tree
//
//      group logowner
//      {
//      RVGLogowner rvg_logowner
//      {
//      IP logowner_ip
//      {
//      NIC nic
//      }
//      }
//      }

```

```
//          }
//          }

group sybasece (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    ClusterList = { clus1 = 0, clus2 = 1 }
    AutoStartList = { system1, system2 }
    ClusterFailOverPolicy = Manual
    Authority = 1
    OnlineRetryLimit = 3
    TriggerResStateChange = 1
    OnlineRetryInterval = 120
)

CFSMount quorum_dg_quorum_vol_mnt (
    MountPoint = "/quorum"
    BlockDevice = "/dev/vx/dsk/quorum_dg/quorum_vol"
)

CFSMount dbdata_dg_sybvool_mnt (
    MountPoint = "/sybdata"
    BlockDevice = "/dev/vx/dsk/dbdata_dg/sybvool"
)

CVMVolDg quorum_dg_voldg (
    CVMDiskGroup = quorum_dg
    CVMVolume = { quorum_vol }
    CVMActivation = sw
)

Process vx fend (
    PathName = "/sbin/vxfend"
    Arguments = "-m sybase -k /tmp/vcmp_socket"
)

RVGSharedPri syb_vvr_shpri (
    RvgResourceName = dbdata_rvg
    OnlineRetryLimit = 0
)

Sybase ase (
    Server @system1 = ase1
```

```
Server @system2 = ase2
Owner = sybase
Home = "/sybase"
Version = 15
SA = sa
Quorum_dev = "/quorum/q.dat"
)

requires group RVGgroup online local firm
dbdata_dg_sybvol_mnt requires syb_vvr_shpri
ase requires vxfsend
ase requires dbdata_dg_sybvol_mnt
ase requires quorum_dg_quorum_vol_mnt
quorum_dg_quorum_vol_mnt requires quorum_dg_voldg

// resource dependency tree
//
//   group sybasece
//   {
//   Sybase ase
//   {
//   CFSMount dbdata_dg_sybvol_mnt
//   {
//   RVGSharedPri syb_vvr_shpri
//   }
//   Process vxfsend
//   CFSMount quorum_dg_quorum_vol_mnt
//   {
//   CVMVolDg quorum_dg_voldg
//   }
//   }
//   }
```

Sample main.cf for a secondary CVM VVR site

This sample main.cf is for a secondary site in a CVM VVR configuration. It is the second of two sample main.cfs for replicating data between two clusters.

The following are the configuration details for this Sybase ASE CE configuration sample main.cf:

- File name: sybasece_cvmvvr_secondary_main.cf
- File location: /etc/VRTSagents/ha/conf/Sybase

This is main.cf for CVM VVR configuration on Secondary site.

```

-----

include "types.cf"
include "CFSTypes.cf"
include "CVMTTypes.cf"
include "SybaseTypes.cf"

cluster clus2 (
    UserNames = { admin = HopHojOlpKppNxpJom }
    ClusterAddress = "10.190.99.199"
    Administrators = { admin }
    HacliUserLevel = COMMANDROOT
    UseFence=SCSI3
)

remoteclass clus1 (
    ClusterAddress = "10.180.88.188"
)

heartbeat Icmp (
    ClusterList = { clus1 }
    Arguments @clus1 = { "10.180.88.188" }
)

system system3 (
)

system system4 (
)

group ClusterService (
    SystemList = { system3 = 0, system4 = 1 }
    AutoStartList = { system3, system4 }
    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 = eth0
        Address = "10.190.99.199"
        NetMask = "255.255.255.0"
    )

    NIC csgnic (
        Device = eth0
    )

    gcoip requires csgnic
    wac requires gcoip

// resource dependency tree
//
// group ClusterService
// {
//   Application wac
//   {
//     IP gcoip
//     {
//       NIC csgnic
//     }
//   }
// }

group RVGgroup (
    SystemList = { system3 = 0, system4 = 1 }
    Parallel = 1
    AutoStartList = { system3, system4 }
)

CVMVolDg dbdata_voldg (
    CVMDiskGroup = dbdata_dg
    CVMActivation = sw
)

RVGShared dbdata_rvg (
    RVG = syb_rvg
    DiskGroup = dbdata_dg
```

```

    )

requires group binmnt online local firm
dbdata_rvg requires dbdata_voldg

group binmnt (
    SystemList = { system3 = 0, system4 = 1 }
    Parallel = 1
    AutoStartList = { system3, system4 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

CFSMount sybbin_dg_sybbin_vol_mnt (
    MountPoint = "/sybase"
    BlockDevice = "/dev/vx/dsk/sybbin_dg/sybbin_vol"
)

CVMVolDg sybbin_dg_voldg (
    CVMDiskGroup = sybbin_dg
    CVMVolume = { sybbin_vol }
    CVMActivation = sw
)

requires group cvm online local firm
sybbin_dg_sybbin_vol_mnt requires sybbin_dg_voldg

group cvm (
    SystemList = { system3 = 0, system4 = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { system3, system4 }
)

CFSfsckd vxfsckd (
)

CVMCluster cvm_clus (
    CVMClustName = clus2
    CVMNodeId = { system3 = 0, system4 = 1 }
    CVMTransport = gab
    CVMTimeout = 200
)

```

```

CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
)

cvm_clus requires cvm_vxconfigd
vxfsckd requires cvm_clus

// resource dependency tree
//
//     group cvm
//     {
//     CFSfsckd vxfsckd
//         {
//             CVMCluster cvm_clus
//                 {
//                     CVMVxconfigd cvm_vxconfigd
//                 }
//         }
//     }

group logowner (
    SystemList = { system3 = 0, system4 = 1 }
    AutoStartList = { system3, system4 }
)

IP logowner_ip (
    Device = eth0
    Address = "10.11.9.102"
    NetMask = "255.255.255.0"
)

NIC nic (
    Device = eth0
)

RVGLogowner rvg_logowner (
    RVG = syb_rvg
    DiskGroup = dbdata_dg
)

requires group RVGgroup online local firm

```

```
logowner requires logowner_ip
logowner_ip requires nic

// resource dependency tree
//
// group logowner
// {
//   RVGLogowner rvg_logowner
//   {
//     IP logowner_ip
//     {
//       NIC nic
//     }
//   }
// }

group sybasece (
    SystemList = { system3 = 0, system4 = 1 }
    Parallel = 1
    ClusterList = { clus2 = 0, clus1 = 1 }
    AutoStartList = { system3, system4 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
)

CFSMount quorum_dg_quorum_vol_mnt (
    MountPoint = "/quorum"
    BlockDevice = "/dev/vx/dsk/quorum_dg/quorum_vol"
)

CVMVolDg quorum_dg_voldg (
    CVMDiskGroup = quorum_dg
    CVMVolume = { quorum_vol }
    CVMActivation = sw
)

CFSMount dbdata_dg_sybvol_mnt (
    MountPoint = "/sybdata"
    BlockDevice = "/dev/vx/dsk/dbdata_dg/sybvol"
)

