Veritas Storage Foundation™ for Oracle® RAC Installation and Configuration Guide

HP-UX 11i v3

5.1 Service Pack 1

Symantec

Veritas Storage Foundation™ for Oracle RAC Installation and Configuration Guide

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

Product version: 5.1 SP1

Document version: 5.1SP1.0

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

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

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

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

docs@symantec.com

About Symantec Connect

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

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

Contents

Technical Support 4

Section 1 Installation overview and planning 25

Chapter 1 Introducing Veritas Storage Foundation for Oracle RAC 27

About Veritas Storage Foundation for Oracle RAC 27
Benefits of SF Oracle RAC 27
About basic SF Oracle RAC components 29
About SF Oracle RAC features 30
About I/O fencing 31
Symantec Operations Readiness Tools 34
About VCS notifications 35
About campus clusters 35
About global clusters 35
About Veritas Volume Replicator 35
About database management using SF Oracle RAC 35
About SF Oracle RAC optional components 36
About Symantec Product Authentication Service (AT) 36
Veritas Operations Manager 36
About Cluster Manager (Java Console) 37
SF Oracle RAC cluster setup models 37
Typical configuration of four-node SF Oracle RAC cluster 38
Typical configuration of SF Oracle RAC clusters in secure mode 39
Typical configuration of VOM-managed SF Oracle RAC clusters 40
Typical configuration of SF Oracle RAC campus clusters for disaster recovery 41
Typical configuration of SF Oracle RAC global clusters for disaster recovery 43

Chapter 2 System requirements 45

Important preinstallation information 45
Hardware requirements 46
I/O fencing requirements 48
Coordinator disk requirements for I/O fencing 48
CP server requirements 48
Supported HP-UX operating systems 51
Supported database software 52
Supported replication technologies for global clusters 52

Chapter 3 Planning to install SF Oracle RAC 53

Planning your network configuration 53
Planning the public network configuration for Oracle RAC 54
Planning the private network configuration for Oracle RAC 54
Planning the storage 56
Planning the storage for SF Oracle RAC 57
Planning the storage for Oracle RAC 57
Planning volume layout 61
Planning file system design 62
About planning to configure I/O fencing 62
Typical SF Oracle RAC cluster configuration with disk-based I/O fencing 64
Typical SF Oracle RAC cluster configuration with server-based I/O fencing 65
Recommended CP server configurations 65
Planning for cluster management 68
Planning for disaster recovery 69
Planning a campus cluster setup 69
Planning a global cluster setup 70
Data replication considerations 70

Chapter 4 Licensing SF Oracle RAC 73

About Veritas product licensing 73
About SF Oracle RAC licenses 74
Setting or changing the product level for keyless licensing 76
Installing Veritas product license keys 77

Section 2 Installation and configuration of SF Oracle RAC 79

Chapter 5 Preparing to install SF Oracle RAC 81

Setting the umask before installation 81
Synchronizing time settings on cluster nodes 81
Mounting the product disc 82
Setting up shared storage 82
Setting the environment variables 83
Optimizing LLT media speed settings on private NICs 83
Guidelines for setting the media speed of the LLT interconnects 84
Verifying the systems before installation 84

Chapter 6 Installing SF Oracle RAC 87

About installing SF Oracle RAC 87
About installation and configuration methods 88
Installing SF Oracle RAC using the Veritas script-based installation program 89
Installing SF Oracle RAC using the Veritas Web-based installation program 92
Before using the Veritas Web-based installer 93
Starting the Veritas Web-based installer 93
Installing products with the Veritas Web-based installer 94

Chapter 7 Preparing to configure SF Oracle RAC 97

Preparing to configure the clusters in secure mode 97
Installing the root broker for the security infrastructure 101
Creating authentication broker accounts on root broker system 102
Creating encrypted files for the security infrastructure 103
Preparing the installation system for the security infrastructure 105
Setting up the CP server 106
Planning your CP server setup 107
Installing the CP server using the installer 108
Configuring the CP server cluster in secure mode 109
Setting up shared storage for the CP server database 110
Configuring the CP server using the configuration utility 111
Configuring the CP server manually 119

Verifying the CP server configuration 121

Chapter 8 Configuring SF Oracle RAC 123

About configuring SF Oracle RAC 123
Configuring the SF Oracle RAC components using the script-based installer 124
Configuring the SF Oracle RAC cluster 125
Creation of SF Oracle RAC configuration files 139
Stopping and starting SF Oracle RAC processes 139
Configuring SF Oracle RAC using the Web-based installer 140

Chapter 9 Configuring SF Oracle RAC clusters for data integrity 147

Setting up disk-based I/O fencing using installsfrac program 147
Initializing disks as VxVM disks 147
Identifying disks to use as coordinator disks 148
Checking shared disks for I/O fencing 149
Configuring disk-based I/O fencing using installsfrac program 152
Setting up disk-based I/O fencing manually 155
Setting up coordinator disk groups 155
Creating I/O fencing configuration files 156
Modifying VCS configuration to use I/O fencing 157
Starting SF Oracle RAC on all nodes 158
Verifying I/O fencing configuration 160
Setting up server-based I/O fencing using installsfrac program 161
Verifying the security configuration on the SF Oracle RAC cluster to use CP server coordination point 161
Configuring server-based I/O fencing using the installsfrac program 163
Setting up server-based I/O fencing manually 172
Preparing the CP servers manually for use by the SF Oracle RAC cluster 172
Configuring server-based fencing on the SF Oracle RAC cluster manually 176
Configuring Coordination Point agent to monitor coordination points 180
Verifying server-based I/O fencing configuration 182

Chapter 10 Performing post-installation and configuration tasks 185

About enabling LDAP authentication for clusters that run in secure mode 185
Enabling LDAP authentication for clusters that run in secure mode 187
Configuring Veritas Volume Replicator 193
Verifying SF Oracle RAC installation using VCS configuration file 194
Verifying LLT, GAB, and cluster operation 194
Verifying LLT 195
Verifying GAB 197
Verifying the cluster 198
Verifying the cluster nodes 199
Running VRTSexplorer to diagnose issues in the cluster 202

Section 3 Upgrade of SF Oracle RAC 203

Chapter 11 Preparing to upgrade to SF Oracle RAC 5.1 SP1 205

About upgrading SF Oracle RAC 205
About types of upgrade 206
Supported upgrade paths 206
Preparing to upgrade to SF Oracle RAC 5.1 SP1 208
Pre-upgrade tasks for migrating the SFDB repository database 210

Chapter 12 Performing a full upgrade to SF Oracle RAC 5.1 SP1 213

About full upgrades 213
Upgrading to SF Oracle RAC 5.1 SP1 214
Upgrading the HP-UX operating system 215
Upgrading SF Oracle RAC using the Veritas script-based installation program 216
Upgrading SF Oracle RAC using a response file 218

Chapter 13 Performing a phased upgrade to SF Oracle RAC 5.1 SP1 223

About phased upgrade 223
Performing phased upgrade of SF Oracle RAC from version 5.0 224
Step 1: Performing pre-upgrade tasks on the first half of the cluster 225

Step 2: Upgrading the first half of the cluster 228
Step 3: Performing pre-upgrade tasks on the second half of the cluster 229
Step 4: Performing post-upgrade tasks on the first half of the cluster 231
Step 5: Upgrading the second half of the cluster 233
Step 6: Performing post-upgrade tasks on the second half of the cluster 234

Chapter 14 Upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1 237

About upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1 237
Upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1 238

Chapter 15 Migrating from single instance Storage Foundation for Oracle HA to SF Oracle RAC 241

Migration overview 241
Sample configuration before and after migration 242
Migration requirements 243
Before you migrate 243
Migrating to SF Oracle RAC 5.1 SP1 244
Migrating Storage Foundation for Oracle HA to SF Oracle RAC 244
Migrating a single instance Oracle database to Oracle RAC database 245
Completing post-migration tasks 249
Sample configuration files 252
VCS configuration file for Storage Foundation for Oracle HA 252
Oracle initialization parameter file for Storage Foundation for Oracle HA 253
tnsnames.ora for Storage Foundation for Oracle HA 254
listener.ora for Storage Foundation for Oracle HA 254

Chapter 16 Performing post-upgrade tasks 257

Relinking Oracle RAC libraries with the SF Oracle RAC libraries 257
Setting or changing the product license level 261
Changing permissions for Storage Foundation for Databases 261
Upgrading disk layout versions 262

Upgrading VxVM disk group version 262
Post upgrade tasks for migrating the SFDB repository database 263
Migrating from a 5.0 repository database to 5.1 Service Pack 1 263
Migrating from a 4.x repository database to 5.1 Service Pack 1 266
After upgrading from 5.0.x and before migrating SFDB 268
Configuring Powerfail Timeout after upgrade 269
Converting from QuickLog to Multi-Volume support 269
Verifying the cluster 270

Section 4 Installation and upgrade of Oracle RAC 273

Chapter 17 Before installing Oracle RAC 275

About preparing to install Oracle RAC 275
Preparing to install Oracle RAC using the SF Oracle RAC installer or manually 276
Identifying the public virtual IP addresses for use by Oracle 277
Setting the kernel parameters 278
Verifying the user "nobody" exists 278
Launching the SF Oracle RAC installer 278
Creating users and groups for Oracle RAC 279
Creating storage for OCR and voting disk 282
Configuring private IP addresses for Oracle RAC 295
Creating Oracle Clusterware/Grid Infrastructure and Oracle database home directories manually 308
Setting up user equivalence 323
Setting privileges for the DBA user 323
Verifying the systems for Oracle RAC installation 324

Chapter 18 Installing Oracle RAC 329

About installing Oracle RAC 329
Installing the Oracle Clusterware/Grid Infrastructure software 330
Installing Oracle Clusterware/Grid Infrastructure using the SF Oracle RAC installer 331
Installing Oracle Clusterware/Grid Infrastructure using the Oracle Universal Installer 334
Configuring LLT links in the GPnP profile 336
Installing the Oracle RAC database software 337

Installing the Oracle RAC database using the SF Oracle RAC installer 338
Installing the Oracle RAC database using the Oracle Universal Installer 340
Verifying the Oracle Clusterware/Grid Infrastructure and database installation 341
Node numbering discrepancies in Oracle RAC 11g Release 2 342

Chapter 19 Performing Oracle RAC post-installation tasks 345

Adding Oracle RAC patches or patchsets 345
Configuring the CSSD resource 346
Configuring the CSSD resource using the SF Oracle RAC installer 346
Configuring the CSSD resource manually 348
Preventing automatic startup of Oracle Clusterware/Grid Infrastructure 350
Relinking the SF Oracle RAC libraries with Oracle RAC 350
Relinking the SF Oracle RAC libraries with Oracle RAC using the SF Oracle RAC installer 351
Relinking the SF Oracle RAC libraries with Oracle RAC manually 352
Verifying whether Oracle uses Veritas libraries 353
Creating the Oracle RAC database 353
Adding Oracle UDP IPC private IP addresses to the Oracle initialization parameter file 354
Preventing automatic database startup 355
Configuring VCS service groups for Oracle RAC 356
Using the CLI to configure VCS service groups for Oracle RAC 360
Location of VCS log files 362
Removing permissions for communication 362
Configuring the SFDB repository database after installation 362

Chapter 20 Upgrading Oracle RAC 363

Supported upgrade paths 363
Preparing to upgrade Oracle RAC 364
Preparing to upgrade from Oracle RAC 10g or Oracle RAC 11g 364
Preparing to upgrade from Oracle RAC 9i 365
Upgrading Oracle RAC binaries 365
Migrating the Oracle RAC database 366
Performing post-upgrade tasks 366

Section 5 Installation of SF Oracle RAC and Oracle RAC using a response file 369

Chapter 21 About response files 371

About response files 371
Modular deployments using response files 373
About the installation simulator 374
Response file syntax 374
Guidelines for creating the SF Oracle RAC response file 375
Installation scenarios for response files 380

Chapter 22 Installing and configuring SF Oracle RAC using a response file 381

Installing and configuring SF Oracle RAC 381
Sample response file for installing SF Oracle RAC 383
Sample response file for configuring SF Oracle RAC 383

Chapter 23 Configuring I/O fencing using a response file 385

Configuring I/O fencing using response files 385
Sample response file for configuring disk-based I/O fencing 386
Sample response file for configuring server-based I/O fencing 386

Chapter 24 Installing Oracle RAC using a response file 389

About installing Oracle RAC using response files 389
Before you install 389
Installing Oracle RAC 391
Sample response file for installing Oracle RAC 392

Chapter 25 Response file variable definitions 395

Response file variables for installing SF Oracle RAC 395
Response file variables to configure SF Oracle RAC 398
Response file variables to configure disk-based I/O fencing 407
Response file variables to configure server-based I/O fencing 409
Response file variable definitions for Oracle RAC 411

Section 6 Adding or removing nodes from an SF Oracle RAC cluster 429

Chapter 26 Adding a node to SF Oracle RAC clusters 431

About adding a node to a cluster 431
Before adding a node to a cluster 432
Meeting hardware and software requirements 432
Setting up the hardware 432
Preparing to add a node to a cluster 434
Adding a node to a cluster 434
Adding a node to a cluster using the SF Oracle RAC installer 434
Adding the node to a cluster manually 438
Preparing the new node for installing Oracle RAC 450
Preparing the new nodes for installing Oracle RAC using the SF Oracle RAC installer 451
Preparing the new node manually for installing Oracle RAC 458
Adding the new node to Oracle RAC 470
Updating the Storage Foundation for Databases (SFDB) repository after adding a node 471

Chapter 27 Removing a node from SF Oracle RAC clusters 473

About removing a node from a cluster 473
Removing a node from a cluster 474
Modifying the VCS configuration files on existing nodes 475
Editing the /etc/llthosts file 475
Editing the /etc/gabtab file 476
Modifying the VCS configuration to remove the node 476
Removing the node configuration from the CP server 477
Removing security credentials from the leaving node 478
Updating the Storage Foundation for Databases (SFDB) repository after removing a node 479
Sample configuration file for removing a node from the cluster 479

Section 7 Configuration of disaster recovery environments 485

Chapter 28 Configuring a campus cluster setup for disaster recovery 487

Requirements for an SF Oracle RAC campus cluster 487
Setting up an SF Oracle RAC campus cluster for disaster recovery 488
Preparing to set up a campus cluster 489
Configuring VxVM disk groups for Oracle RAC on a campus cluster 489
Tuning guidelines for campus clusters 492
Best practices for a campus cluster 492

Chapter 29 Setting up a replicated global cluster 495

Replication in the SF Oracle RAC environment 495
Requirements for SF Oracle RAC global clusters 496
Supported software and hardware for SF Oracle RAC 496
Supported replication technologies for SF Oracle RAC 496
About setting up a global cluster in an SF Oracle RAC environment 498
Configuring a cluster at the primary site 499
Configuring a cluster at the secondary site 501
Setting up the cluster on the secondary site 501
Setting up the database for the secondary site 502
Configuring replication on clusters at both sites 504
Modifying the ClusterService group for global clusters 505
Modifying the global clustering configuration using the wizard 505
Defining the remote cluster and heartbeat objects 506
Configuring the VCS service groups for global clusters 509

Chapter 30 Configuring a global cluster using VVR 511

About configuring global clustering using VVR 511
Setting up replication using VVR on the primary site 512
Creating the SRL volume on the primary site 512
Setting up the Replicated Volume Group (RVG) on the primary site 513
Setting up replication using VVR on the secondary site 515
Creating the data and SRL volumes on the secondary site 515

Editing the /etc/vx/vras/.rdg files 516
Setting up IP addresses for RLINKs on each cluster 516
Setting up the disk group on secondary site for replication 517
Starting replication of Oracle RAC database volume 519
Starting replication using automatic synchronization 520
Starting replication using full synchronization with Checkpoint 520
Verifying replication status 521
Configuring VCS to replicate the database volume using VVR 521
About modifying the VCS configuration for replication 522
Configuration examples before and after modification 523
Modifying the VCS Configuration on the Primary Site 526
Modifying the VCS Configuration on the Secondary Site 529
Using VCS commands on SF Oracle RAC global clusters 534
Using VVR commands on SF Oracle RAC global clusters 534
About migration and takeover of the primary site role 534
Migrating the role of primary site to the secondary site 535
Migrating the role of new primary site back to the original primary site 536
Taking over the primary role by the remote cluster 536
VCS agents to manage wide-area failover 540

Section 8 Uninstallation of SF Oracle RAC 543

Chapter 31 Preparing to uninstall SF Oracle RAC from a cluster 545

About uninstalling SF Oracle RAC from a cluster 545
Options for uninstalling SF Oracle RAC 546
Preparing to uninstall SF Oracle RAC from a cluster 547
Stopping Oracle instances 548
Backing up the Oracle database 549
Unlinking the SF Oracle RAC libraries from Oracle RAC 549
Uninstalling Oracle RAC (optional) 551
Stopping the applications that use CVM or CFS (outside of VCS control) 551
Unmounting CFS file systems (outside of VCS control) 551
Stopping VCS 552
Stopping the applications that use VxVM or VxFS (outside of VCS control) 553
Unmounting VxFS file systems (outside of VCS control) 553
Stopping the AMF driver 553

Chapter 32 Uninstalling SF Oracle RAC from a cluster 555

Uninstalling SF Oracle RAC from a cluster 555
Removing the CP server configuration using the removal script 556
Removing the SF Oracle RAC depots 560
Removing other configuration files (optional) 561
Removing the Storage Foundation for Databases (SFDB) repository after removing the product 562
Uninstalling SF Oracle RAC with the Veritas Web-based installer 563
Uninstalling SF Oracle RAC using a response file 564
Response file variables to uninstall SF Oracle RAC 565
Sample response file for uninstalling SF Oracle RAC 566

Section 9 Installation reference 567

Appendix A SF Oracle RAC installation depots 569

SF Oracle RAC installation depots 569

Appendix B Installation scripts 573

About installation scripts 573
Installation script options 574

Appendix C SF Oracle RAC installation and configuration sample values 581

About the installation and configuration worksheets 581
SF Oracle RAC worksheet 582
Veritas Cluster Server component information 585
I/O fencing information 586
Cluster Volume Manager information 587
SF Oracle RAC secure mode cluster information 587
SF Oracle RAC add user information 588
Global cluster information 589
Veritas Volume Replicator information 589
Oracle RAC worksheet 590
Replicated cluster using VVR worksheet 596
Replicated cluster using SRDF worksheet 597
Required installation information for Oracle Clusterware/Grid Infrastructure 599
Required installation information for Oracle database 603

Appendix D Sample configuration files 605

About VCS configuration file 605
About the LLT and GAB configuration files 606
About I/O fencing configuration files 608
Sample configuration files 610
sfrac01_main.cf file 611
sfrac02_main.cf file 612
sfrac03_main.cf file 613
sfrac04_main.cf file 614
sfrac05_main.cf file 616
sfrac06_main.cf file 617
sfrac07_main.cf and sample08_main.cf files 618
sfrac09_main.cf and sample10_main.cf files 620
sfrac11_main.cf file 623
sfrac12_main.cf and sample13_main.cf files 624
sfrac14_main.cf file 627
Sample configuration files for CP server 628

Appendix E Setting up inter-system communication 635

About configuring ssh or remsh using the Veritas installer 635
Setting up inter-system communication 636
Setting up ssh on cluster systems 636

Appendix F Automatic Storage Management 639

About ASM in SF Oracle RAC environments 639
ASM configuration with SF Oracle RAC 640
Configuring ASM in SF Oracle RAC environments 642
Setting up Automatic Storage Management 643
Unlinking the SF Oracle RAC ODM library 645
Creating database storage on ASM 646
Creating ASM disk groups and instances 647
Verify the ASM setup 648
Configuring VCS service groups for database instances on ASM 648
Sample configuration file Veritas CVM and ASM main.cf file 651

Appendix G Creating a test database 653

About creating a test database 653
Creating a database for Oracle 653
Creating the database storage on raw volumes 654
Creating the database storage on CFS 655

Appendix H High availability agent information 657

About agents 657
VCS agents included within SF Oracle RAC 658
VCS agents for Oracle included within SF Oracle RAC 658
CVMCluster agent 659
Entry points for CVMCluster agent 659
Attribute definition for CVMCluster agent 660
CVMCluster agent type definition 660
CVMCluster agent sample configuration 661
CVMVxconfigd agent 661
Entry points for CVMVxconfigd agent 662
Attribute definition for CVMVxconfigd agent 662
CVMVxconfigd agent type definition 666
CVMVxconfigd agent sample configuration 666
CVMVolDg agent 666
Entry points for CVMVolDg agent 667
Attribute definition for CVMVolDg agent 668
CVMVolDg agent type definition 670
CVMVolDg agent sample configuration 670
CFSMount agent 670
Entry points for CFSMount agent 671
Attribute definition for CFSMount agent 671
CFSMount agent type definition 675
CFSMount agent sample configuration 675
CFSfsckd agent 676
Entry points for CFSfsckd agent 676
Attribute definition for CFSfsckd agent 676
CFSfsckd agent type definition 679
CFSfsckd agent sample configuration 679
PrivNIC agent 679
Functions of the PrivNIC agent 680
Attributes of the PrivNIC agent 680
States of the PrivNIC agent 683
Sample service group configuration with the PrivNIC agent 683
Type definition of the PrivNIC resource 684
Sample configuration of the PrivNIC resource 684
MultiPrivNIC agent 685
Managing high availability of private interconnects 685
Functions of the MultiPrivNIC agent 685
Attributes of the MultiPrivNIC agent 686
States of the MultiPrivNIC agent 688

Sample service group configuration with the MultiPrivNIC agent 688
Type definition of the MultiPrivNIC resource 689
Sample configuration of the MultiPrivNIC resource 689
CSSD agent 690
Functions of the CSSD agent 691
Attributes of the CSSD agent 691
States of the CSSD agent 691
Sample service group configurations with the CSSD agent 692
Type definition of the CSSD resource 692
Sample configuration of the CSSD resource 693
VCS agents for Oracle 693
Oracle agent functions 693
Resource type definition for the Oracle agent 699
Netlsnr agent functions 705
Resource type definition for the Netlsnr agent 707
ASMDG agent functions 711
Resource type definition for the ASMDG agent 711
CRSResource agent 714
Functions of the CRSResource agent 714
States of the CRSResource agent 714
Attributes of the CRSResource agent 715
VCS service group dependencies with the CRSResource agent 716
Resource type definition for the CRSResource agent 721
Sample configuration for the CRSResource agent 721

Appendix I SF Oracle RAC deployment scenarios 723

SF Oracle RAC cluster with VCS IPC and PrivNIC agent 723
SF Oracle RAC cluster with UDP IPC and PrivNIC agent 726
SF Oracle RAC cluster for multiple databases with UDP IPC and MultiPrivNIC agent 727
SF Oracle RAC cluster with isolated Oracle traffic and MultiPrivNIC agent 730
SF Oracle RAC cluster with NIC bonding, VCS IPC and PrivNIC agent 732
SF Oracle RAC cluster with NIC bonding, UDP IPC, and PrivNIC agent 734
Configuration diagrams for setting up server-based I/O fencing 736
Two unique client clusters served by 3 CP servers 736
Client cluster served by highly available CPS and 2 SCSI-3 disks 737

Two node campus cluster served by remote CP server and 2 SCSI-3 disks 739
Multiple client clusters served by highly available CP server and 2 SCSI-3 disks 741
Deploying Storage Foundation for Databases (SFDB) tools in a Storage Foundation for Oracle RAC environment 743

Glossary 745

Index 749

Section 1

Installation overview and planning

- Chapter 1. Introducing Veritas Storage Foundation for Oracle RAC
- Chapter 2. System requirements
- Chapter 3. Planning to install SF Oracle RAC
- Chapter 4. Licensing SF Oracle RAC

Chapter 1

Introducing Veritas Storage Foundation for Oracle RAC

This chapter includes the following topics:

- About Veritas Storage Foundation for Oracle RAC
- About basic SF Oracle RAC components
- About SF Oracle RAC features
- About SF Oracle RAC optional components
- SF Oracle RAC cluster setup models

About Veritas Storage Foundation for Oracle RAC

Veritas Storage Foundation™ for Oracle® RAC (SF Oracle RAC) leverages proprietary storage management and high availability technologies to enable robust, manageable, and scalable deployment of Oracle RAC on UNIX platforms. The solution uses Veritas 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.

The solution stack comprises the Veritas Cluster Server (VCS), Veritas Cluster Volume Manager (CVM), Veritas Oracle Real Application Cluster Support (VRTSdbac), Veritas Oracle Disk Manager (VRTSodm), Veritas Cluster File System (CFS), and Veritas Storage Foundation, which includes the base Veritas Volume Manager (VxVM) and Veritas File System (VxFS).

Benefits of SF Oracle RAC

SF Oracle RAC provides the following benefits:

- Support for file system-based management. SF Oracle RAC provides a generic clustered file system technology for storing and managing Oracle data files as well as other application data.
- Support for high-availability of cluster interconnects.
  For Oracle RAC 10g Release 2:
  The combination of LMX/LLT protocols and the PrivNIC/MultiPrivNIC agents provides maximum bandwidth as well as high availability of the cluster interconnects, including switch redundancy.
  For Oracle RAC 11g Release 1/Oracle RAC 11g Release 2:
  The PrivNIC/MultiPrivNIC agents provide maximum bandwidth as well as high availability of the cluster interconnects, including switch redundancy.
- Use of clustered file system and volume management technologies for placement of Oracle Cluster Registry (OCR) and voting disks. These technologies provide robust shared block and raw interfaces for placement of OCR and voting disks. In the absence of SF Oracle RAC, separate LUNs need to be configured for OCR and voting disks.
- Support for a standardized approach toward application and database management. A single-vendor solution for the complete SF Oracle RAC software stack lets you devise a standardized approach toward application and database management. Further, administrators can apply existing expertise of Veritas technologies toward SF Oracle RAC.
- Increased availability and performance using dynamic multi-pathing (DMP). DMP provides wide storage array support for protection from failures and performance bottlenecks in the HBAs, SAN switches, and storage arrays.
- Easy administration and monitoring of SF Oracle RAC clusters from a single web console.
- Support for many types of applications and databases.
- Improved file system access times using Oracle Disk Manager (ODM).
- Ability to configure ASM disk groups over CVM volumes to take advantage of dynamic multi-pathing (DMP).
- Enhanced scalability and availability with access to multiple Oracle RAC instances per database in a cluster.
- Support for backup and recovery solutions using volume-level and file system-level snapshot technologies. SF Oracle RAC enables full volume-level snapshots for off-host processing and file system-level snapshots for efficient backup and rollback.
- Ability to failover applications without downtime using clustered file system technology.

- Prevention of data corruption in split-brain scenarios with robust SCSI-3 Persistent Group Reservation (PGR) based I/O fencing or Coordination Point Server-based I/O fencing. The preferred fencing feature also enables you to specify how the fencing driver determines the surviving subcluster.
- Support for sharing all types of files, in addition to Oracle database files, across nodes.
- 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 Oracle RAC environment is far quicker than recovery for a failover database.
- Verification of disaster recovery configuration using fire drill technology without affecting production systems.
- Support for a wide range of hardware replication technologies as well as block-level replication using VVR.
- Support for campus clusters with the following capabilities:
  - Consistent reattach with Site Awareness
  - Site aware reads with VxVM mirroring
  - Monitoring of Oracle resources
  - Protection against split-brain scenarios

About basic SF Oracle RAC components

The basic components of SF Oracle RAC are as follows:

Veritas Cluster Server	Veritas Cluster Server (VCS) manages Oracle RAC databases and infrastructure components in a clustered environment.
Cluster Volume Manager	Cluster Volume Manager (CVM) enables simultaneous access to the shared volumes that are based on technology from Veritas Volume Manager (VxVM).
Cluster File System	Cluster File System (CFS) enables simultaneous access to the shared file systems that are based on technology from Veritas File System (VxFS).

Oracle Disk Manager	Oracle Disk Manager (ODM) is a disk and file management interface that is provided by Oracle to improve disk I/O performance. ODM enables Oracle to allocate and release disk space, manage tablespaces, and read/write disk blocks directly. SF Oracle RAC uses a custom driver that enables applications to use ODM for enhanced file system performance and easy file administration.
RAC Extensions	RAC Extensions manage the cluster membership and communications between cluster nodes.

For a detailed understanding of each component and the architectural overview, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

About SF Oracle RAC features

You can configure the following features in an SF Oracle RAC cluster:

- I/O fencing
  See "About I/O fencing" on page 31.
- Symantec Operations Readiness Tools
  See "Symantec Operations Readiness Tools" on page 34.
- VCS notifications
  See "About VCS notifications" on page 35.
- Campus clusters
  See "About campus clusters" on page 35.
- Global clusters
  See "About global clusters" on page 35.
- Storage Foundation Database Management tools
  See "About database management using SF Oracle RAC" on page 35.
- Veritas Volume Replicator
  See "About Veritas Volume Replicator" on page 35.

Note: I/O fencing is mandatory in SF Oracle RAC installations. All other features are optional and may be configured to suit your business needs.

About I/O fencing

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

The fencing operation determines the following:

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

This decision prevents possible data corruption. The installer installs the I/O fencing driver, VRTSvxfen, when you install SF Oracle RAC. To protect data on shared disks, you must configure I/O fencing after you install and configure SF Oracle RAC.

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

You can configure I/O fencing to use one or both of the following components as coordination points:

Coordinator disk	I/O fencing that uses coordinator disks is referred to as disk-based I/O fencing. Disk-based I/O fencing ensures data integrity in a single cluster.
Coordination point server (CP server)	I/O fencing that uses at least one CP server system is referred to as server-based I/O fencing. Server-based I/O fencing ensures data integrity in multiple clusters.

See the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

About server-based I/O fencing

In a disk-based I/O fencing implementation, the vxfen driver handles various SCSI-3 PR based arbitration operations completely within the driver. I/O fencing also provides a framework referred to as customized fencing wherein arbitration operations are implemented in custom scripts. The vxfen driver invokes the custom scripts.