Process vxfend (
```

```

        PathName = "/sbin/vxfend"
        Arguments = "-m sybase -k /tmp/vcmp_socket"
    )

    RVGSharedPri syb_vvr_shpri (
        RvgResourceName = dbdata_rvg
        OnlineRetryLimit = 0
    )

    Sybase ase (
        Server @system3 = ase1
        Server @system4 = ase2
        Owner = sybase
        Home = "/sybase"
        Version = 15
        SA = sa
        Quorum_dev = "/quorum/q.dat"
    )

requires group RVGgroup online local firm
dbdata_dg_sybvol_mnt requires syb_vvr_shpri
ase requires vxfend
ase requires dbdata_dg_sybvol_mnt
ase requires quorum_dg_quorum_vol_mnt
quorum_dg_quorum_vol_mnt requires quorum_dg_voldg

```

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

- [About configuring secure shell or remote shell communication modes before installing products](#)

About configuring secure shell or remote shell communication modes before installing products

Establishing communication between nodes is required to install Symantec software from a remote system, or to install and configure a system. The system from which the installer is run must have permissions to run `rsh` (remote shell) or `ssh` (secure shell) utilities. You need to run the installer with superuser privileges on the systems where you plan to install Symantec software.

Establishing communication between nodes is required to install Symantec software from a remote system, or to install and configure a cluster. The node from which the installer is run must have permissions to run `rsh` (remote shell) or `ssh` (secure shell) utilities. You need to run the installer with superuser privileges on the systems where you plan to install Symantec software.

You can install products to remote systems using either secure shell (`ssh`) or remote shell (`rsh`). Symantec recommends that you use `ssh` as it is more secure than `rsh`.

Note: When installing on an RHEL5 / OEL5 system with SELinux enabled, only `ssh` is supported due to RedHat's SELinux policy restrictions.

You can set up ssh and rsh connections in many ways.

- You can manually set up the SSH and RSH connection with UNIX shell commands.
- You can run the `installmr -comsetup` command to interactively set up SSH and RSH connection.
- You can run the password utility, `pwdutil.pl`.

This section contains an example of how to set up ssh password free communication. The example sets up ssh between a source system (sys1) that contains the installation directories, and a target system (sys2). This procedure also applies to multiple target systems.

Note: The script based installer supports establishing passwordless communication for you.

Manually configuring passwordless ssh

The ssh program enables you to log into and execute commands on a remote system. ssh enables encrypted communications and an authentication process between two untrusted hosts over an insecure network.

In this procedure, you first create a DSA key pair. From the key pair, you append the public key from the source system to the `authorized_keys` file on the target systems.

If you are installing Oracle, you must configure a DSA key and an RSA key for the Oracle user in addition to the DSA key required for the root user to install SF Oracle RAC.

Read the ssh documentation and online manual pages before enabling ssh. Contact your operating system support provider for issues regarding ssh configuration.

Visit the OpenSSH website that is located at: <http://openssh.org> to access online manuals and other resources.

To create the DSA key pair

- 1 On the source system (sys1), log in as root, and navigate to the root directory.

```
sys1 # cd /root
```

- 2 To generate a DSA key pair on the source system, type the following command:

```
sys1 # 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 (/root/.ssh/id_dsa):
```

- 3 Press Enter to accept the default location of `/root/.ssh/id_dsa`.
- 4 When the program asks you to enter the passphrase, press the Enter key twice.

```
Enter passphrase (empty for no passphrase):
```

Do not enter a passphrase. Press Enter.

```
Enter same passphrase again:
```

Press Enter again.

- 5 Output similar to the following lines appears.

```
Your identification has been saved in /root/.ssh/id_dsa.  
Your public key has been saved in /root/.ssh/id_dsa.pub.  
The key fingerprint is:  
1f:00:e0:c2:9b:4e:29:b4:0b:6e:08:f8:50:de:48:d2 root@sys1
```


To append the public key from the source system to the `authorized_keys` file on the target system, using secure file transfer

- 1 From the source system (sys1), move the public key to a temporary file on the target system (sys2).

Use the secure file transfer program.

In this example, the file name `id_dsa.pub` in the root directory is the name for the temporary file for the public key.

Use the following command for secure file transfer:

```
sys1 # sftp sys2
```

If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

```
Connecting to sys2 ...
The authenticity of host 'sys2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

- 2 Enter `yes`.

Output similar to the following is displayed:

```
Warning: Permanently added 'sys2,10.182.00.00'
(DSA) to the list of known hosts.
root@sys2 password:
```

- 3 Enter the root password of sys2.
- 4 At the `sftp` prompt, type the following command:

```
sftp> put /root/.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /root/.ssh/id_dsa.pub to /root/id_dsa.pub
```

- 5 To quit the SFTP session, type the following command:

```
sftp> quit
```

- 6 Add the `id_dsa.pub` keys to the `authorized_keys` file on the target system. To begin the `ssh` session on the target system (`sys2` in this example), type the following command on `sys1`:

```
sys1 # ssh sys2
```

Enter the root password of `sys2` at the prompt:

```
password:
```

Type the following commands on `sys2`:

```
sys2 # cat /root/id_dsa.pub >> /root/.ssh/authorized_keys
sys2 # rm /root/id_dsa.pub
```

- 7 Run the following commands on the source installation system. If your `ssh` session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and make the key globally available to the user `root`:

```
sys1 # exec /usr/bin/ssh-agent $SHELL
sys1 # ssh-add
```

```
Identity added: /root/.ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

To verify that you can connect to a target system

- 1 On the source system (`sys1`), enter the following command:

```
sys1 # ssh -l root sys2 uname -a
```

where `sys2` is the name of the target system.

- 2 The command should execute from the source system (`sys1`) to the target system (`sys2`) without the system requesting a passphrase or password.
- 3 Repeat this procedure for each target system.

Setting up `ssh` and `rsh` connection using the `installer -comsetup` command

You can interactively set up the `ssh` and `rsh` connections using the `installer -comsetup` command.

Enter the following:

```
# ./installmr -comsetup
```

```
Input the name of the systems to set up communication:  
Enter the Solaris 10 Sparc system names separated by spaces:  
[q,?] sys2  
Set up communication for the system sys2:
```

```
Checking communication on sys2 ..... Failed
```

```
CPI ERROR V-9-20-1303 ssh permission was denied on sys2. rsh  
permission was denied on sys2. Either ssh or rsh is required  
to be set up and ensure that it is working properly between the local  
node and sys2 for communication
```

```
Either ssh or rsh needs to be set up between the local system and  
sys2 for communication
```

```
Would you like the installer to setup ssh or rsh communication  
automatically between the systems?
```

```
Superuser passwords for the systems will be asked. [y,n,q,?] (y) y
```

```
Enter the superuser password for system sys2:
```

- 1) Setup ssh between the systems
- 2) Setup rsh between the systems
- b) Back to previous menu

```
Select the communication method [1-2,b,q,?] (1) 1
```

```
Setting up communication between systems. Please wait.  
Re-verifying systems.
```

```
Checking communication on sys2 ..... Done
```

```
Successfully set up communication for the system sys2
```

Setting up ssh and rsh connection using the pwdutil.pl utility

The password utility, `pwdutil.pl`, is bundled in the 6.2 release under the `scripts` directory. The users can run the utility in their script to set up the ssh and rsh connection automatically.