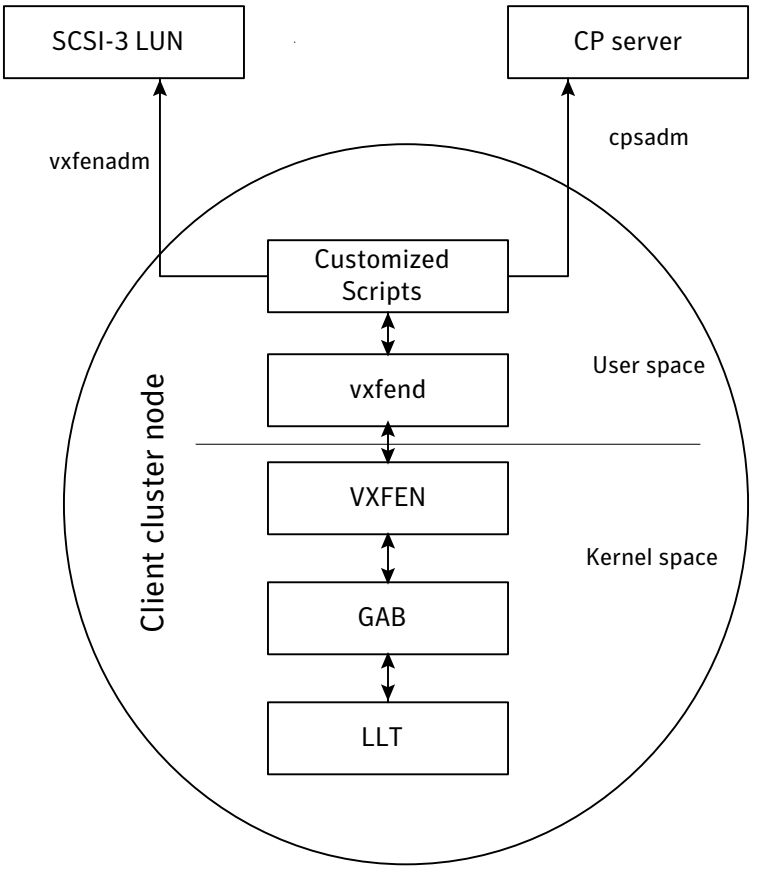
The CP server-based coordination point uses a customized fencing framework. Note that SCSI-3 PR based fencing arbitration can also be enabled using customized fencing framework. This allows the user to specify a combination of SCSI-3 LUNs and CP servers as coordination points using customized fencing. Customized

fencing can be enabled by specifying vxfen_mode=customized and vxfen_mechanism=cps in the `/etc/vxfenmode` file.

Moreover, both `/etc/vxfenmode` and `/etc/vxfentab` files contain additional parameter "security" which indicates if communication between CP server and SF Oracle RAC cluster nodes is secure.

Figure 1-1 displays a schematic of the customized fencing options.

Figure 1-1 Customized fencing



A user level daemon vxfend interacts with the vxfen driver, which in turn interacts with GAB to get the node membership update. Upon receiving membership updates, vxfend invokes various scripts to race for the coordination point and fence off data disks. The vxfend daemon manages various fencing agents. The customized fencing scripts are located in the `/opt/VRTSvcs/vxfen/bin/customized/cps` directory.

The scripts that are involved include the following:

- generate_snapshot.sh : Retrieves the SCSI ID's of the coordinator disks and/or UUID ID's of the CP servers
  For information about the UUID (Universally Unique Identifier), see the *Veritas Cluster Server Administrator's Guide*.
- join_local_node.sh: Registers the keys with the coordinator disks or CP servers
- race_for_coordination_point.sh: Races to determine a winner after cluster reconfiguration
- unjoin_local_node.sh: Removes the keys that are registered in join_local_node.sh
- fence_data_disks.sh: Fences the data disks from access by the losing nodes.
- local_info.sh: Lists local node's configuration parameters and coordination points, which are used by the vxfen driver.

About the CP server database

CP server requires a database for storing the registration keys of the SF Oracle RAC cluster nodes. CP server uses a SQLite database for its operations. By default, the database is located at /etc/VRTScps/db.

For a single node VCS cluster hosting a CP server, the database can be placed on a local file system. For an SFHA cluster hosting a CP server, the database must be placed on a shared file system. The file system must be shared among all nodes that are part of the SFHA cluster.

In an SFHA cluster hosting the CP server, the shared database is protected by setting up SCSI-3 PR based I/O fencing. SCSI-3 PR based I/O fencing protects against split-brain scenarios.

Warning: The CP server database must not be edited directly and should only be accessed using `cpsadm`(1M). Manipulating the database manually may lead to undesirable results including system panics.

About the CP server user types and privileges

The CP server supports the following user types, each with a different access level privilege:

- CP server administrator (admin)
- CP server operator

Different access level privileges permit the user to issue different commands. If a user is neither a CP server admin nor a CP server operator user, then the user has guest status and can issue limited commands.

The user types and their access level privileges are assigned to individual users during SF Oracle RAC cluster configuration for fencing. During the installation process, you are prompted for a user name, password, and access level privilege (CP server admin or CP server operator).

To administer and operate a CP server, there must be at least one CP server admin.

A root user on a CP server is given all the administrator privileges, and these administrator privileges can be used to perform all the CP server specific operations.

About preferred fencing

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

You can configure the preferred fencing policy using the cluster-level attribute PreferredFencingPolicy as follows:

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

See the *Veritas Storage Foundation for Oracle RAC Administrator's Guide* for more details.

Symantec Operations Readiness Tools

Symantec™ Operations Readiness Tools (SORT) is a set of Web-based tools that supports Symantec enterprise products. SORT increases operational efficiency and helps improve application availability.

Among its broad set of features, SORT provides patches, patch notifications, and documentation for Symantec enterprise products.

To access SORT, go to:

http://sort.symantec.com

About VCS notifications

You can configure both SNMP and SMTP notifications for VCS. Symantec recommends you to configure at least one of these notifications. You have the following options:

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

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

About campus clusters

A campus cluster has alternate nodes located in different data centers. Campus clusters are connected using a high speed cable that guarantees network access between the nodes. The campus cluster configuration provides local high availability and disaster recovery functionality in a single SF Oracle RAC cluster. This configuration uses data mirroring to duplicate data at different sites.

SF Oracle RAC supports campus clusters that employ shared disk groups mirrored with Veritas Volume Manager (VxVM).

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 hardware-based or software-based replication technologies.

About Veritas Volume Replicator

Veritas Volume Replicator (VVR) is a software-based replication technology used in global cluster disaster recovery setups that replicates data to remote sites over any standard IP network. You can have up to 32 remote sites.

About database management using SF Oracle RAC

You can leverage the database management capabilities of the Storage Foundation for Databases (SFDB) tools to simplify storage management and improve database performance.

For information on supported capabilities, see the *Veritas Storage Foundation: Storage and Availability Management for Oracle Databases* guide.

About SF Oracle RAC optional components

You can add the following optional components to SF Oracle RAC:

Symantec Product Authentication Service	See "About Symantec Product Authentication Service (AT)" on page 36.
Veritas Operations Manager	See "Veritas Operations Manager" on page 36.
Cluster Manager (Java console)	See "About Cluster Manager (Java Console)" on page 37.

About Symantec Product Authentication Service (AT)

SF Oracle RAC uses Symantec Product Authentication Service (AT) to provide secure communication between cluster nodes and clients. It uses digital certificates for authentication and SSL to encrypt communication over the public network to secure communications.

AT uses the following brokers to establish trust relationship between the cluster components:

- Root broker
  A root broker serves as the main registration and certification authority; it has a self-signed certificate and can authenticate other brokers. The root broker is only used during initial creation of an authentication broker.
  A root broker on a stable external system can serve multiple clusters. Symantec recommends that you install a single root broker on a utility system. The utility system, such as an email server or domain controller, can be highly available. You can also configure one of the nodes in the SF Oracle RAC cluster to serve as a root and an authentication broker.
- Authentication brokers
  Authentication brokers serve as intermediate registration and certification authorities. Authentication brokers have root-signed certificates. Each node in VCS serves as an authentication broker.

See Symantec Product Authentication Service documentation for more information.

See "Preparing to configure the clusters in secure mode" on page 97.

Veritas Operations Manager

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

The Veritas Enterprise Administrator (VEA) console is no longer packaged with Storage Foundation products. If you wish to continue using VEA, a version is available for download from http://go.symantec.com/vcsm_download. Veritas Storage Foundation Management Server is no longer supported.

If you wish to manage a single cluster using Cluster Manager (Java Console), a version is available for download from http://go.symantec.com/vcsm_download. Veritas Cluster Server Management Console is no longer supported.

Veritas Operations Manager provides a centralized management console for Veritas Storage Foundation and High Availability products. You can use Veritas Operations Manager to monitor, visualize, and manage storage resources and generate reports. Veritas Operations Manager is not available on the Storage Foundation and High Availability Solutions release. You can download Veritas Operations Manager at no charge at http://go.symantec.com/vom.

Refer to the Veritas Operations Manger documentation for installation, upgrade, and configuration instructions.

About Cluster Manager (Java Console)

Cluster Manager (Java Console) offers complete administration capabilities for your cluster. Use the different views in the Java Console to monitor clusters and VCS objects, including service groups, systems, resources, and resource types.

See *Veritas Cluster Server Administrator's Guide*.

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

SF Oracle RAC cluster setup models

SF Oracle RAC supports a variety of cluster configurations.

Depending on your business needs, you may choose from the following setup models:

- Basic setup
  See "Typical configuration of four-node SF Oracle RAC cluster" on page 38.
- Secure setup
  See "Typical configuration of SF Oracle RAC clusters in secure mode" on page 39.
- Central management setup
  See "Typical configuration of VOM-managed SF Oracle RAC clusters" on page 40.
- Campus cluster setup

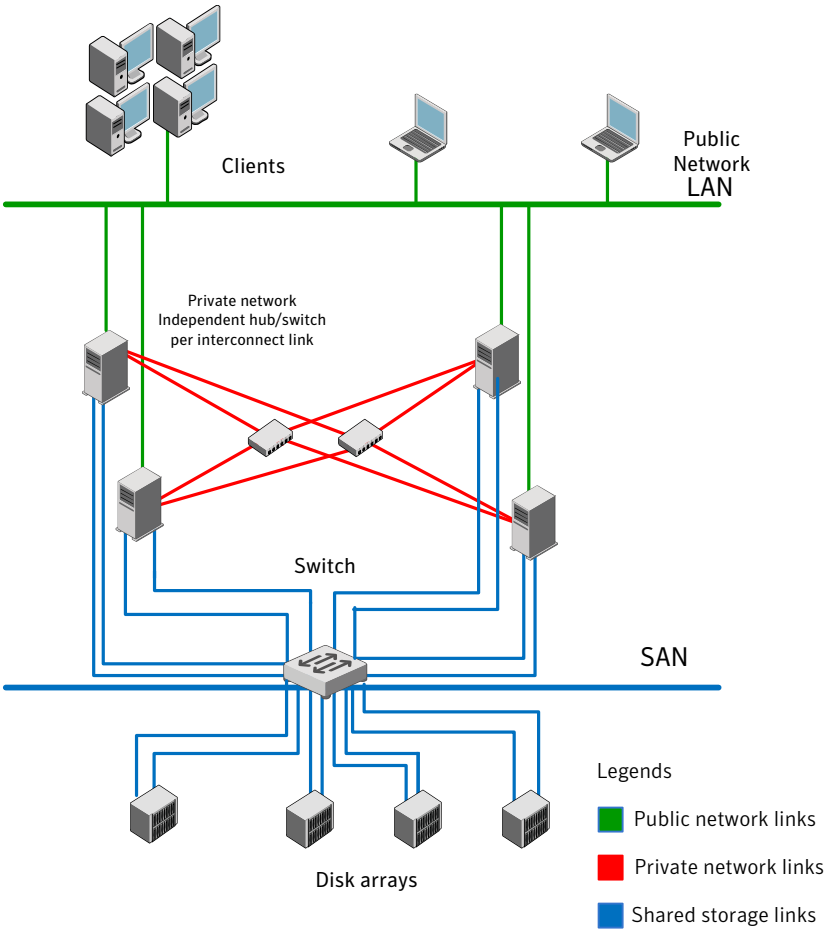
See "Typical configuration of SF Oracle RAC campus clusters for disaster recovery" on page 41.

- Global cluster setup
  See "Typical configuration of SF Oracle RAC global clusters for disaster recovery" on page 43.

Typical configuration of four-node SF Oracle RAC cluster

Figure 1-2 depicts a high-level view of a basic SF Oracle RAC configuration for a four-node cluster.

Figure 1-2 Sample four-node SF Oracle RAC 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.
  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.
- Nodes that are connected with private network links using similar network devices.
- Each system has a VxVM encapsulated root drive or an internal disk.
- The Oracle Cluster Registry and vote disks configured on the shared storage that is available to each node.
  For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: The shared storage for Oracle Cluster Registry and vote disks can be a cluster file system or raw VxVM volumes.
  For Oracle RAC 11g Release 2: The shared storage for Oracle Cluster Registry and vote disks can be a cluster file system or ASM disk groups created using raw VxVM volumes.
- Three or more odd number of disks or LUNs used as coordinator disks for I/O fencing.
- VCS manages the resources that are required by Oracle RAC. The resources must run in parallel on each node.

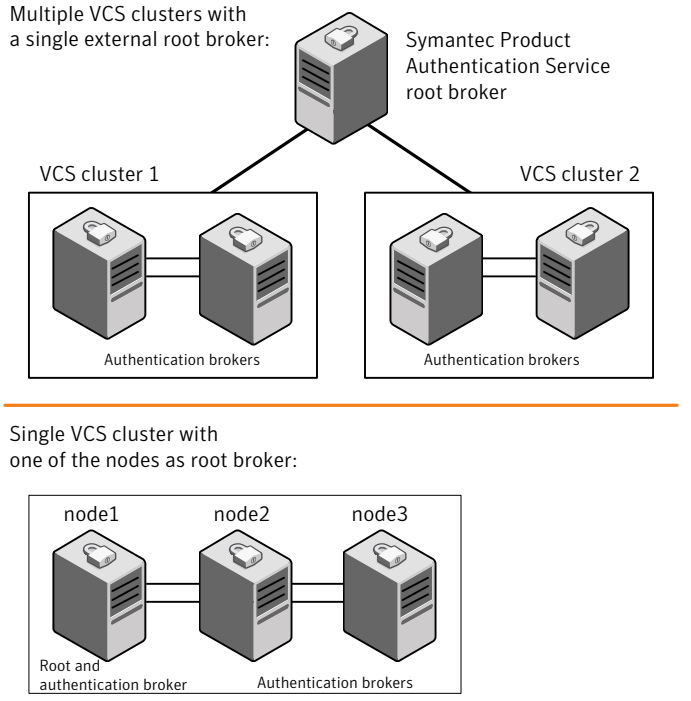
Typical configuration of SF Oracle RAC clusters in secure mode

SF Oracle RAC uses Symantec Product Authentication Service (AT) to provide secure communication between cluster nodes and clients.

See "About Symantec Product Authentication Service (AT)" on page 36.

Figure 1-3 illustrates typical configuration of VCS clusters in secure mode. You can use one of the cluster nodes as AT root broker or you can use a stable system outside the cluster as AT root broker.

Figure 1-3 Typical configuration of VCS clusters in secure mode



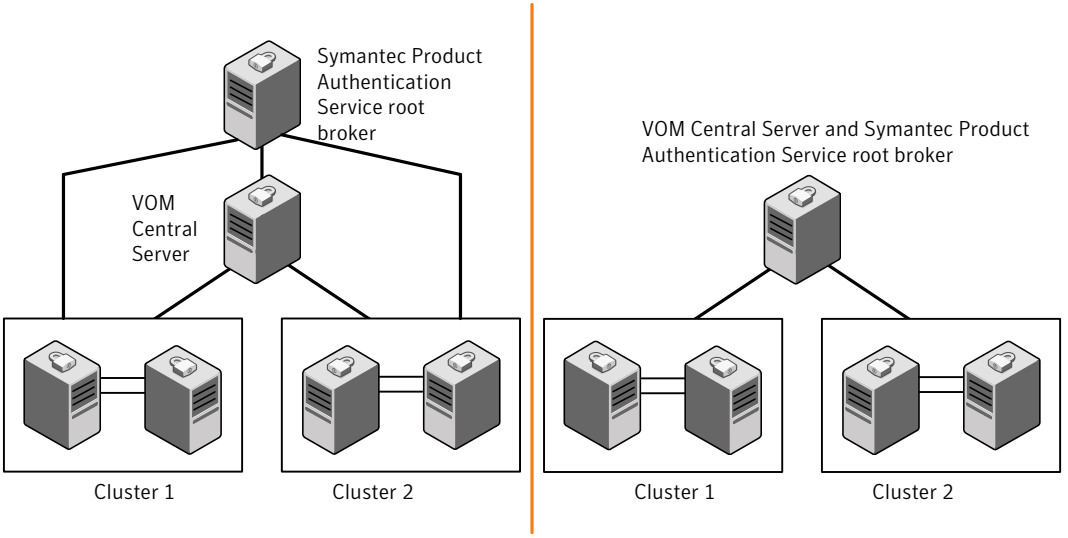
Typical configuration of VOM-managed SF Oracle RAC clusters

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

See "Veritas Operations Manager" on page 36.

Figure 1-4 illustrates a typical setup of SF Oracle RAC clusters that are centrally managed using Veritas Operations Manager. You can install Symantec Product Authentication Service root broker on the same system as that of VOM Central Server or on a different system.

Figure 1-4 Typical configuration of VOM-managed clusters



Typical configuration of SF Oracle RAC campus clusters for disaster recovery

A campus cluster configuration provides local high availability and disaster recovery capability in a single SF Oracle RAC cluster. This configuration uses data mirroring to duplicate data at different sites. No host or array replication is involved in the process. SF Oracle RAC supports campus clusters that employ shared disk groups mirrored with Cluster Volume Manager (CVM).

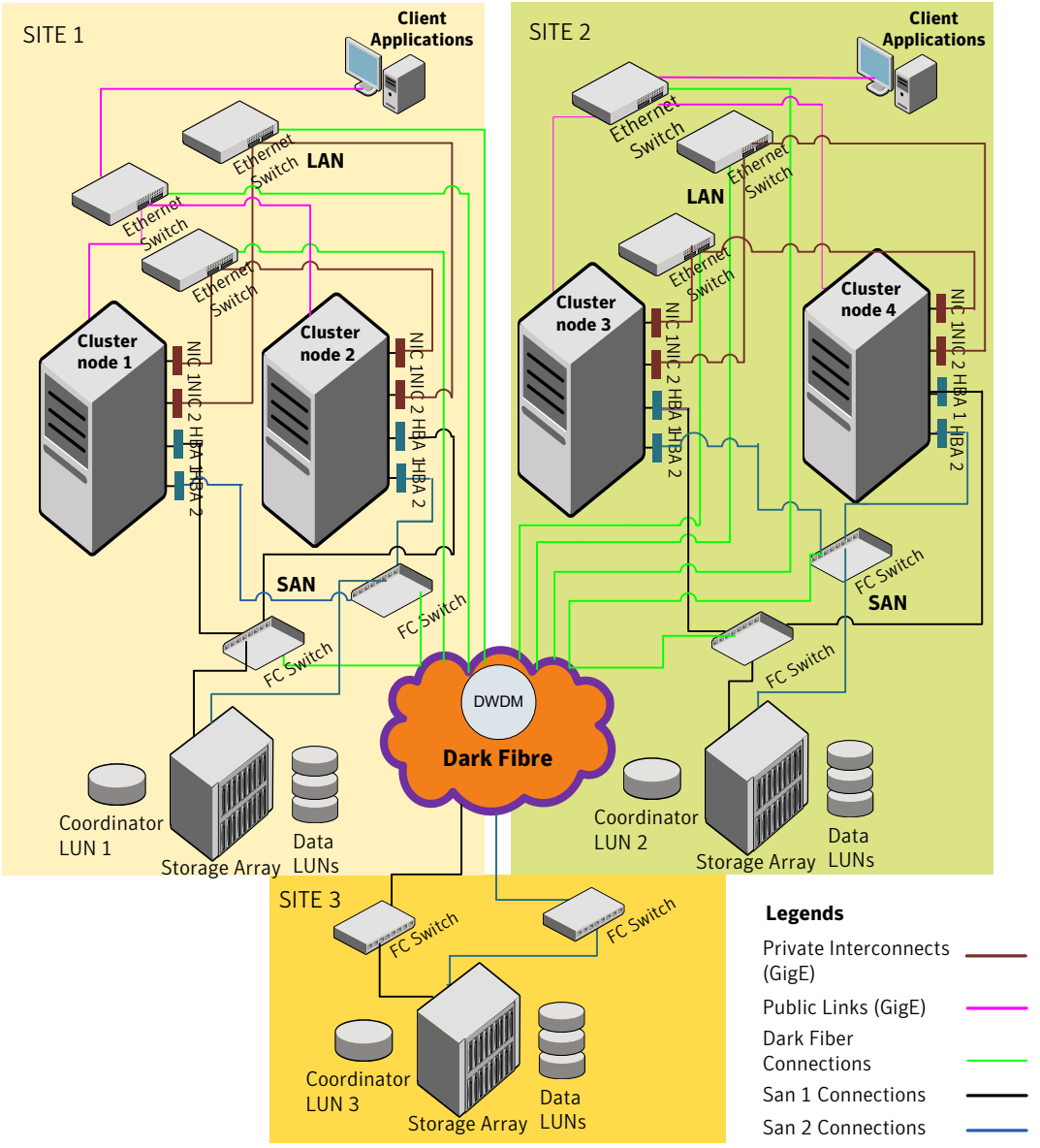
The SF Oracle RAC campus cluster addresses the following basic challenges in campus cluster configurations:

Latency challenges	An SF Oracle RAC campus cluster handles latency challenges in keeping mirrors synchronized while ensuring the efficient recovery in case of site failures for both data and VxVM metadata.
Read performance	The read performance is enhanced as data is read from local mirrors.
Site awareness	SF Oracle RAC makes sure that all the mirrors on a site are detached proactively even when a part of the site goes down.

Note: The DiskGroupSnap agent is not supported for SF Oracle RAC.

Figure 1-5 illustrates a basic campus cluster setup.

Figure 1-5 Basic campus cluster setup



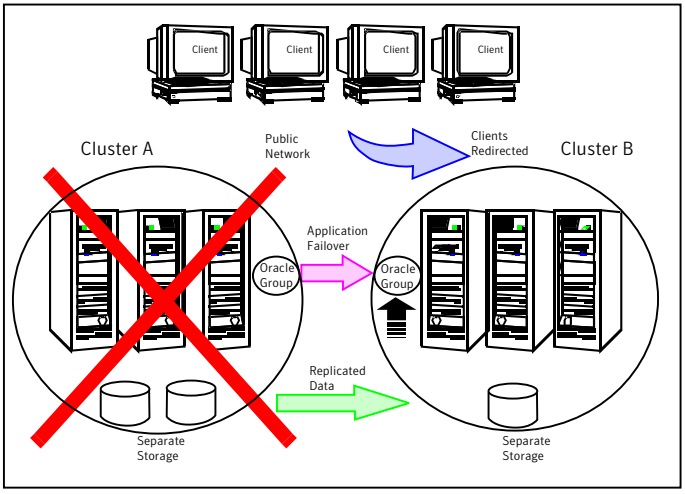
For more information, see the *Veritas Storage Foundation for Oracle RAC Installation and Configuration Guide*.

Typical configuration of SF Oracle RAC global clusters for disaster recovery

SF Oracle RAC 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 hardware-based or software-based replication technologies.

Figure 1-6 Global clusters



To understand how global clusters work, review the example of an Oracle RAC database configured using global clustering. Oracle RAC is installed and configured in cluster A and cluster B. Oracle database is located on shared disks within each cluster and is replicated across clusters to ensure data concurrency. The VCS service groups for Oracle are online on a node in cluster A and are configured to fail over on cluster A and cluster B.

VCS continuously monitors and communicates events between clusters. If cluster A fails, the Oracle database is started on the remote cluster B.

Note: You must have an SF Oracle RAC 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 Oracle RAC installation.

For information on supported replication technologies and more information, see the *Veritas Storage Foundation for Oracle RAC Installation and Configuration Guide*.

Chapter 2

System requirements

This chapter includes the following topics:

- Important preinstallation information
- Hardware requirements
- I/O fencing requirements
- Supported HP-UX operating systems
- Supported database software
- Supported replication technologies for global clusters

Important preinstallation information

Before you install SF Oracle RAC, make sure you have reviewed the following information:

- Hardware compatibility list for information about supported hardware:
  http://entsupport.symantec.com/docs/330441
- Disk storage array support information:
  http://entsupport.symantec.com/docs/283282
- Latest information on support for Oracle database versions:
  http://www.symantec.com/docs/TECH44807
- General information regarding the release, installation notes, known issues, and fixed issues:
  See *Veritas Storage Foundation for Oracle RAC Release Notes*.
- Oracle documentation for additional requirements pertaining to your version of Oracle.

Hardware requirements

Depending on the type of setup planned, make sure you meet the necessary hardware requirements.

For basic clusters See Table 2-1 on page 46.

For campus clusters See Table 2-2 on page 47.

Table 2-1 Hardware requirements for basic clusters

Item	Description
SF Oracle RAC systems	Two to sixteen HP-UX systems that are connected to the public network.
DVD drive	A DVD drive on one of the nodes in the cluster.
Disks	SF Oracle RAC requires that all storage disks support SCSI-3 Persistent Reservations (PR). **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. DMP devices are mandatory for use as coordinator disks.
Disk space	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: `# ./installsfrac -precheck node_name` For details on the additional space that is required for Oracle, see the Oracle documentation.
RAM	Each SF Oracle RAC system requires at least 2 GB. Symantec recommends additional amount of at least twice the Oracle SGA size.
Swap space	See the Oracle Metalink document: 169706.1

Table 2-1 Hardware requirements for basic clusters *(continued)*

Item	Description
Network links	Two or more private links and one public link. 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. Symantec recommends gigabit Ethernet using enterprise-class switches for the private links. You can also configure aggregated interfaces.
Fiber Channel or SCSI host bus adapters	At least one additional SCSI or Fibre Channel Host Bus Adapter per system for shared data disks.

Table 2-2 lists the hardware requirements for campus clusters in addition to the basic cluster requirements.

Table 2-2 Hardware requirements for campus clusters

Item	Description
Storage	■ The storage switch (to which each host on a site connects) must have access to storage arrays at all the sites. ■ Volumes must be mirrored with storage allocated from at least two sites. ■ DWDM links are recommended between sites for storage links. DWDM works at the physical layer and requires multiplexer and de-multiplexer devices. ■ The storage and networks must have redundant-loop access between each node and each storage array to prevent the links from becoming a single point of failure.
Network	■ Oracle requires that all nodes use the IP addresses from the same subnet. ■ Symantec recommends two Network Interface Cards (NIC) per host for LLT heartbeats. Oracle Clusterware requires one private and one virtual IP for each host. ■ Symantec recommends a common cross-site physical infrastructure for storage and LLT private networks.
I/O fencing	I/O fencing requires placement of a third coordinator disk at a third site. The DWDM can be extended to the third site or the iSCSI LUN at the third site can be used as the third coordination point. Alternatively Coordination Point Server can be deployed at the third remote site as an arbitration point.

I/O fencing requirements

Depending on whether you plan to configure disk-based fencing or server-based fencing, make sure that you meet the requirements for coordination points:

- Coordinator disks
  See "Coordinator disk requirements for I/O fencing" on page 48.
- CP servers
  See "CP server requirements" on page 48.

Coordinator disk requirements for I/O fencing

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

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

CP server requirements

SF Oracle RAC 5.1SP1 clusters (application clusters) support CP servers which are hosted on the following VCS and SFHA versions:

- VCS 5.1 or 5.1SP1 single-node cluster
  CP server requires LLT and GAB to be configured on the single-node VCS cluster that hosts CP server. This requirement also applies to any single-node application cluster that uses server-based fencing.
- SFHA 5.1 or 5.1SP1 cluster

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

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

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

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

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

- Hardware requirements
- Operating system requirements
- Networking requirements (and recommendations)
- Security requirements

Table 2-3 lists additional requirements for hosting the CP server.

Table 2-3 CP server hardware requirements

Hardware required	Description
Disk space	To host the CP server on a VCS cluster or SFHA cluster, each host requires the following file system space: ■ 550 MB in the /opt directory (additionally, the language pack requires another 15 MB) ■ 300 MB in /usr ■ 20 MB in /var
Storage	When CP server is hosted on an SFHA cluster, there must be shared storage between the CP servers.
RAM	Each CP server requires at least 512 MB.

Table 2-3 CP server hardware requirements *(continued)*

Hardware required	Description
CP server to client node physical link	A secure TCP/IP connection is required to connect the CP servers to the SF Oracle RAC clusters (application clusters).

Table 2-4 displays the CP server supported operating systems and versions. An application cluster can use a CP server that runs any of the following supported operating systems.

Table 2-4 CP server supported operating systems and versions

CP server	Operating system and version

CP server hosted on a VCS single-node cluster or on an SFHA cluster	CP server supports any of the following operating systems:
	■ AIX 5.3 and 6.1
	■ HP-UX 11i v3
	■ Linux:
	  ■ RHEL 5
	  ■ SLES 10
	  ■ SLES 11
	■ Solaris 9 and 10
	Review other details such as supported operating system levels and architecture for the supported operating systems.
	See the *Veritas Cluster Server Installation Guide* or the *Veritas Storage Foundation High Availability Installation Guide*.

Following are the CP server networking requirements and recommendations:

- Symantec recommends that network access from the application clusters to the CP servers should be made highly-available and redundant. The network connections require either a secure LAN or VPN.
- The CP server uses the TCP/IP protocol to connect to and communicate with the application clusters by these network paths. The CP server listens for messages from the application clusters using TCP port 14250. This is the default port that can be changed during a CP server configuration.
- The CP server supports either Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with the application clusters. If the CP server is configured to use an IPv6 virtual IP address, then the application clusters should also be on the IPv6 network where the CP server is being hosted.

- When placing the CP servers within a specific network configuration, you must take into consideration the number of hops from the different application cluster nodes to the CP servers. As a best practice, Symantec recommends that the number of hops from the different application cluster nodes to the CP servers should be equal. This ensures that if an event occurs that results in an I/O fencing scenario, there is no bias in the race due to the number of hops between the nodes.

For secure communications between the SF Oracle RAC cluster and CP server, consider the following requirements and suggestions:

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

For information about establishing secure communications between the application cluster and CP server, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

Supported HP-UX operating systems

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

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

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

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

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

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

Supported database software

For the latest information on supported Oracle database versions, see the following Technical Support TechNote:

http://www.symantec.com/docs/TECH44807

Note: SF Oracle RAC supports only 64-bit Oracle.