```
# ./pwdutil.pl -h
```

Usage:

Command syntax with simple format:

```
pwdutil.pl check|configure|unconfigure ssh|rsh <hostname|IP addr>
[<user>] [<password>] [<port>]
```

Command syntax with advanced format:

```
pwdutil.pl [--action|-a 'check|configure|unconfigure']
           [--type|-t 'ssh|rsh']
           [--user|-u '<user>']
           [--password|-p '<password>']
           [--port|-P '<port>']
           [--hostfile|-f '<hostfile>']
           [--keyfile|-k '<keyfile>']
           [-debug|-d]
           <host_URI>
```

```
pwdutil.pl -h | -?
```

Table G-1 Options with pwdutil.pl utility

| Option | Usage |
|---|---|
| --action -a 'check configure unconfigure' | Specifies action type, default is 'check'. |
| --type -t 'ssh rsh' | Specifies connection type, default is 'ssh'. |
| --user -u '<user>' | Specifies user id, default is the local user id. |
| --password -p '<password>' | Specifies user password, default is the user id. |
| --port -P '<port>' | Specifies port number for ssh connection, default is 22 |
| --keyfile -k '<keyfile>' | Specifies the private key file. |
| --hostfile -f '<hostfile>' | Specifies the file which list the hosts. |
| -debug | Prints debug information. |
| -h -? | Prints help messages. |

Table G-1 Options with `pwdutil.pl` utility (*continued*)

| Option | Usage |
|-------------------------------|---|
| <code><host_URI></code> | Can be in the following formats: <code><hostname></code> <code><user>:<password>@<hostname></code> <code><user>:<password>@<hostname>:</code> <code><port></code> |

You can check, configure, and unconfigure ssh or rsh using the `pwdutil.pl` utility. For example:

- To check ssh connection for only one host:


```
pwdutil.pl check ssh hostname
```
- To configure ssh for only one host:


```
pwdutil.pl configure ssh hostname user password
```
- To unconfigure rsh for only one host:


```
pwdutil.pl unconfigure rsh hostname
```
- To configure ssh for multiple hosts with same user ID and password:


```
pwdutil.pl -a configure -t ssh -u user -p password hostname1
hostname2 hostname3
```
- To configure ssh or rsh for different hosts with different user ID and password:


```
pwdutil.pl -a configure -t ssh user1:password1@hostname1
user2:password2@hostname2
```
- To check or configure ssh or rsh for multiple hosts with one configuration file:


```
pwdutil.pl -a configure -t ssh --hostfile /tmp/sshrsh_hostfile
```
- To keep the host configuration file secret, you can use the 3rd party utility to encrypt and decrypt the host file with password.
For example:

```

### run openssl to encrypt the host file in base64 format
# openssl aes-256-cbc -a -salt -in /hostfile -out /hostfile.enc
enter aes-256-cbc encryption password: <password>
Verifying - enter aes-256-cbc encryption password: <password>

### remove the original plain text file
# rm /hostfile

### run openssl to decrypt the encrypted host file
# pwduutil.pl -a configure -t ssh `openssl aes-256-cbc -d -a
-in /hostfile.enc`
enter aes-256-cbc decryption password: <password>

```

- To use the ssh authentication keys which are not under the default `$HOME/.ssh` directory, you can use `--keyfile` option to specify the ssh keys. For example:

```

### create a directory to host the key pairs:
# mkdir /keystore

### generate private and public key pair under the directory:
# ssh-keygen -t rsa -f /keystore/id_rsa

### setup ssh connection with the new generated key pair under
the directory:
# pwduutil.pl -a configure -t ssh --keyfile /keystore/id_rsa
user:password@hostname

```

You can see the contents of the configuration file by using the following command:

```

# cat /tmp/sshrsh_hostfile
user1:password1@hostname1
user2:password2@hostname2
user3:password3@hostname3
user4:password4@hostname4

# all default: check ssh connection with local user
hostname5
The following exit values are returned:

0    Successful completion.
1    Command syntax error.
2    Ssh or rsh binaries do not exist.
3    Ssh or rsh service is down on the remote machine.

```

```

4      Ssh or rsh command execution is denied due to password is required.
5      Invalid password is provided.
255   Other unknown error.

```

Restarting the ssh session

After you complete this procedure, ssh can be restarted in any of the following scenarios:

- After a terminal session is closed
- After a new terminal session is opened
- After a system is restarted
- After too much time has elapsed, to refresh ssh

To restart ssh

- 1 On the source installation system (sys1), bring the private key into the shell environment.

```
sys1 # exec /usr/bin/ssh-agent $SHELL
```

- 2 Make the key globally available for the user `root`

```
sys1 # ssh-add
```

Enabling rsh for Linux

The following section describes how to enable remote shell.

Symantec recommends configuring a secure shell environment for Symantec product installations.

See [“Manually configuring passwordless ssh”](#) on page 423.

See the operating system documentation for more information on configuring remote shell.

To enable rsh for rhel6

- 1 To ensure that the `rsh` and `rsh-server` RPMs are installed, type the following command:

```
# rpm -qa | grep -i rsh
```

If it is not already in the file, type the following command to append the line "rsh" to the `/etc/securetty` file:

```
# echo "rsh" >> /etc/securetty
```

- 2 Modify the line `disable = no` in the `/etc/xinetd.d/rsh` file.
- 3 In the `/etc/pam.d/rsh` file, change the "auth" type from "required" to "sufficient":

```
auth    sufficient
```

- 4 Add the "promiscuous" flag into `/etc/pam.d/rsh` and `/etc/pam.d/rlogin` after item "pam_rhosts_auth.so".

- 5 To enable the rsh server, type the following command:

```
# chkconfig rsh on
```

- 6 Modify the `.rhosts` file. Each line of the `.rhosts` file contains a fully qualified domain name or IP address for each remote system. This file also contains the name of a user having access to the local system. For example, if the root user must remotely access `sys1` from `sys2`, add an entry for `sys2.companyname.com` to the `.rhosts` file on `sys1` by typing the following command:

```
# echo "sys2.companyname.com" >> $HOME/.rhosts
```

- 7 Install the Symantec product.

To disable rsh for rhel6/sles

- 1 Remove the "rsh" entry in the `/etc/securetty` file.
- 2 Disable the rsh server by typing the following command:

```
# chkconfig rsh off
```

- 3 After you complete an installation procedure, delete the `.rhosts` file from each user's `$HOME` directory to ensure security:

```
# rm -f $HOME/.rhosts
```

To enable rsh for rhel7

- ◆ Run the following commands to enable rsh passwordless connection:

```
# systemctl start rsh.socket  
# systemctl start rlogin.socket  
# systemctl enable rsh.socket  
# systemctl enable rlogin.socket  
# echo rsh >> /etc/securetty  
# echo rlogin >> /etc/securetty  
#echo "+ +" >> /root/.rhosts
```

To disable rsh for rhel7

- ◆ Run the following commands to disable rsh passwordless connection:

```
# systemctl stop rsh.socket  
# systemctl stop rlogin.socket  
# systemctl disable rsh.socket  
# systemctl disable rlogin.socket
```

High availability agent information

This appendix includes the following topics:

- [About agents](#)
- [CVMCluster agent](#)
- [CVMVxconfigd agent](#)
- [CVMVolDg agent](#)
- [CFSMount agent](#)
- [Process agent](#)
- [Monitoring options for the Sybase agent](#)
- [Sybase resource type](#)

About agents

An agent is defined as a process that starts, stops, and monitors all configured resources of a type, and reports their status to Symantec Cluster Server (VCS). Agents have both entry points and attributes. Entry points are also known as agent functions and are referred to as "agent functions" throughout the document.

Attributes contain data about the agent. An attribute has a definition and a value. You change attribute values to configure resources, which are defined as the individual components that work together to provide application services to the public network. For example, a resource may be a physical component such as a disk or a network interface card, a software component such as Oracle or a web server, or a configuration component such as an IP address or mounted file system.

Attributes are either optional or required, although sometimes the attributes that are optional in one configuration may be required in other configurations. Many optional attributes have predefined or default values, which you should change as required. A variety of internal use only attributes also exist. Do not modify these attributes—modifying them can lead to significant problems for your clusters. Attributes have type and dimension. Some attribute values can accept numbers, others can accept alphanumeric values or groups of alphanumeric values, while others are simple boolean on/off values.

The entry points and attributes for each SF Sybase CE agent are described in this appendix.

VCS agents included within SF Sybase CE

SF Sybase CE includes the following VCS agents:

- CVMCluster agent
- CVMVxconfigd agent
- CVMVolDg agent
- CFSSMount agent
- CFSfsckd
- Coordination Point agent

An SF Sybase CE installation automatically configures the CVMCluster resource and the CVMVxconfigd resource.

You must configure the CVMVolDg agent for each disk group that is used by an SF Sybase CE service group. Configure a disk group for only a single SF Sybase CE service group. If the database uses cluster file systems, configure the CFSSMount agent for each volume in the disk group.

You must configure the CVMVolDg agent for each shared disk group. If the database uses cluster file systems, configure the CFSSMount agent for each volume in the disk group.

Use the information in this appendix about the entry points and attributes of the listed agents to make necessary configuration changes. For information on how to modify the VCS configuration:

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

VCS agent for Sybase included within SF Sybase CE

SFHA includes an additional agent for Sybase.

See the *Symantec Cluster Server Agent for Oracle Installation and Configuration Guide* for more information on the Sybase agent.

CVMCluster agent

The CVMCluster agent controls system membership on the cluster port that is associated with Veritas Volume Manager (VxVM).

The CVMCluster agent performs the following functions:

- Joins a node to the CVM cluster port.
- Removes a node from the CVM cluster port.
- Monitors the node's cluster membership state.

Entry points for CVMCluster agent

[Table H-1](#) describes the entry points used by the CVMCluster agent.

Table H-1 CVMCluster agent entry points

| Entry Point | Description |
|-------------|---|
| Online | Joins a node to the CVM cluster port. Enables the Volume Manager cluster functionality by automatically importing the shared disk groups. |
| Offline | Removes a node from the CVM cluster port. |
| Monitor | Monitors the node's CVM cluster membership state. |

Attribute definition for CVMCluster agent

[Table H-2](#) describes the user-modifiable attributes of the CVMCluster resource type.

Table H-2 CVMCluster agent attributes

| Attribute | Description |
|--------------|---|
| CVMClustName | Name of the cluster. <ul style="list-style-type: none"> ■ Type and dimension: string-scalar |
| CVMNodeAddr | List of host names and IP addresses. <ul style="list-style-type: none"> ■ Type and dimension: string-association |

Table H-2 CVMCluster agent attributes (continued)

| Attribute | Description |
|--------------|---|
| CVMNodeId | <p>Associative list. The first part names the system; the second part contains the LLT ID number for the system.</p> <ul style="list-style-type: none"> Type and dimension: string-association |
| CVMTransport | <p>Specifies the cluster messaging mechanism.</p> <ul style="list-style-type: none"> Type and dimension: string-scalar Default = gab <p>Note: Do not change this value.</p> |
| PortConfigd | <p>The port number that is used by CVM for vxconfigd-level communication.</p> <ul style="list-style-type: none"> Type and dimension: integer-scalar |
| PortKmsgd | <p>The port number that is used by CVM for kernel-level communication.</p> <ul style="list-style-type: none"> Type and dimension: integer-scalar |
| CVMTimeout | <p>Timeout in seconds used for CVM cluster reconfiguration.</p> <ul style="list-style-type: none"> Type and dimension: integer-scalar Default = 200 |

CVMCluster agent type definition

The following type definition is included in the file, `CVMTypes.cf`:

```

type CVMCluster (
    static keylist RegList = { CVMNodePreference }
    static int NumThreads = 1
    static int OnlineRetryLimit = 2
    static int OnlineTimeout = 400
    static str ArgList[] = { CVMTransport, CVMClustName,
                            CVMNodeAddr, CVMNodeId, PortConfigd,
                            PortKmsgd, CVMTimeout }

    str CVMClustName
    str CVMNodeAddr{}
    str CVMNodeId{}
    str CVMTransport
    str CVMNodePreference
    int PortConfigd
    int PortKmsgd

```

```
        int CVMTimeout  
    )
```

Note: The attributes `CVMNodeAddr`, `PortConfigd`, and `PortKmsgd` are not used in an SF Sybase CE environment. GAB, the required cluster communication messaging mechanism, does not use them.

CVMCluster agent sample configuration

The following is an example definition for the CVMCluster service group:

```
CVMCluster cvm_clus (  
    Critical = 0  
    CVMClustName = clus1  
    CVMNodeId = { node01 = 0, node02 = 1 }  
    CVMTransport = gab  
    CVMTimeout = 200  
)
```

CVMVxconfigd agent

The CVMVxconfigd agent starts and monitors the vxconfigd daemon. The vxconfigd daemon maintains disk and disk group configurations, communicates configuration changes to the kernel, and modifies the configuration information that is stored on disks. CVMVxconfigd must be present in the CVM service group.

The CVMVxconfigd agent is an OnOnly agent; the agent starts the resource when the cluster starts up and VCS restarts the resource when necessary. The Operations attribute specifies these default aspects of startup.

Symantec recommends starting the vxconfigd daemon with the `syslog` option, which enables logging of debug messages. Note that the SF Sybase CE installation configures the `syslog` option for the CVMVxconfigd agent.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Symantec Cluster Server Administrator's Guide*.

Entry points for CVMVxconfigd agent

[Table H-3](#) describes the entry points for the CVMVxconfigd agent.

Table H-3 CVMVxconfigd entry points

| Entry Point | Description |
|----------------------------------|---|
| Online | Starts the <code>vxconfigd</code> daemon |
| Offline | N/A |
| Monitor | Monitors whether <code>vxconfigd</code> daemon is running |
| <code>imf_init</code> | Initializes the agent to interface with the AMF kernel module. This function runs when the agent starts up. |
| <code>imf_getnotification</code> | Gets notification about the <code>vxconfigd</code> process state. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification. If the <code>vxconfigd</code> process fails, the function initiates a traditional CVMVxconfigd monitor entry point. |
| <code>imf_register</code> | Registers or unregisters the <code>vxconfigd</code> process id (pid) with the AMF kernel module. This function runs after the resource goes into steady online state. |

Attribute definition for CVMVxconfigd agent

[Table H-4](#) describes the modifiable attributes of the CVMVxconfigd resource type.

Table H-4 CVMVxconfigd agent attribute

| Attribute | Description |
|------------------|---|
| CVMVxconfigdArgs | <p>List of the arguments that are sent to the <code>online</code> entry point.</p> <p>Symantec recommends always specifying the <code>syslog</code> option.</p> <ul style="list-style-type: none"> Type and dimension: keylist |

Table H-4 CVMVxconfigd agent attribute (continued)

| Attribute | Description |
|-----------|---|
| IMF | <p>This resource-type level attribute determines whether the CVMVxconfigd agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level.</p> <p>This attribute includes the following keys:</p> <ul style="list-style-type: none"> ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: <ul style="list-style-type: none"> ■ 0—Does not perform intelligent resource monitoring ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources Default: 0 ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 1 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: <ul style="list-style-type: none"> ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources ■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3. ■ Type and dimension: integer-association <p>For more details of IMF attribute for the agent type, refer to the <i>Symantec Cluster Server Administrator's Guide</i>.</p> |

CVMVxconfigd agent type definition

The following type definition is included in the CVMTypes.cf file:

```
type CVMVxconfigd (
    static int IMF{} = { Mode=2, MonitorFreq=1, RegisterRetryLimit=3 }
    static int FaultOnMonitorTimeouts = 2
```



```
static int RestartLimit = 5
static str ArgList[] = { CVMVxconfigdArgs }
static str Operations = OnOnly
keylist CVMVxconfigdArgs
)
```

CVMVxconfigd agent sample configuration

The following is an example definition for the `CVMVxconfigd` resource in the CVM service group:

```
CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
)
```

For a more extensive `main.cf` that includes the `CVMVxconfigd` resource:

See [“About sample main.cf files”](#) on page 399.

CVMVoIDg agent

The CVMVoIDg agent represents and controls CVM diskgroups and CVM volumes within the diskgroups. The global nature of CVM diskgroups and volumes requires importing them only once on the CVM master node.

The CVMVoIDg agent manages the CVM disk groups and CVM volumes and volume sets within the disk groups by performing the following functions:

- Imports the shared disk group from the CVM master node
- Starts the volumes and volume sets in the disk group
- Monitors the disk group, volumes, and volume sets
- Optionally, deports the disk group when the dependent applications are taken offline. The agent deports the disk group only if the appropriate attribute is set.

Configure the CVMVoIDg agent for each disk group used by a Sybase service group. A disk group must be configured to only one Sybase service group. If cluster file systems are used for the database, configure the CFMount agent for each volume or volume set in the disk group.

Entry points for CVMVoIDg agent

[Table H-5](#) describes the entry points used by the CVMVoIDg agent.

Table H-5 CVMVoIDg agent entry points

| Entry Point | Description |
|-------------|--|
| Online | <p>Starts all volumes in the shared disk group specified by the CVMVolume attribute.</p> <p>Imports the shared disk group from the CVM master node, if the disk group is not already imported.</p> <p>Starts all volumes and volume sets in the shared disk group specified by the CVMVolume attribute.</p> <p>Sets the disk group activation mode to shared-write if the value of the CVMActivation attribute is sw. You can set the activation mode on both slave and master systems.</p> |
| Offline | <p>Sets the activation mode of the shared disk group to “off.”</p> <p>Removes the temporary files created by the online entry point.</p> <p>If the <code>CVMDeportOnOffline</code> attribute is set to 1 and if the shared disk group does not contain open volumes on any node in the cluster, the disk group is deported from the CVM master node.</p> |
| Monitor | <p>Monitors specified critical volumes in the diskgroup. The CVMVolume attribute specifies these volumes. SFHA requires specifying at least one volume in a disk group.</p> <p>Determines whether the disk group, the volumes, and the volume sets are online.</p> <p>The agent takes a volume set offline if the file system metadata volume of a volume set is discovered to be offline in a monitor cycle.</p> <p>Note: If the CFSMount resource goes offline and the file system on the volume set is unmounted, the agent retains the online state of the volume set even if the file system metadata volume in the volume set is offline. This is because the CVMVoIDg agent is unable to determine whether or not the volumes that are offline are metadata volumes.</p> |
| Clean | <p>Removes the temporary files created by the online entry point.</p> |

Attribute definition for CVMVoIDg agent

[Table H-6](#) describes the user-modifiable attributes of the CVMVoIDg resource type.

Table H-6 CVMVoIDg agent attributes

| Attribute | Description |
|-----------------------------|---|
| CVMDiskGroup (required) | <p>Shared disk group name.</p> <ul style="list-style-type: none"> Type and dimension: string-scalar |
| CVMVolume (required) | <p>Lists critical volumes in the disk group. SF Sybase CE requires specifying at least one volume in the disk group.</p> <p>Name of shared volumes or volume sets. This list is used to check that the volumes or volume sets are in the correct state before allowing the resource to come online, and that the volumes remain in an enabled state.</p> <ul style="list-style-type: none"> Type and dimension: string-keylist |
| CVMActivation (required) | <p>Activation mode for the disk group.</p> <ul style="list-style-type: none"> Type and dimension: string-scalar Default = <code>sw</code> (<code>shared-write</code>) <p>This is a localized attribute.</p> |
| CVMVolumeloTest(optional) | <p>List of volumes and volume sets that will be periodically polled to test availability. The polling is in the form of 4 KB reads every monitor cycle to a maximum of 10 of the volumes or volume sets in the list. For volume sets, reads are done on a maximum of 10 component volumes in each volume set.</p> <ul style="list-style-type: none"> Type and dimension: string-keylist |
| CVMDeportOffline (optional) | <p>Indicates whether or not the shared disk group must be deported when the last online CVMVoIDg resource for a disk group is taken offline.</p> <p>The value 1 indicates that the agent will deport the shared disk group from the CVM master node, if not already deported, when the last online CVMVoIDg resource for the disk group is taken offline.</p> <p>The value 0 indicates that the agent will not deport the shared disk group when the CVMVoIDg resource is taken offline.</p> <ul style="list-style-type: none"> Type and dimension: integer-scalar Default = 0 <p>Note: If multiple CVMVoIDg resources are configured for a shared disk group, set the value of the attribute to either 1 or 0 for all of the resources.</p> <p>The CVM disk group is deported based on the order in which the CVMVoIDg resources are taken offline. If the CVMVoIDg resources in the disk group contain a mixed setting of 1 and 0 for the <code>CVMDeportOffline</code> attribute, the disk group is deported only if the attribute value is 1 for the last CVMVoIDg resource taken offline. If the attribute value is 0 for the last CVMVoIDg resource taken offline, the disk group is not deported.</p> <p>The deport operation fails if the shared disk group contains open volumes.</p> |

CVMVoIDg agent type definition

The CVMTypes.cf file includes the CVMVoIDg type definition:

```
type CVMVoIDg (
    static keylist RegList = { CVMActivation, CVMVolume }
    static int OnlineRetryLimit = 2
    static int OnlineTimeout = 400
    static keylist ExternalStateChange = { OnlineGroup }
    static str ArgList[] = { CVMDiskGroup, CVMVolume, CVMActivation,
                            CVMVolumeIoTest, CVMDGAction,
                            CVMDeportOnOffline, CVMDeactivateOnOffline,
                            State }

    str CVMDiskGroup
    str CVMDGAction
    keylist CVMVolume
    str CVMActivation
    keylist CVMVolumeIoTest
    int CVMDeportOnOffline
    int CVMDeactivateOnOffline
    temp int voldg_stat
)

type CVMVoIDg (
    static keylist RegList = { CVMActivation }
    static str ArgList[] = { CVMDiskGroup, CVMVolume,
                            CVMActivation }
    str CVMDiskGroup
    keylist CVMVolume[]
    str CVMActivation
    temp int voldg_stat
)
```

CVMVoIDg agent sample configuration

Each Oracle service group requires a CVMVoIDg resource type to be defined. The following is a sample configuration:

```
CVMVoIDg cvmvoldg1 (
    Critical = 0
    CVMDiskgroup = testdg
    CVMVolume = { vol1, vol2, mvoll, mvoll2, snapvol, vset1 }
    CVMVolumeIoTest = { snapvol, vset1 }
    CVMActivation @sys1 = sw
```

```
CVMActivation @sys2 = sw
CVMDeportOnOffline = 1
)

CVMVolDg sybbin_dg_voldg (
  CVMDiskGroup = sybbin_dg
  CVMVolume = { sybbin_vol }
  CVMActivation = sw
)
```

CVMVolDg agent sample configuration

Each Sybase service group requires a CVMVolDg resource type to be defined. The following is a sample configuration:

```
CVMVolDg ora_voldg (
  Critical = 0
  CVMDiskGroup = oradatadg
  CVMVolume = { oradata1, oradata2 }
  CVMActivation = sw
)
```

CFSMount agent

The CFSMount agent brings online, takes offline, and monitors a cluster file system mount point.

The agent executable is located in `/opt/VRTSvcs/bin/CFSMount/CFSMountAgent`.

The CFSMount type definition is described in the `/etc/VRTSvcs/conf/config/CFSTypes.cf` file.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Symantec Cluster Server Administrator's Guide*.

Entry points for CFSMount agent

[Table H-7](#) provides the entry points for the CFSMount agent.

Table H-7 CFSMount agent entry points

| Entry Point | Description |
|---------------------|--|
| Online | Mounts a block device in cluster mode. |
| Offline | Unmounts the file system, forcing unmount if necessary, and sets primary to secondary if necessary. |
| Monitor | Determines if the file system is mounted. Checks mount status using the <code>fsclustadm</code> command. |
| Clean | Generates a null operation for a cluster file system mount. |
| imf_init | Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for the agent. This function runs when the agent starts up. |
| imf_getnotification | Gets notification about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification. |
| imf_register | Registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into steady state (online or offline). |

Attribute definition for CFSMount agent

[Table H-8](#) lists user-modifiable attributes of the CFSMount Agent resource type.

Table H-8 CFSMount Agent attributes

| Attribute | Description |
|-------------|--|
| MountPoint | Directory for the mount point. <ul style="list-style-type: none"> Type and dimension: string-scalar |
| BlockDevice | Block device for the mount point. <ul style="list-style-type: none"> Type and dimension: string-scalar |
| NodeList | List of nodes on which to mount. If NodeList is NULL, the agent uses the service group system list. <ul style="list-style-type: none"> Type and dimension: string-keylist |

Table H-8 CFSMount Agent attributes (*continued*)

| Attribute | Description |
|-----------|---|
| IMF | <p>Resource-type level attribute that determines whether the CFSMount agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level.</p> <p>This attribute includes the following keys:</p> <ul style="list-style-type: none"> ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: <ul style="list-style-type: none"> ■ 0—Does not perform intelligent resource monitoring ■ 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources ■ 3—Performs intelligent resource monitoring for both online and for offline resources Default: 0 ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 1 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: <ul style="list-style-type: none"> ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources ■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3. ■ Type and dimension: integer-association |

Table H-8 CFSMount Agent attributes (*continued*)

| Attribute | Description |
|------------------------|--|
| MountOpt (optional) | <p>Options for the mount command. To create a valid MountOpt attribute string:</p> <ul style="list-style-type: none"> Use the VxFS type-specific options only. Do not use the <code>-o</code> flag to specify the VxFS-specific options. Do not use the <code>-t vxfs</code> file system type option. Be aware the cluster option is not required. Specify options in comma-separated list: <pre>ro ro,cluster blkclear,mincache=closesync</pre> <ul style="list-style-type: none"> Type and dimension: string-scalar |
| Policy (optional) | <p>List of nodes to assume the primaryship of the cluster file system if the primary fails. If set to NULL or if none of the hosts specified in the list is active when the primary fails, a node is randomly selected from the set of active nodes to assume primaryship.</p> <ul style="list-style-type: none"> Type and dimension: string-scalar |

CFSMount agent type definition

The `CFSTypes.cf` file includes the CFSMount agent type definition:

```
type CFSMount (
    static int IMF{} = { Mode=3, MonitorFreq=1, RegisterRetryLimit=3 }
    static keylist RegList = { MountOpt, Policy, NodeList, ForceOff, SetPrimary }
    static keylist SupportedActions = { primary }
    static int FaultOnMonitorTimeouts = 1
    static int OnlineWaitLimit = 1
    static str ArgList[] = { MountPoint, BlockDevice, MountOpt, Primary, AMFMountType }
    str MountPoint
    str MountType
    str BlockDevice
    str MountOpt
    keylist NodeList
    keylist Policy
    temp str Primary
    str SetPrimary
    temp str RemountRes
    temp str AMFMountType
```



```

str ForceOff
)

```

CFSMount agent sample configuration

Each Oracle service group requires a CFSMount resource type to be defined:

```

CFSMount ora_mount (
    MountPoint = "/oradata"
    BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol1"
    Primary = node02;
)