The following database versions are supported:

- Oracle RAC 10g Release 2
- Oracle RAC 11g Release 1
- Oracle RAC 11g Release 2

Additionally, see the Oracle documentation for patches that may be required by Oracle for each release.

Supported replication technologies for global clusters

SF Oracle RAC supports the following hardware-based replication and software-based replication technologies for global cluster configurations:

Hardware-based replication	■ EMC SRDF ■ Hitachi TrueCopy ■ IBM Metro Mirror ■ IBM SAN Volume Controller (SVC) ■ EMC MirrorView
Software-based replication	■ Veritas Volume Replicator ■ Oracle Data Guard

Chapter 3

Planning to install SF Oracle RAC

This chapter includes the following topics:

- Planning your network configuration
- Planning the storage
- Planning volume layout
- Planning file system design
- About planning to configure I/O fencing
- Planning for cluster management
- Planning for disaster recovery

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. The value should be set based on service availability requirements and the propagation

delay between the cluster nodes in case of campus cluster setup. The LLT peer inactivity timeout value indicates the interval after which SF Oracle RAC on one node declares the other node in the cluster dead, if there is no network communication (heartbeat) from that node.

The default value for the CSS miss-count in case of SF Oracle RAC is 600 seconds. The value of this parameter is much higher than the LLT peer inactivity timeout so that the two clusterwares, VCS and Oracle Clusterware, do not interfere with each other's decisions on which nodes should remain in the cluster in the event of network split-brain. Veritas I/O fencing is allowed to decide on the surviving nodes first, followed by Oracle Clusterware. The CSS miss-count value indicates the amount of time Oracle Clusterware waits before evicting another node from the cluster, when it fails to respond across the interconnect.

For more information, see the Oracle Metalink document: 782148.1

Planning the public network configuration for Oracle RAC

Identify separate public virtual IP addresses for each node in the cluster. Oracle requires one public virtual IP address for the Oracle listener process on each node. Public virtual IP addresses are used by client applications to connect to the Oracle database and help mitigate TCP/IP timeout delays. Oracle Clusterware manages the virtual IP addresses.

Planning the private network configuration for Oracle RAC

Oracle RAC requires a minimum of one private IP address for Oracle Clusterware heartbeat.

Depending on the version of Oracle RAC you want to install, use one of the following options for setting up the private network configuration for Oracle database cache fusion:

Oracle RAC 10g	Use either Oracle UDP IPC or VCSIPC/LMX/LLT for the database cache fusion traffic. By default, the database cache fusion traffic is configured to use VCSIPC/LMX/LLT.
Oracle RAC 11g	You must use UDP IPC for the database cache fusion traffic.

The Oracle UDP IPC protocol requires an IP address. Symantec recommends that an additional private IP address from a different subnet be used for load balancing the Oracle cache fusion traffic.

Note: Oracle UDP IPC is supported for both Oracle RAC 10g and Oracle RAC 11g with SF Oracle RAC.

Note: The private IP addresses of all nodes that are on the same physical network must be in the same IP subnet.

The following practices provide a resilient private network setup:

- Configure Oracle Clusterware interconnects over LLT links to prevent data corruption.
  In an SF Oracle RAC cluster, the Oracle Clusterware heartbeat link MUST be configured as an LLT link. If Oracle Clusterware and LLT use different links for their communication, then the membership change between VCS and Oracle Clusterware is not coordinated correctly. For example, if only the Oracle Clusterware links are down, Oracle Clusterware kills one set of nodes after the expiry of the css-misscount interval and initiates the Oracle Clusterware and database recovery, even before CVM and CFS detect the node failures. This uncoordinated recovery may cause data corruption.
- Oracle Clusterware interconnects need to be protected against NIC failures and link failures. The PrivNIC or MultiPrivNIC agent can be used to protect against NIC failures and link failures, if multiple links are available. Even if link aggregation solutions in the form of bonded NICs are implemented, the PrivNIC or MultiPrivNIC agent can be used to provide additional protection against the failure of the aggregated link by failing over to available alternate links. These alternate links can be simple NIC interfaces or bonded NICs.
  An alternative option is to configure the Oracle Clusterware interconnects over bonded NIC interfaces.
  See "High availability solutions for Oracle RAC private network" on page 56.
- Configure Oracle Cache Fusion traffic to take place through the private network. Symantec also recommends that all UDP cache-fusion links be LLT links.
  Oracle database clients use the public network for database services. Whenever there is a node failure or network failure, the client fails over the connection, for both existing and new connections, to the surviving node in the cluster with which it is able to connect. Client failover occurs as a result of Oracle Fast Application Notification, VIP failover and client connection TCP timeout. It is strongly recommended not to send Oracle Cache Fusion traffic through the public network.
- Use NIC bonding to provide redundancy for public networks so that Oracle can fail over virtual IP addresses if there is a public link failure.

High availability solutions for Oracle RAC private network

Table 3-1 lists the high availability solutions that you may adopt for your private network.

Table 3-1 High availability solutions for Oracle RAC private network

Options	Description
Using link aggregation/ NIC bonding for Oracle Clusterware	Use a native NIC bonding solution to provide redundancy, in case of NIC failures. Make sure that a link configured under a aggregated link or NIC bond is not configured as a separate LLT link. When LLT is configured over a bonded interface, do one of the following steps to prevent GAB from reporting jeopardy membership: ■ Configure an additional NIC under LLT in addition to the bonded NIC. ■ Add the following line in the `/etc/llttab` file: `set-dbg-minlinks 2`
Using PrivNIC/MultiPrivNIC agents	Use the PrivNIC agent when operating system limitations prevent you from using NIC bonding to provide high availability using multiple network interfaces. Use the MultiPrivNIC agent when operating system limitations prevent you from using NIC bonding to provide high availability and increased bandwidth using multiple network interfaces. For more deployment scenarios that illustrate the use of PrivNIC/MultiPrivNIC deployments, see the appendix "SF Oracle RAC deployment scenarios" in this document.

Planning the storage

SF Oracle RAC provides the following options for shared storage:

- CVM
  CVM provides native naming 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

- Oracle ASM over CVM

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 Oracle RAC

Table 3-2 lists the type of storage required for SF Oracle RAC.

Table 3-2 Type of storage required for SF Oracle RAC

SF Oracle RAC files	Type of storage
SF Oracle RAC binaries	Local
SF Oracle RAC fencing coordinator disks	Shared

Planning the storage for Oracle RAC

Review the storage options and guidelines for Oracle RAC:

- Storage options for OCR and voting disk
  See "Planning the storage for OCR and voting disk" on page 57.
- Storage options for the Oracle RAC installation directories (ORACLE_BASE, CRS_HOME or GRID_HOME (depending on Oracle RAC version), and ORACLE_HOME)
  See "Planning the storage for Oracle RAC binaries and data files" on page 59.

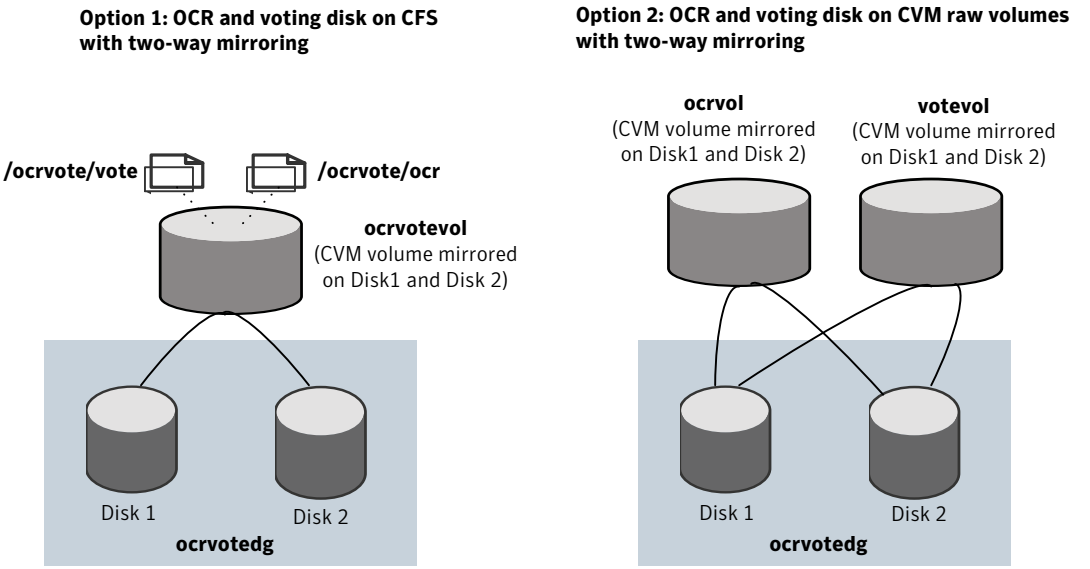
Planning the storage for OCR and voting disk

Depending on the Oracle RAC version, use one of the following options to place the OCR and voting disk information:

Oracle RAC 10g Release 2/ Oracle RAC 11g Release 1	Clustered File System CVM raw volumes
Oracle RAC 11g Release 2	Clustered File System ASM disk groups created using CVM raw volumes

Figure 3-1 illustrates the options for storing OCR and voting disk information.

Figure 3-1 OCR and voting disk storage options



- If you want to place OCR and voting disk on a clustered file system (option 1), you need to have two separate files for OCR and voting information respectively on CFS mounted on a CVM mirrored volume.
- If you want to place OCR and voting disk on CVM raw volumes or on ASM disk groups that use CVM raw volumes (option 2), you need to use two CVM mirrored volumes for configuring OCR and voting disk on these volumes.

For both option 1 and option 2:

- The installer needs at least two LUNs of 640 MB each for creating the OCR and voting disk storage.
  Additionally, refer to the Oracle documentation for Oracle's recommendation on the required disk space for OCR and voting disk.
- The option **External Redundancy** must be selected at the time of installing Oracle Clusterware.

Note: Update the default setting of the CVM disk group fail policy to `leave` for OCR and voting disk. Retain the default setting (`global`) for the disk detach policy.

Once you have planned for the storage, you need to create the storage for OCR and voting disk manually as described later in the chapter "Installing Oracle RAC".

Note: For setting up replicated clusters, OCR and voting disk must be on non-replicated shared storage.

Planning the storage for Oracle RAC binaries and data files

The Oracle RAC binaries can be stored on local storage or on shared storage, based on your high availability requirements.

Note: Symantec recommends that you install the Oracle Clusterware and Oracle database binaries local to each node in the cluster.

Consider the following points while planning the installation:

- Local installations provide improved protection against a single point of failure and also allows for applying Oracle RAC patches in a rolling fashion.
- CFS installations provide a single Oracle installation to manage, regardless of the number of nodes. This scenario offers a reduction in storage requirements and easy addition of nodes.

Table 3-3 lists the type of storage for Oracle RAC binaries and data files.

Table 3-3 Type of storage for Oracle RAC binaries and data files

Oracle RAC files	Type of storage
Oracle base	Local The ORACLE_BASE directory specified during the Oracle Clusterware/Grid Infrastructure installation is used to store the Oracle Inventory files. Oracle requires that the Oracle inventory files be placed on the local file system.
Oracle Clusterware	Local or shared
Oracle Grid Infrastructure binaries	Local Placing the Oracle Grid Infrastructure binaries on local disks enables rolling upgrade of the cluster.

Table 3-3 Type of storage for Oracle RAC binaries and data files *(continued)*

Oracle RAC files	Type of storage
Oracle database binaries	Local or shared Placing the Oracle database binaries on local disks enables rolling upgrade of the cluster.
Database datafiles	Shared Store the Oracle database files on CFS rather than on raw device or CVM raw device for easier management. Create separate clustered file systems for each Oracle database. Keeping the Oracle database datafiles on separate mount points enables you to unmount the database for maintenance purposes without affecting other databases. **Note:** Set the CVM disk group fail policy to `leave` for disk groups containing the data files. If you plan to store the Oracle database on ASM, configure the ASM disk groups over CVM volumes to take advantage of dynamic multi-pathing.
SF Oracle RAC database storage management repository	Shared
Database recovery data (archive, flash recovery)	Shared Place archived logs on CFS rather than on local file systems.

Planning for Oracle ASM over CVM

Review the following information on storage support provided by Oracle ASM:

Supported by ASM

ASM provides storage for data files, control files, online and archive log files, and backup files. Starting with Oracle RAC 11g Release 2, ASM also supports storage for OCR and voting disk.

Not supported by ASM	Oracle RAC 11g Release 1 and earlier versions: ASM does not support Oracle binaries, trace files, alert logs, export files, tar files, core files, Oracle Cluster Registry devices (OCR), and voting disk, and application binaries on ASM. Oracle RAC 11g Release 2: ASM does not support Oracle binaries, trace files, alert logs, export files, tar files, core files, and application binaries on ASM.

The following practices offer high availability and better performance:

- Use VxVM mirrored volumes with dynamic multi-pathing with external redundancy to ensure high availability.
- Do not use VxVM volumes, which are used by ASM, for any other purpose such as creation of file systems.
- Do not enable ODM when databases are created on ASM.

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.
- Separate the Oracle recovery structures from the database files to ensure high availability when you design placement policies.
- Separate redo logs and place them on the fastest storage (for example, RAID 1+ 0) for better performance.
- Use "third-mirror break-off" snapshots for cloning the Oracle log volumes. Do not create Oracle log volumes on a Space-Optimized (SO) snapshot.
- Create as many Cache Objects (CO) as possible when you use Space-Optimized (SO) snapshots for Oracle data volumes.
- Distribute the I/O load uniformly on all Cache Objects when you create multiple Cache Objects.
- If using VxVM mirroring, 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.

- 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.

Planning file system design

The following recommendations ensure an optimal file system design for databases:

- If using VxVM mirroring, use ODM with CFS for better performance. ODM with SmartSync enables faster recovery of mirrored volumes using Oracle resilvering.
- Create separate file systems for Oracle binaries, data, redo logs, and archive logs. This ensures that recovery data is available if you encounter problems with database data files storage.
- Always place archived logs on CFS file systems rather then local file systems.

About planning to configure I/O fencing

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

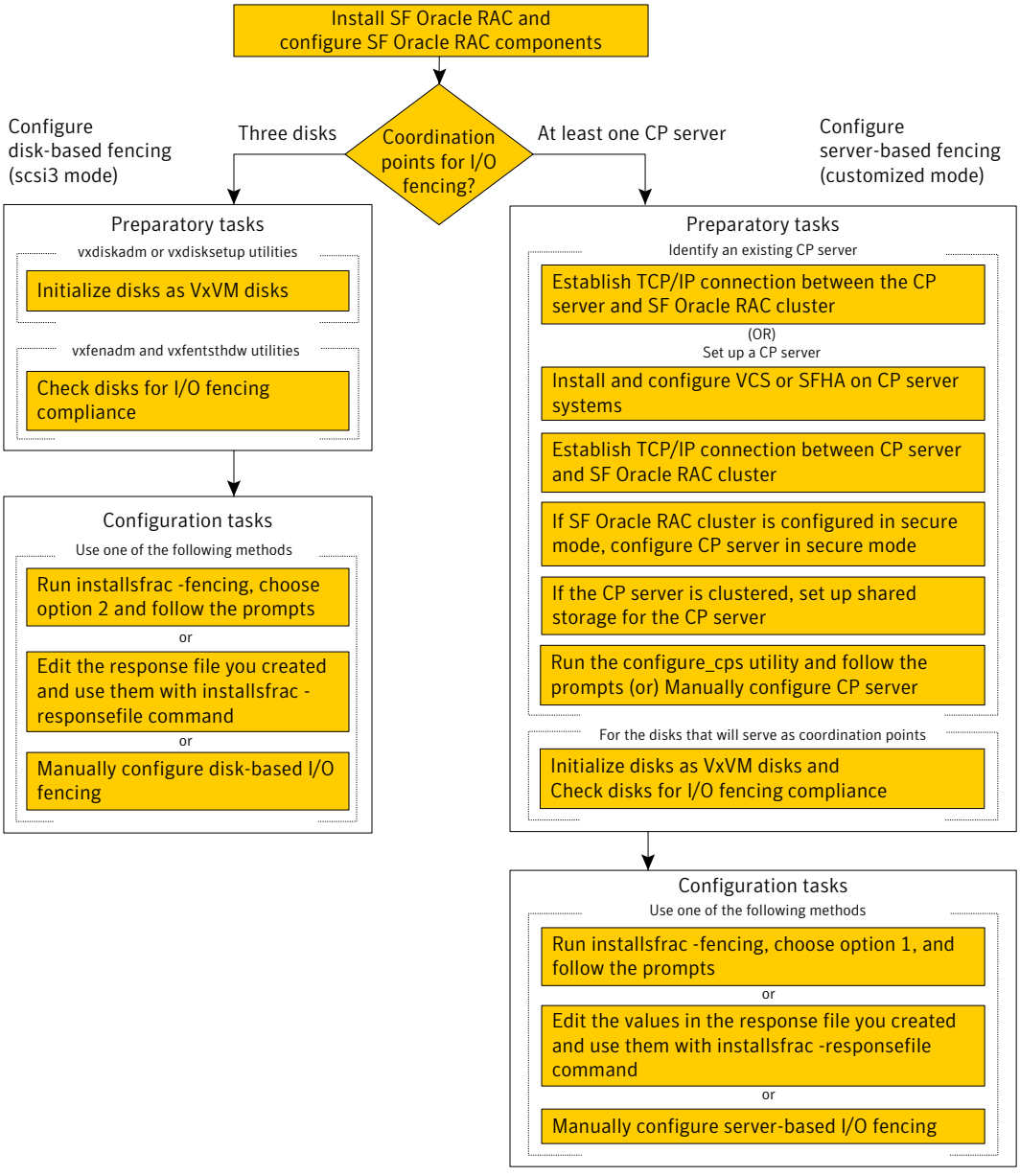
You can configure either disk-based I/O fencing or server-based I/O fencing. If your enterprise setup has multiple clusters that use VCS for clustering, Symantec recommends you to configure server-based I/O fencing.

The coordination points in server-based fencing can include only CP servers or a mix of CP servers and coordinator disks. Symantec also supports server-based fencing with a a single coordination point which is a single highly available CP server that is hosted on an SFHA cluster.

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

Figure 3-2 illustrates a high-level flowchart to configure I/O fencing for the SF Oracle RAC cluster.

Figure 3-2 Workflow to configure I/O fencing



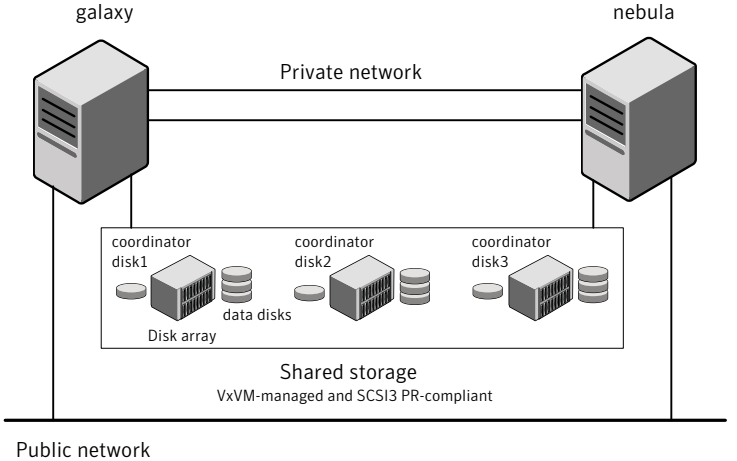
After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:

Using the installsfrac program	See "Setting up disk-based I/O fencing using installsfrac program" on page 147. See "Setting up server-based I/O fencing using installsfrac program" on page 161.
Using response files	See "Response file variables to configure disk-based I/O fencing" on page 407. See "Response file variables to configure server-based I/O fencing" on page 409. See "Response file variables to configure server-based I/O fencing" on page 409. See "Configuring I/O fencing using response files" on page 385.
Manually editing configuration files	See "Setting up disk-based I/O fencing manually" on page 155. See "Setting up server-based I/O fencing manually" on page 172.

Typical SF Oracle RAC cluster configuration with disk-based I/O fencing

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

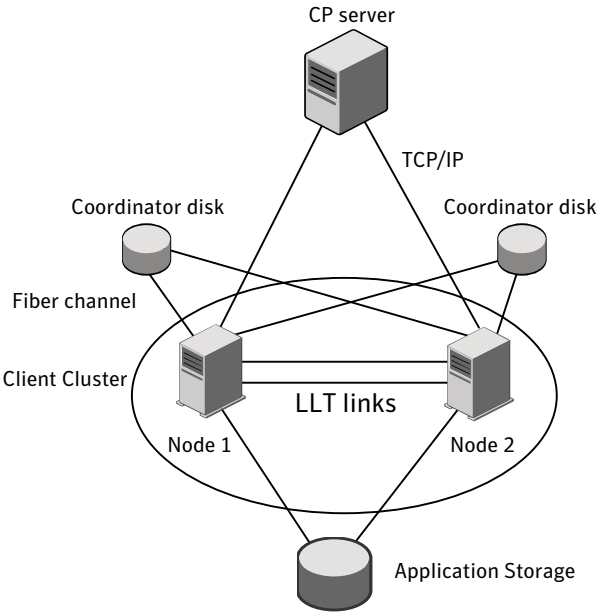
Figure 3-3 Typical SF Oracle RAC cluster configuration with disk-based I/O fencing



Typical SF Oracle RAC cluster configuration with server-based I/O fencing

Figure 3-4 displays a configuration using a SF Oracle RAC cluster (with two nodes), a single CP server, and two coordinator disks. The nodes within the SF Oracle RAC cluster are connected to and communicate with each other using LLT links.

Figure 3-4 CP server, SF Oracle RAC cluster, and coordinator disks



Recommended CP server configurations

Following are the recommended CP server configurations:

- Multiple application clusters use three CP servers as their coordination points.
  See Figure 3-5 on page 66.
- Multiple application clusters use a single CP server and multiple pairs of coordinator disks (two) as their coordination points.
  See Figure 3-6 on page 67.
- Multiple application clusters use a single CP server as their coordination point
  This single coordination point fencing configuration must use a highly available CP server that is configured on an SFHA cluster as its coordination point.
  See Figure 3-7 on page 67.

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

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

Figure 3-5 displays a configuration using three CP servers that are connected to multiple application clusters.

Figure 3-5 Three CP servers connecting to multiple application clusters

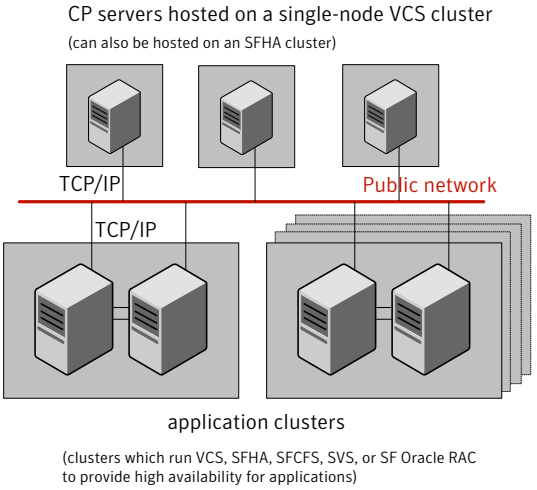


Figure 3-6 displays a configuration using a single CP server that is connected to multiple application clusters with each application cluster also using two coordinator disks.

Figure 3-6 Single CP server with two coordinator disks for each application cluster

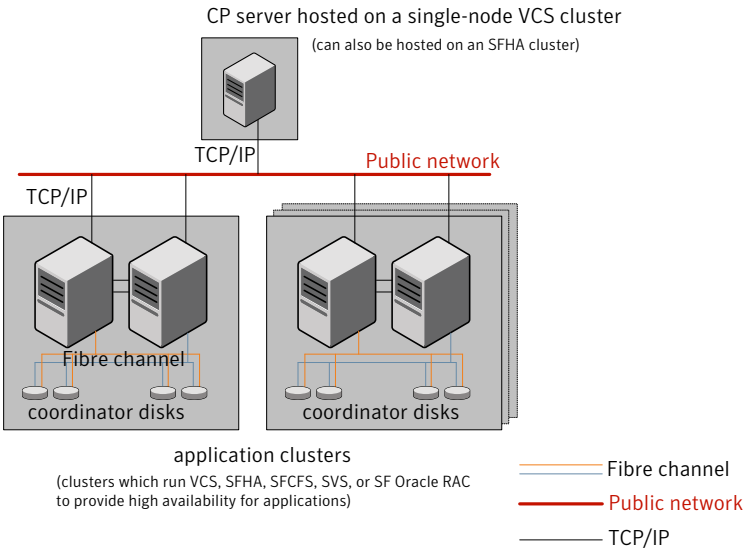
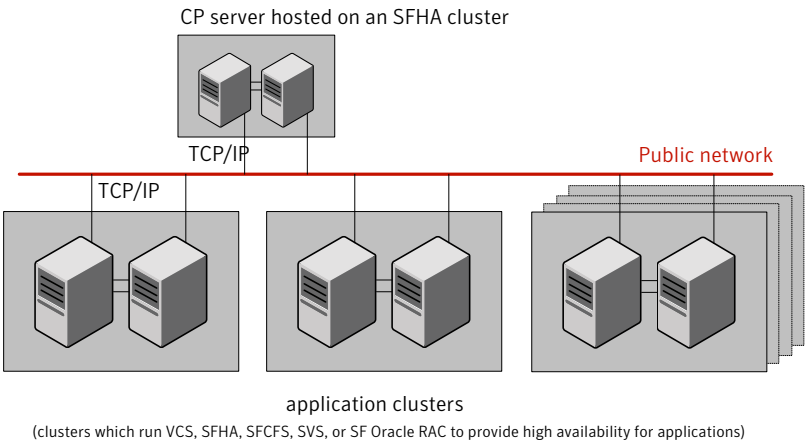


Figure 3-7 displays a configuration using a single CP server that is connected to multiple application clusters.

Figure 3-7 Single CP server connecting to multiple application clusters



See "Configuration diagrams for setting up server-based I/O fencing" on page 736.

Planning for cluster management

Table 3-4 lists the various agents supported in SF Oracle RAC installations for effective cluster management.

Table 3-4 List of agents

Agent	Description
VCS agent for Oracle	Oracle database management The VCS Oracle agent is recommended for managing Oracle databases. VCS controls the Oracle database in this configuration. The configuration without VCS Oracle agent may be used only in a single database setup.
VCS agent for CVM	Volume management An SF Oracle RAC installation automatically configures the CVMCluster resource and the CVMVxconfigd resource. You must configure the CVMVolDg agent for each shared disk group.
VCS agent for CFS	File system management If the database uses cluster file systems, configure the CFSMount agent for each volume in the disk group.
CSSD agent	Oracle Clusterware management The CSSD agent starts, stops, and monitors Oracle Clusterware. It ensures that the OCR, the voting disk and the private IP address resources required by Oracle Clusterware are online before Oracle Clusterware starts. **Note:** It is mandatory to use CSSD agent in SF Oracle RAC installations to ensure adequate handling of inter-dependencies and thereby prevent the premature startup of Oracle Clusterware.
PrivNIC agent	High availability for a private IP address The PrivNIC agent provides a reliable alternative when operating system limitations prevent you from using NIC bonding to provide high availability using multiple network interfaces.
MultiPrivNIC agent	High availability for multiple private IP addresses The MultiPrivNIC agent provides a reliable alternative when operating system limitations prevent you from using NIC bonding to provide high availability and increased bandwidth using multiple network interfaces.

Table 3-4 List of agents *(continued)*

Agent	Description
CRSResource agent	Oracle database management The CRSResource agent provides an alternative mechanism for monitoring the Oracle database in the absence of the VCS Oracle agent. It is useful in scenarios where the database is not managed by VCS and the applications need to be started using VCS after Oracle Clusterware starts the database.

Planning for disaster recovery

SF Oracle RAC provides various disaster recovery configurations, such as campus clusters and global clusters, for multi-site clusters. In multi-site clusters, the nodes can be placed in different parts of a building, in separate buildings, or in separate cities. The distance between the nodes depends on the type of disaster from which protection is needed and on the technology used to replicate data. SF Oracle RAC supports various replication technologies for data replication.

To protect clusters against outages caused by disasters, the cluster components must be geographically separated.

Planning a campus cluster setup

A campus cluster is also known as a stretch cluster or remote mirror configuration. In a campus cluster, the hosts and storage of a cluster span multiple sites separated by a few miles.

Bear in mind the following best practices mind when you configure a SF Oracle RAC campus cluster:

- Campus cluster sites are typically connected using a redundant high-capacity network that provides access to storage and private network communication between the cluster nodes. A single DWDM link can be used for both storage and private network communication.
- Tag the disks or enclosures that belong to a site with the corresponding VxVM site name. VxVM allocates storage from the correct site when creating or resizing a volume and when changing a volume's layout if the disks in the VxVM disk group that contain the volume are tagged with the site name.
- Tag each host with the corresponding VxVM site name. Make sure the read policy of the volumes is set to `SITEREAD`. This setting ensures that the reads on the volumes are satisfied from the local site's plex.

- Turn on the `allsites` attribute for all volumes that have data required by the application, to make sure they are evenly mirrored. Each site must have at least one mirror of all volumes hosting application data, including the FlashSnap log volume.
- In the case of a two-site campus cluster, place the third coordinator disk on the third site. You may use iSCSI disk on the third site as an alternative to Dark Fiber connected FC-SAN disk.
  Starting with version 5.1, you may use the software-based arbitration solution, Coordination Point Server (CPS), as a third coordination point.
- Turn on the `siteconsistent` attribute for the disk groups and the volumes to enable site-aware plex detaches. Snapshot volumes need not be site-consistent.
- Make sure that a DCO log version 20 or higher is attached to the volumes to enable Fast Resync operations.
- Set the CVM disk detach policy as "global" and the disk group fail policy as "leave" for all disk groups containing data volumes as well as disk groups containing the OCR and VOTE volumes.

Planning a global cluster setup

Global clusters provide the ability to fail over applications between geographically distributed clusters when a disaster occurs.

Global clustering involves two steps:

1. Replication of data between the sites
2. Migration of the application when disaster occurs

The following aspects need to be considered when you design a disaster recovery solution:

- The amount of data lost in the event of a disaster (Recovery Point Objective)
- The acceptable recovery time after the disaster (Recovery Time Objective)

Data replication considerations

When you choose a replication solution, one of the important factors that you need to consider is the required level of data throughput. Data throughput is the rate at which the application is expected to write data. The impact of write operations on replication are of more significance than the read operations.