CFSMount sybbindg_mnt (
    MountPoint = "/sybase"
    BlockDevice = "/dev/vx/dsk/sybbindg/sybbin_vol"
    Primary = node02;
)

```

To see CFSMount defined in a more extensive example:

See [“About sample main.cf files”](#) on page 399.

Process agent

The Process agent starts, stops, and monitors a process that you specify. You can use the agent to make a process highly available or to monitor it.

Agent functions

| | |
|---------|--|
| Online | Starts a process in the background with optional arguments and priority in the specified user context. |
| Offline | Terminates the process with a SIGTERM. If the process does not exit, a SIGKILL is sent. |
| Monitor | Checks to see if the process is running by scanning the process table for the name of the executable pathname and argument list. |
| Clean | Terminates all ongoing resource actions and takes the resource offline, forcibly when necessary. |

State definitions

| | |
|---------|--|
| ONLINE | Indicates that the specified process is running in the specified user context. |
| OFFLINE | Indicates that the specified process is not running in the specified user context. |
| FAULTED | Indicates that the process has terminated unexpectedly. |
| UNKNOWN | Indicates that the agent can not determine the state of the process. |

Attributes

Table H-9 Required attribute

| Required attribute | Description |
|--------------------|---|
| PathName | Complete pathname to access an executable program. This path includes the program name. If a script controls the process, the PathName defines the complete path to the shell. Type and dimension: string-scalar |

Table H-10 Optional attributes

| Optional attribute | Description |
|--------------------|---|
| Arguments | Passes arguments to the process. If a script controls the process, the script is passed as an argument. Separate multiple arguments with a single space. A string cannot accommodate more than one space between arguments, nor allow for leading or trailing whitespace characters. Type and dimension: string-scalar |

Table H-10 Optional attributes (*continued*)

| Optional attribute | Description |
|--------------------|--|
| | <p>The file that contains the process ID for the monitoring process. Specify the PidFile attribute for the monitoring process to use the Pid. Otherwise, to complete the monitoring process the agent uses the ps output.</p> <p>Note that when you use scripts, or other indirect mechanisms, to start processes, you must set the PidFile attribute if the ps output is different from the configured values for the PathName or Arguments attributes.</p> <p>Type and dimension: string-scalar</p> <p>Example: "/var/lock/sendmail.pid"</p> |
| Priority | <p>Priority that the process runs. Priority values range between -20 (highest) to +19 (lowest).</p> <p>Type and dimension: string-scalar</p> <p>Default: 10</p> |
| UserName | <p>This attribute is the owner of the process. The process runs with the user ID.</p> <p>Type and dimension: string-scalar</p> <p>Default: root</p> |

Resource type definition

```

type Process (
    static keylist SupportedActions = { "program.vfd", getcksum }
    static str ArgList[] = { PathName, Arguments, UserName,
        Priority, PidFile }
    str PathName
    str Arguments
    str UserName = root
    str Priority = 10
    str PidFile
)

```

Sample configurations

```
Process vxfsend (
    PathName = "/sbin/vxfsend"
    Arguments = "-m sybase -k /tmp/vcmp_socket"
)
```

Monitoring options for the Sybase agent

The VCS agent for Sybase provides two levels of application monitoring: basic and detail.

In the basic monitoring mode, the agent for Sybase monitors the Sybase dataserver processes to verify whether they are running.

For Sybase cluster edition, the agent uses `qrmutil` utility that Sybase provides to get the status of the Sybase instance. If the state returned by `qrmutil` utility is 'failure pending', the agent panics the node. When the Sybase agent detects that the configured Sybase server is not running on a system, based on the value of the `OnlineRetryLimit` attribute of the Sybase service group, the service group is restarted on the same system on which the group faulted.

For example:

```
# qrmutil --quorum_dev=/quorum/quorum.dat --monitor=ase1
Executing 'monitor' command for instance 'ase1'
Instance 'ase1' has a failure pending.
# echo $?
99
```

In this example instance 'ase1' has a failure pending state. The agent will panic the node running the instance 'ase1'. The node will automatically rejoin the cluster after reboot.

In the detail monitoring mode, the agent performs a transaction on a test table in the database to ensure that Sybase server is functioning properly. The test table should be created by the user, and the table is specified in the attribute `Table` for the Sybase agent. The agent uses this test table for internal purposes. Symantec recommends that you do not perform any other transaction on the test table.

Sybase resource type

The type definitions and attribute definitions for the Sybase resource type are described as follows.

Type definition for the Sybase agent

The resource type definition for the agent for Sybase is as follows.

```
type Sybase (
    static boolean AEPTimeout = 1
    static keylist SupportedActions = { "checkpoint_all" }
    str Server
    str Owner
    str Home
    str Version
    str SA
    str SApwd
    str Run_ServerFile
    str User
    str UPword
    str Db
    str Table
    str Monscript = "/opt/VRTSagents/ha/bin/Sybase/SqlTest.pl"
    boolean WaitForRecovery = 0
    str Quorum_dev
    str interfaces_File
    int ShutdownWaitLimit = 60
    int DelayAfterOnline = 10
    int DelayAfterOffline = 2
    static int ToleranceLimit = 1
    static str ArgList[] = { Server, Owner, Home, Version, SA,
        SApwd, User, UPword, Db, Table, Monscript,
        WaitForRecovery, Run_ServerFile, Quorum_dev, State,
        interfaces_File, ShutdownWaitLimit, DelayAfterOnline,
        DelayAfterOffline }
    static int IMF{} = { Mode=3, MonitorFreq=5, RegisterRetryLimit=3 }
    static str IMFRegList[] = { Server, Owner, Quorum_dev }
    static str AgentDirectory = "/opt/VRTSagents/ha/bin/Sybase"
)
```

Attribute definitions for the Sybase agent

Review the description of the Sybase agent attributes. The agent attributes are classified as required, optional, and internal.

[Table H-11](#) lists the required attributes.

Table H-11 Required attributes

| Required Attributes | Definition |
|---------------------|---|
| Home | <p>The \$SYBASE path to Sybase binaries and configuration files.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> |
| Owner | <p>Sybase user as the defined owner of executables and database files in any of the sources (such as NIS+, /etc/hosts, and so on) specified in the /etc/nsswitch.conf file for passwd entry. The Sybase executables and database files are accessed in the context of this user.</p> <p>Type and dimension: string-scalar</p> |
| Quorum_dev | <p>The quorum device manages the cluster membership, stores cluster configuration data, and contains information shared among server instances and nodes. The quorum device is a disk that is accessible to all the nodes in the cluster. Specify a fully qualified quorum device name.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> <p>Note: This attribute should be specified only for the cluster edition.</p> <p>Note: If you do not set the Quorum_dev attribute for Sybase Cluster Edition, the Sybase agent does not perform the qrmutil-based checks. This error in configuration may lead to undesirable results. For example, if qrmutil returns failure pending, the agent does not panic the system.</p> |
| SA | <p>Sybase database administrator. This attribute is required to connect to the ASE for shutdown.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> |
| SAPswd | <p>Encrypted password for Sybase database administrator. This password is required to connect to the ASE for shutdown.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> <p>Note: You need not specify a value for this attribute if the SA user does not require a password.</p> |

Table H-11 Required attributes (*continued*)

| Required Attributes | Definition |
|---------------------|---|
| Server | <p>The \$DSQUERY ASE name. Only one server should be configured in a Sybase service group. The advantage of configuring Sybase resources in a separate service group is, each Sybase data server can failover independently.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> |
| Version | <p>Version of Sybase ASE.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> <p>Note: After the Sybase resource is online in VCS, you must not modify the Home and Version attributes. For the Sybase cluster edition, setting invalid values for Home and Version attributes when the resource is in Online state causes the node to panic.</p> <p>Note: For Sybase cluster edition, after the Sybase resource is online in VCS, you must not modify the Home and Version attributes. For the Sybase cluster edition, setting invalid values for Home and Version attributes when the resource is in Online state causes the node to panic.</p> |

Table H-12 lists the optional attributes.

Table H-12 Optional attributes

| Optional Attributes | Definition |
|---------------------|--|
| DetailMonitor | <p>Specifies whether the Sybase server is monitored in detail. A positive integer value indicates that the resource monitors the Sybase server in detail. Value 0 denotes it does not.</p> <p>Note: This attribute has been removed from the agent version 6.1.0 onwards.</p> <p>Default is 0.</p> <p>Type and dimension: int-scalar</p> <p>Note: The DetailMonitor attribute is deprecated in SF Sybase CE 6.2.1. Instead, LevelTwoMonitorFreq attribute at the Sybase resource type level may be used.</p> |

Table H-12 Optional attributes (*continued*)

| Optional Attributes | Definition |
|---------------------|---|
| LevelTwoMonitorFreq | <p>Specifies the frequency at which the agent for this resource type must perform second-level or detailed monitoring.</p> <p>This is a resource type level attribute. You can override the value of this attribute at the resource level.</p> <p>The default value of LevelTwoMonitorFreq attribute is 0 (zero).</p> <p>If required, the value of LevelTwoMonitorFreq attribute can be overridden at resource level.</p> |
| User | <p>The database user, in the context of which, the transactions are performed on the database. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> |
| UPword | <p>Encrypted password for the database user. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value. However, you need not specify a value for this attribute if the database user does not require a password.</p> <p>intercType and dimension: string-scalar</p> <p>Default value: No default value</p> |
| Db | <p>Name of the database used for detailed monitoring. The table used by the detail monitor script resides in this database. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> |
| Table | <p>Name of the table on which the detail monitoring script performs the transactions. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> |

Table H-12 Optional attributes (*continued*)

| Optional Attributes | Definition |
|---------------------|--|
| Monscript | <p>The path to the detail monitor script; the default value for this attribute is the path for the script, SqlTest.pl, provided with the agent. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> <p>Note: By default, SqlTest.pl script has the execute permission set. If you specify custom detail monitor script, ensure that custom detail monitor script also has the execute permissions set.</p> |
| Run_ServerFile | <p>Specifies the location of the RUN_SERVER file for the Sybase instance. The default location of this file is used if no value is specified for this attribute.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> |
| IMF | <p>This resource-type level attribute determines whether the Sybase agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level.</p> <p>This attribute includes the following keys:</p> <ul style="list-style-type: none"> ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. <p>Valid values are as follows:</p> <ul style="list-style-type: none"> ■ 0—Does not perform intelligent resource monitoring ■ 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources ■ 3—Performs intelligent resource monitoring for both online and for offline resources <p>Default: 3</p> |

Table H-12 Optional attributes (*continued*)

| Optional Attributes | Definition |
|---------------------|---|
| IMF (cont.) | <ul style="list-style-type: none"> ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 5 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: <ul style="list-style-type: none"> ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources ■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the sybase_imf_register agent function to register the resource with the AMFkernel driver. The value of the RegisterRetryLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3 <p>Type and dimension: Integer-association.</p> |
| interfaces_File | <p>Specifies the location of interfaces file, including the directory name and the file name for the Sybase instance. If this attribute is configured, [-I interfaces file] option is used when connecting to the isql session. If this attribute is not configured, the agent does not use the -I option.</p> <p>Type and dimension: string-scalar</p> <p>Default value: No default value</p> <p>For example: /sybase/my_interfaces_file</p> <p>Note: It is assumed that you have modified the RUN_ServerFile with the non-default interface file location if the interfaces_File attribute is configured.</p> |

Table H-12 Optional attributes (*continued*)

| Optional Attributes | Definition |
|---------------------|--|
| DelayAfterOnline | <p>Specifies the number of seconds that elapse after the Online entry point is complete and before the next monitor cycle is invoked.</p> <p>Type and dimension: integer-scalar</p> <p>Default value: 10</p> |
| DelayAfterOffline | <p>Specifies the number of seconds that elapse after the Offline entry point is complete and before the next monitor cycle is invoked.</p> <p>Type and dimension: integer-scalar</p> <p>Default value: 2</p> |
| ShutdownWaitLimit | <p>Maximum number of seconds for which the agent waits for the Sybase instance to stop after issuing the <code>shutdown with wait</code> command, and before attempting to issue the <code>kill -15 <data server-pid></code> command, if required.</p> <p>Type and dimension: integer-scalar</p> <p>Default value: 60</p> |
| Quorum_dev | <p>The quorum device manages the cluster membership, stores cluster configuration data and contains information shared among server instances and nodes. It must be a disk accessible to all nodes in the cluster. Specify fully qualified quorum device name.</p> <p>Note: If you do not set the Quorum_dev attribute for Sybase Cluster Edition, the Sybase agent does not perform the qrmutil-based checks. This error in configuration may lead to undesirable results. For example, if qrmutil returns failure pending, the agent does not panic the system.</p> <p>Type and dimension: String-scalar</p> <p>Default value: No default value</p> |
| Run_ServerFile | <p>Specifies the location of the RUN_SERVER file of the Sybase instance. The default location of the file is used if no value is specified for this attribute.</p> <p>Type and dimension: String-scalar</p> <p>Default value: No default value</p> |

Compatibility issues when installing Storage Foundation for Sybase ASE CE with other products

This appendix includes the following topics:

- [Installing, uninstalling, or upgrading Storage Foundation products when other Symantec products are present](#)
- [Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present](#)
- [Installing, uninstalling, or upgrading Storage Foundation products when ApplicationHA is already present](#)
- [Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present](#)

Installing, uninstalling, or upgrading Storage Foundation products when other Symantec products are present

Installing Storage Foundation when other Symantec 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 VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the VOM Central Server and Managed Host RPMs as is.
- When uninstalling Storage Foundation products where VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

Installing, uninstalling, or upgrading Storage Foundation products when ApplicationHA is already present

If you plan to install or upgrade Storage Foundation on systems where ApplicationHA has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where ApplicationHA is present, the installer does not consider VCS as an installed product even though it uses the bundled VRTSvcs RPM.
- When you install or upgrade Storage Foundation products where ApplicationHA is present, the installer does not allow the installation or upgrade for products that use VCS. The following products cannot be installed or upgrade: VCS, SFHA, SFCFS, SFCFSHA, SF Oracle RAC, SFCFSRAC or SFSYBASECE.
- When you install or upgrade Storage Foundation products where ApplicationHA is present, the installer allows the installation or upgrade of VM, FS, SF, or DMP.
- When you uninstall Storage Foundation products where ApplicationHA is present, the installer does not uninstall VRTSsfmh.

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

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpx and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpx, VRTSicsco, and VRTSat.