In addition to the business needs discussed earlier, the following factors need to be considered while choosing the replication options:

- Mode of replication
- Network bandwidth
- Network latency between the two sites
- Ability of the remote site to keep up with the data changes at the first site

Chapter 4

Licensing SF Oracle RAC

This chapter includes the following topics:

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

About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

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

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

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

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See "Setting or changing the product level for keyless licensing" on page 76.
  See the `vxkeyless(1m)` manual page.
- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.
  See "Installing Veritas product license keys" on page 77.
  See the `vxlicinst(1m)` manual page.

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

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

About SF Oracle RAC licenses

Table 4-1 lists the various SF Oracle RAC license levels in keyless licensing and the corresponding features.

Table 4-1 SF Oracle RAC license levels (keyless licensing)

License	Description	Features enabled
SFRACENT	SF Oracle RAC Enterprise Edition	The license enables the following features: ■ Veritas Volume Manager ■ Veritas Storage and Availability Management Tools for Oracle databases ■ Veritas Extension for ODM ■ Veritas File System ■ Veritas Cluster Server ■ Veritas Mapping Services
SFRACENT_VVR	SF Oracle RAC Enterprise Edition with VVR	The license enables the following features: ■ Veritas Volume Manager Veritas Volume Replicator is enabled. ■ Veritas Storage and Availability Management Tools for Oracle databases ■ Veritas Extension for ODM ■ Veritas File System ■ Veritas Cluster Server ■ Veritas Mapping Services
SFRACENT_GCO	SF Oracle RAC Enterprise Edition with Global Cluster Option (GCO)	The license enables the following features: ■ Veritas Volume Manager ■ Veritas Storage and Availability Management Tools for Oracle databases ■ Veritas Extension for ODM ■ Veritas File System ■ Veritas Cluster Server Global Cluster Option is enabled. ■ Veritas Mapping Services

Table 4-1 SF Oracle RAC license levels (keyless licensing) *(continued)*

License	Description	Features enabled
SFRACENT_VVR_GCO	SF Oracle RAC Enterprise Edition with VVR and GCO	The license enables the following features: ■ Veritas Volume Manager Veritas Volume Replicator is enabled. ■ Veritas Storage and Availability Management Tools for Oracle databases ■ Veritas Extension for ODM ■ Veritas File System ■ Veritas 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 Veritas products and functionality that are licensed. In order to use keyless licensing, you must set up a Management Server to manage your systems.

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

http://go.symantec.com/vom

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

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

To set or change the product level

1 View the current setting for the product level.

```
# vxkeyless -v display
```

2 View the possible settings for the product level.

```
# vxkeyless displayall
```

3 Set the desired product level.

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

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

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

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

To clear the product license level

1 View the current setting for the product license level.

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

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

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

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

Installing Veritas product license keys

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

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

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

To install a new license

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

```
# cd /opt/VRTS/bin

# ./vxlicinst -k xxxx-xxxx-xxxx-xxxx-xxxx-xxx
```

Section 2

Installation and configuration of SF Oracle RAC

- Chapter 5. Preparing to install SF Oracle RAC
- Chapter 6. Installing SF Oracle RAC
- Chapter 7. Preparing to configure SF Oracle RAC
- Chapter 8. Configuring SF Oracle RAC
- Chapter 9. Configuring SF Oracle RAC clusters for data integrity
- Chapter 10. Performing post-installation and configuration tasks

Chapter 5

Preparing to install SF Oracle RAC

This chapter includes the following topics:

- Setting the umask before installation
- Synchronizing time settings on cluster nodes
- Mounting the product disc
- Setting up shared storage
- Setting the environment variables
- Optimizing LLT media speed settings on private NICs
- Verifying the systems before installation

Setting the umask before installation

Set the umask to provide appropriate permissions for SF Oracle RAC binaries and files. This setting is valid only for the duration of the current session.

```
# umask 0022
```

Synchronizing time settings on cluster nodes

Make sure that the time settings on all cluster nodes are synchronized.

Note: For Oracle RAC 11g Release 2, it is mandatory to configure NTP for synchronizing time on all nodes in the cluster.

Mounting the product disc

You must have superuser (root) privileges to load the SF Oracle RAC software.

You can unmount the product disc after completing the SF Oracle RAC installation.

To mount the product disc

1. Log in as the superuser to a cluster node or a remote node in the same subnet as the cluster nodes.
2. Insert the product disc with the SF Oracle RAC software into a drive that is connected to the system.
3. Identify the block device file for the disc drive:

   ```
   # ioscan -fnC disk
   ```

   Make a note of the device file as it applies to your system.
4. Create a directory in which to mount the software disc. Then, mount the disc using the appropriate drive name:

   ```
   # mkdir -p /dvd_mount
   # mount /dev/rdsk/c3t2d0 /dvd_mount
   ```

5. Verify that the disc is mounted:

   ```
   # mount
   ```

6. Navigate to the location of the depots:

   ```
   # cd /dvd_mount/storage_foundation_for_oracle_rac
   ```

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:

  ```
  # ioscan -fnC disk
  ```

- The shared storage must support SCSI-3 persistent reservations (PR). Run the vxfentsthdw(1M) utility to ensure that the shared storage is SCSI-3 compliant.

The `vxfentsthdw` utility is located in the directory `cluster_server/tools/vxfentsthdw`.

```
# ./vxfentsthdw
```

For more information on setting up shared storage, see the *Veritas Cluster Server Installation Guide*.

Setting the environment variables

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

```
# MANPATH=/usr/share/man:/opt/VRTS/man
# export MANPATH
```

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.

Note: Do not define $ORACLE_HOME/lib in LIBPATH for root user. You should define $ORACLE_HOME/lib in LIBPATH for the oracle user.

Based on the shell you use, type one of the following:

For sh, ksh, or bash

```
# PATH=/usr/sbin:/sbin:/usr/bin:\
/usr/lib/vxvm/bin:/opt/VRTSvxfs/cfs/bin:\
/opt/VRTSvcs/bin:/opt/VRTS/bin:\
/opt/VRTSvcs/rac/bin:/opt/VRTSob/bin:\
$PATH; export PATH
```

Optimizing LLT media speed settings on private NICs

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

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

Guidelines for setting the media speed of the LLT interconnects

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

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

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

Verifying the systems before installation

Use any of the following options to verify your systems before installation:

- Option 1: Run the Veritas Operations Services (VOS) utility.
  For information on downloading and running VOS:
  http://go.symantec.com/vos
- Option 2: Run the installsfrac program with the "-precheck" option as follows:
  Navigate to the directory that contains the installsfrac program. The program is located in the product directory.
  Start the preinstallation check:

  ```
  # ./installsfrac -precheck galaxy nebula
  ```

  The program proceeds in a non-interactive mode, examining the systems for licenses, depots, 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.
- Option 3: Run the Veritas Web-based installation program as follows:

- Start the Web-based installer:

  ```
  # ./webinstaller start
  ```

  Paste the link in the address bar of the Web browser to access the installer.

- On the Select a task and a product page, select **Perform a Pre-installation check** from the **Task** drop-down list.
  Select the product from the **Product** drop-down list, and click **Next**.
  The installer performs the precheck and displays the results.

Chapter 6

Installing SF Oracle RAC

This chapter includes the following topics:

- About installing SF Oracle RAC
- About installation and configuration methods
- Installing SF Oracle RAC using the Veritas script-based installation program
- Installing SF Oracle RAC using the Veritas Web-based installation program

About installing SF Oracle RAC

You can install SF Oracle RAC on clusters of up to 16 nodes.

The installation requires passwordless communication between systems for installing SF Oracle RAC. The installer prompts you to configure passwordless communication at the time of installation, if it is not already set up.

The product installer has improved ability to recover from failed installations. A recovery file is created if an installation fails due to a failed network connection. This file enables the install program to resume from the point where the installation failed.

By default, the installer generates a response file that you can reuse or customize for silent installations on other systems. If you need to suspend the installation, make sure that you select the option **Exit the installer** to create the response file before exiting the installation.

Note: If you enter **q** to quit the installation, the installer does not create a response file.

About installation and configuration methods

You can use one of the following methods to install and configure SF Oracle RAC.

Table 6-1 Installation and configuration methods

Method	Description
Interactive installation and configuration using the script-based installer **Note:** If you obtained SF Oracle RAC from an electronic download site, you must use the `installsfrac program` script instead of the `installer` script.	You can use one of the following script-based installers: ■ Common product installer script: `installer` The common product installer script provides a menu that simplifies the selection of installation and configuration options. Use this method to install other products, such as the Symantec Product Authentication Service (AT), along with SF Oracle RAC. ■ Product-specific installation script: `installsfrac program` ■ The product-specific installation script provides command-line interface options. Installing and configuring with the `installsfrac program` script is identical to specifying SF Oracle RAC from the `installer` script. Use this method to install or configure only SF Oracle RAC.
Silent installation using the response file	The response file automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. You can use the script-based installers with the response file to install silently on one or more systems. See "About response files" on page 371.

Table 6-1 Installation and configuration methods *(continued)*

Method	Description
Web-based installer	The Web-based installer provides an interface to manage the installation and configuration from a remote site using a standard Web browser. `./webinstaller` See "Installing SF Oracle RAC using the Veritas Web-based installation program" on page 92.

Installing SF Oracle RAC using the Veritas script-based installation program

Before you start the installation, make sure that you have the installation and configuration worksheet with the values on hand for the installation.

During the installation, the installer performs the following tasks:

- Verifies system readiness for installation by checking system communication, network speed, installed depots, operating system patches, 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 SF Oracle RAC installation.

- Installs the SF Oracle RAC 5.1 SP1 depots.

If you encounter issues during the installation, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*, Chapter "Performance and troubleshooting" for information on resolving the issue.

The following sample procedure installs SF Oracle RAC on two systems—galaxy and nebula.

To install SF Oracle RAC

1 Review the installer note on VxVM and confirm if you want to proceed with the installation.

The installer replaces any previous VxVM version with VxVM 5.1 Service Pack 1.

2 Log in as the superuser on one of the systems.

3 Start the installation program:

SF Oracle RAC installer	Navigate to the directory that contains the installation program. The program is located in the product directory. Run the program: `# ./installsfrac galaxy nebula`
Common product installer	Navigate to the directory that contains the installation program. Run the program: `# ./installer galaxy nebula` From the opening Selection Menu, choose: "**I**" for "Install a Product." From the displayed list of products to install, choose **Veritas Storage Foundation for Oracle RAC**.

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

4 Set up the systems so that commands between systems execute without prompting for passwords or confirmations.

5 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 configure of SF Oracle RAC
on galaxy.
Do you want to resume this process? [y,n,q,?] (y) n
```

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

7 Select the type of installation—Minimal, Recommended, All. Symantec recommends you to choose option **3 Install all Veritas Storage Foundation for Oracle RAC depots**.

```
1)  Install minimal required Veritas Storage Foundation for
    Oracle RAC depots
2)  Install recommended Veritas Storage Foundation for
```

```
    Oracle RAC depots
3)  Install all Veritas Storage Foundation for
    Oracle RAC depots
4)  Display depots to be installed for each option
Select the depots to be installed on all systems? [1-4,q,?] (2) 3
```

The installer verifies the systems for compatibility and displays the list of depots and patches that will be installed.

The installer installs the SF Oracle RAC depots and patches.

8 Select the appropriate license option.

```
1) Enter a valid license key
2) Enable keyless licensing
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 Oracle RAC 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 Oracle RAC without entering a key. However, you must still acquire a valid license to install and use SF Oracle RAC. Keyless licensing requires that you manage the systems with a Management Server.

  Enter **y** if you want to configure Veritas Volume Replicator (VVR) and Global Cluster Option (GCO) during the installation. VVR is configured with default values while GCO is configured with the settings you specify. You can reconfigure VVR and GCO manually at any time.

  ```
  Would you like to enable the Veritas Volume Replicator? [y,n,q] y

  Would you like to enable the Global Cluster Option? [y,n,q] y
  ```

  The installer registers the 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 Restart the nodes after installation. Some of the depots require a restart operation before you can proceed to configure SF Oracle RAC.

Note: Do not use the reboot command to restart the nodes.

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

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
```

Installing SF Oracle RAC using the Veritas Web-based installation program

Before you start the installation, make sure that you have the installation and configuration worksheet with the values on hand for the installation.

The installation of SF Oracle RAC using the Web-based installation program involves the following tasks:

- Review the system configuration requirements for a Web-based installation.
  See "Before using the Veritas Web-based installer" on page 93.
- Start the Veritas Web installer.
  See "Starting the Veritas Web-based installer" on page 93.
- Install SF Oracle RAC.
  See "Installing products with the Veritas Web-based installer" on page 94.

During the installation, the installer performs the following tasks:

- Verifies system readiness for installation by checking system communication, network speed, installed depots, operating system patches, 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 SF Oracle RAC installation.

- Installs the SF Oracle RAC 5.1 SP1 depots.

If you encounter issues during the installation, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*, Chapter "Performance and troubleshooting" for information on resolving the issue.

Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

Table 6-2 Web-based installer requirements

System	Function	Requirements
Target system	The systems where you plan to install the Veritas products.	Must be a supported platform for SF Oracle RAC 5.1 SP1.
Installation server	The server where you start the installation. The installation media is accessible from the installation server.	Must use the same operating system as the target systems and must be at one of the supported operating system update levels.
Administrative system	The system where you run the Web browser to perform the installation.	Must have a Web browser. Supported browsers: ■ Internet Explorer 6, 7, and 8 ■ Firefox 3.x

Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

To start the Web-based installer

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

   ```
   # ./webinstaller start
   ```

   The webinstaller script displays a URL. Note this URL.

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

2. On the administrative server, start the Web browser.
3. Navigate to the URL that the script displayed.
4. The browser may display the following message:

   ```
   Secure Connection Failed
   ```

   Obtain a security exception for your browser.
5. When prompted, enter `root` and root's password of the installation server.

Installing products with the Veritas Web-based installer

This section describes installing SF Oracle RAC with the Veritas Web-based installer.

To install SF Oracle RAC

1. Perform preliminary steps.
2. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 93.
3. Select **Veritas Storage Foundation for Oracle RAC** from the Product drop-down list, and click Next.
4. On the License agreement page, select whether you accept the terms of the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.
5. Choose minimal, recommended, or all packages. Click **Next**.
6. Indicate the systems on which to install. Enter one or more system names, separated by spaces. Click **Validate**.
7. After the validation completes successfully, click **Next** to install SF Oracle RAC on the selected system.
8. After the installation completes, you must choose your licensing method.

On the license page, select one of the following tabs:

- Keyless licensing

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

  For more information, go to the following website:

  http://go.symantec.com/sfhakeyless

  Complete the following information:
  Choose whether you want to enable Global Cluster option.
  Click Register.

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

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

If you select No, you can exit the installer. You must configure the product before you can use SF Oracle RAC.

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

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

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

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

Chapter 7

Preparing to configure SF Oracle RAC

This chapter includes the following topics:

- Preparing to configure the clusters in secure mode
- Setting up the CP server

Preparing to configure the clusters in secure mode

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

In a cluster that is online, if you want to enable or disable AT using the `installsfrac -security` command, see the *Veritas Cluster Server Administrator's Guide* for instructions.

The prerequisites to configure a cluster in secure mode are as follows:

- A system in your enterprise that serves as root broker (RB).

  You can either use an external system as root broker, or use one of the cluster nodes as root broker.

  - To use an external root broker, identify an existing root broker system in your enterprise or install and configure root broker on a stable system.
    See "Installing the root broker for the security infrastructure" on page 101.
  - To use one of the cluster nodes as root broker, the installer does not require you to do any preparatory tasks.
    When you configure the cluster in secure mode using the script-based installer, choose the automatic mode and choose one of the nodes for the installer to configure as root broker.

Symantec recommends that you configure a single root broker system for your entire enterprise. If you use different root broker systems, then you must establish trust between the root brokers.
For example, if the management server and the cluster use different root brokers, then you must establish trust.

- For external root broker, an authentication broker (AB) account for each node in the cluster is set up on the root broker system.
  See "Creating authentication broker accounts on root broker system" on page 102.
- The system clocks of the external root broker and authentication brokers must be in sync.

The script-based installer provides the following configuration modes:

Automatic mode	The external root broker system must allow remsh or ssh passwordless login to use this mode.
Semi-automatic mode	This mode requires encrypted files (BLOB files) from the AT administrator to configure a cluster in secure mode. The nodes in the cluster must allow remsh or ssh passwordless login. See "Setting up inter-system communication" on page 636.
Manual mode	This mode requires root_hash file and the root broker information from the AT administrator to configure a cluster in secure mode. The nodes in the cluster must allow remsh or ssh passwordless login. See "Setting up inter-system communication" on page 636.

Figure 7-1 depicts the flow of configuring SF Oracle RAC cluster in secure mode.

Figure 7-1 Workflow to configure SF Oracle RAC cluster in secure mode

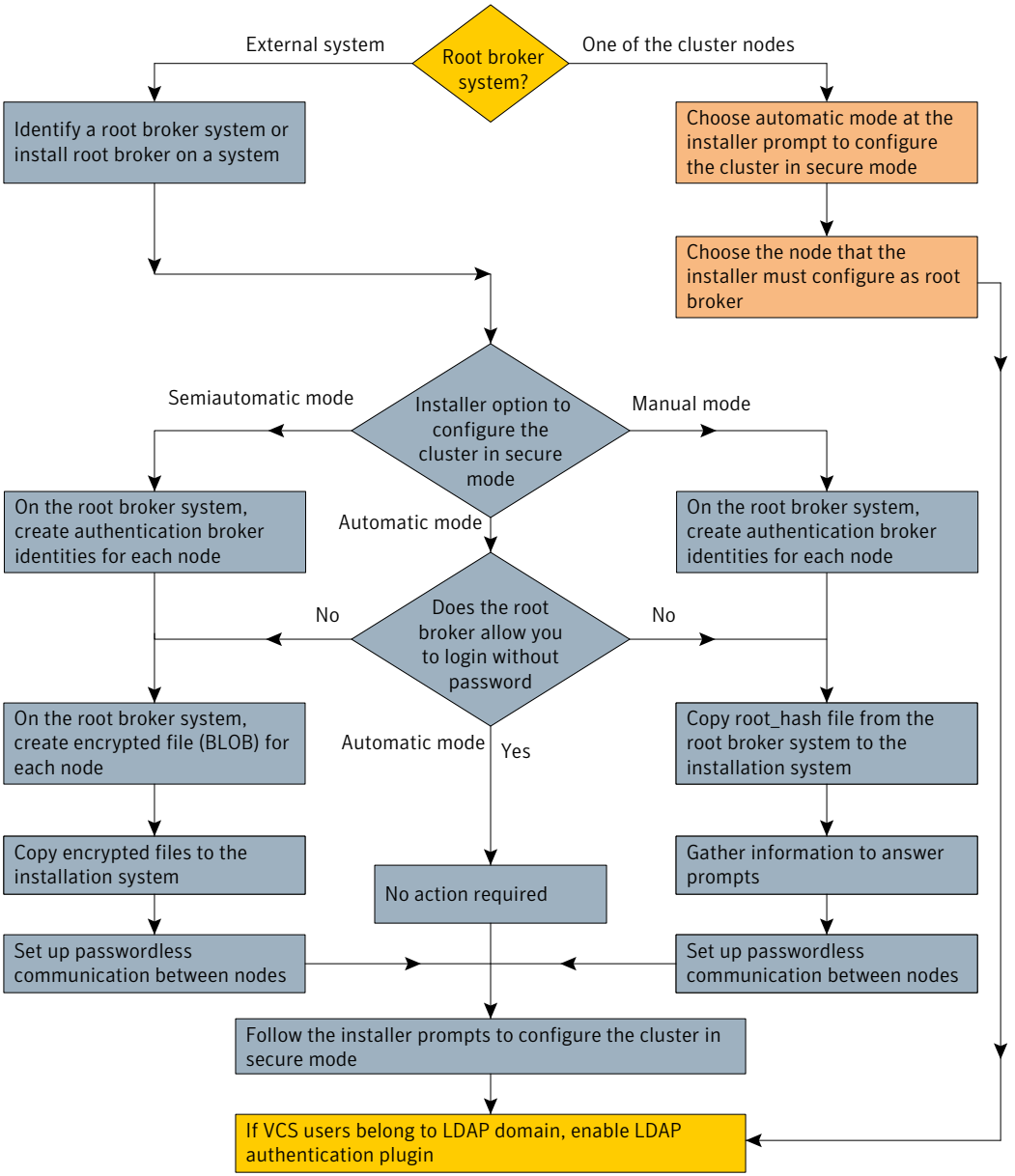


Table 7-1 lists the preparatory tasks in the order which the AT and VCS administrators must perform. These preparatory tasks apply only when you use an external root broker system for the cluster.

Table 7-1 Preparatory tasks to configure a cluster in secure mode (with an external root broker)

Tasks	Who performs this task
Decide one of the following configuration modes to set up a cluster in secure mode: ■ Automatic mode ■ Semi-automatic mode ■ Manual mode	VCS administrator
Install the root broker on a stable system in the enterprise. See "Installing the root broker for the security infrastructure" on page 101.	AT administrator
To use the semi-automatic mode or the manual mode, on the root broker system, create authentication broker accounts for each node in the cluster. See "Creating authentication broker accounts on root broker system" on page 102. The AT administrator requires the following information from the VCS administrator: ■ Node names that are designated to serve as authentication brokers ■ Password for each authentication broker	AT administrator
To use the semi-automatic mode, create the encrypted files (BLOB files) for each node and provide the files to the VCS administrator. See "Creating encrypted files for the security infrastructure" on page 103. The AT administrator requires the following additional information from the VCS administrator: ■ Administrator password for each authentication broker Typically, the password is the same for all nodes.	AT administrator
To use the manual mode, provide the root_hash file (/opt/VRTSat/bin/root_hash) from the root broker system to the VCS administrator.	AT administrator

Table 7-1 Preparatory tasks to configure a cluster in secure mode (with an external root broker) *(continued)*

Tasks	Who performs this task
Copy the files that are required to configure a cluster in secure mode to the system from where you plan to install and configure SF Oracle RAC. See "Preparing the installation system for the security infrastructure" on page 105.	VCS administrator

Installing the root broker for the security infrastructure

Install the root broker only if you plan to use AT to configure the cluster in secure mode. You can use a system outside the cluster or one of the systems within the cluster as root broker. If you plan to use an external broker, the root broker administrator must install and configure the root broker before you configure the Authentication Service for SF Oracle RAC. Symantec recommends that you install the root broker on a stable system that is outside the cluster.

You can also identify an existing root broker system in the data center to configure the cluster in secure mode. The root broker system can run AIX, HP-UX, Linux, or Solaris operating system.

See Symantec Product Authentication Service documentation for more information.

See "About Symantec Product Authentication Service (AT)" on page 36.

To install the root broker

1. Mount the product disc and start the installer.

```
# ./installer
```

2. From the Task Menu, choose I for "Install a Product."
3. From the displayed list of products to install, choose: Symantec Product Authentication Service (AT).
4. Enter **y** to agree to the End User License Agreement (EULA).
5. Enter 2 to install the recommended packages.
6. Enter the name of the system where you want to install the Root Broker.

```
Enter the operating_system system names separated by space [q,?]: venus
```

7 Review the output as the installer does the following:

- Checks to make sure that AT supports the operating system
- Checks if the depots are already on the system.

The installer lists the depots that the program is about to install on the system. Press Enter to continue.

8 Review the output as the installer installs the root broker on the system.

9 After the installation, configure the root broker.

10 Select a mode to configure the root broker from the three choices that the installer presents:

```
1)Root+AB Mode
2)Root Mode
3)AB Mode

Enter the mode in which you would like AT to be configured? [1-3,q] 2

All AT processes that are currently running must be stopped

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

11 Press Enter to continue and review the output as the installer starts the Authentication Service.

Creating authentication broker accounts on root broker system

On the root broker system, the administrator must create an authentication broker (AB) account for each node in the cluster.

To create authentication broker accounts on root broker system

1 Determine the root broker domain name. Enter the following command on the root broker system:

```
venus> # vssat showalltrustedcreds
```

For example, the domain name resembles "Domain Name: root@venus.symantecexample.com" in the output.

2 For each node in the cluster, verify whether an account exists on the root broker system.

For example, to verify that an account exists for node galaxy:

```
venus> # vssat showprpl --pdrtype root \
--domain root@venus.symantecexample.com --prplname galaxy
```

- If the output displays the principal account on root broker for the authentication broker on the node, then delete the existing principal accounts. For example:

  ```
  venus> # vssat deleteprpl --pdrtype root \
  --domain root@venus.symantecexample.com \
  --prplname galaxy --silent
  ```

- If the output displays the following error, then the account for the given authentication broker is not created on this root broker:

  ```
  "Failed To Get Attributes For Principal"
  ```

  Proceed to step 3.

3 Create a principal account for each authentication broker in the cluster. For example:

```
venus> # vssat addprpl --pdrtype root --domain \
root@venus.symantecexample.com --prplname galaxy \
--password password --prpltype service
```

You must use this password that you create in the input file for the encrypted file.

Creating encrypted files for the security infrastructure

Create encrypted files (BLOB files) only if you plan to choose the semiautomatic mode that uses an encrypted file to configure the Authentication Service. The administrator must create the encrypted files on the root broker node. The administrator must create encrypted files for each node that is going to be a part of the cluster before you configure the Authentication Service for SF Oracle RAC.

To create encrypted files

1 Make a note of the following root broker information. This information is required for the input file for the encrypted file:

hash	The value of the root hash string, which consists of 40 characters. Execute the following command to find this value: `venus> # vssat showbrokerhash`

root_domain — The value for the domain name of the root broker system. Execute the following command to find this value:

```
venus> # vssat showalltrustedcreds
```

2 Make a note of the following authentication broker information for each node. This information is required for the input file for the encrypted file:

identity — The value for the authentication broker identity, which you provided to create authentication broker principal on the root broker system.

This is the value for the **--prplname** option of the `addprpl` command.

See "Creating authentication broker accounts on root broker system" on page 102.

password — The value for the authentication broker password, which you provided to create authentication broker principal on the root broker system.

This is the value for the **--password** option of the `addprpl` command.

See "Creating authentication broker accounts on root broker system" on page 102.

3 For each node in the cluster, create the input file for the encrypted file.

The installer presents the format of the input file for the encrypted file when you proceed to configure the Authentication Service using encrypted file. For example, the input file for authentication broker on galaxy resembles:

```
[setuptrust]
broker=venus.symantecexample.com
hash=758a33dbd6fae751630058ace3dedb54e562fe98
securitylevel=high

[configab]
identity=galaxy
password=password
root_domain=root@venus.symantecexample.com
root_broker=venus.symantecexample.com:2821
```

```
start_broker=false
enable_pbx=false
```

4 Back up these input files that you created for the authentication broker on each node in the cluster.

Note that for security purposes, the command to create the output file for the encrypted file deletes the input file.

5 For each node in the cluster, create the output file for the encrypted file from the root broker system using the following command:

```
RootBroker> # vssat createpkg \
--in /path/to/blob/input/file.txt \
--out /path/to/encrypted/blob/file.txt \
--host_ctx AB-hostname
```

For example:

```
venus> # vssat createpkg --in /tmp/galaxy.blob.in \
--out /tmp/galaxy.blob.out --host_ctx galaxy
```

Note that this command creates an encrypted file even if you provide wrong password for "password=" entry. But such an encrypted file with wrong password fails to install on authentication broker node.

6 After you complete creating the output files for the encrypted file, you must copy these encrypted BLOB files for each node in the cluster.

Preparing the installation system for the security infrastructure

The VCS administrator must gather the required information and prepare the installation system to configure a cluster in secure mode.

To prepare the installation system for the security infrastructure

- Depending on the configuration mode you decided to use, do one of the following:

Automatic mode	Do the following: ■ Gather the root broker system name from the AT administrator. ■ During SF Oracle RAC configuration, choose the configuration option 1 when the installsfrac program prompts.

Semi-automatic mode	Do the following: ■ Copy the encrypted files (BLOB files) to the system from where you plan to install VCS. Note the path of these files that you copied to the installation system. ■ During SF Oracle RAC configuration, choose the configuration option 2 when the installsfrac program prompts.
Manual mode	Do the following: ■ Copy the root_hash file that you fetched to the system from where you plan to install VCS. Note the path of the root hash file that you copied to the installation system. ■ Gather the root broker information such as name, fully qualified domain name, domain, and port from the AT administrator. ■ Note the principal name and password information for each authentication broker that you provided to the AT administrator to create the authentication broker accounts. ■ During SF Oracle RAC configuration, choose the configuration option 3 when the installsfrac program prompts.

Setting up the CP server

Table 7-2 lists the tasks to set up the CP server for server-based I/O fencing.

Table 7-2 Tasks to set up CP server for server-based I/O fencing

Task	Reference
Plan your CP server setup	See "Planning your CP server setup" on page 107.
Install the CP server	See "Installing the CP server using the installer" on page 108.
Configure the CP server cluster in secure mode	See "Configuring the CP server cluster in secure mode" on page 109.
Set up shared storage for the CP server database	See "Setting up shared storage for the CP server database" on page 110.

Table 7-2 Tasks to set up CP server for server-based I/O fencing *(continued)*

Task	Reference
Configure the CP server	See " Configuring the CP server using the configuration utility" on page 111. See "Configuring the CP server manually" on page 119.
Verify the CP server configuration	See "Verifying the CP server configuration" on page 121.

Planning your CP server setup

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

To plan your CP server setup

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

   Symantec recommends hosting the CP server on an SFHA cluster.

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

   - You must configure fencing in enabled mode during the SFHA configuration.
   - You must set up shared storage for the CP server database during your CP server setup.
   - Decide whether you want to configure server-based fencing for the SF Oracle RAC cluster (application cluster) with a single CP server as coordination point or with at least three coordination points.

     Symantec recommends using at least three coordination points.

3. Decide whether you want to configure the CP server cluster in secure mode using the Symantec Product Authentication Service (AT).

   Symantec recommends configuring the CP server cluster in secure mode. Setting up AT secures the communication between the CP server and its clients (SF Oracle RAC clusters). It also secures the HAD communication on the CP server cluster, and makes the authentication broker highly available.

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

   See "CP server requirements" on page 48.

5 Have the following information handy for CP server configuration:

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

---

Note: If a CP server is configured to use an IPv6 network address for the virtual IP, then the operating system of the cluster nodes where SF Oracle RAC is hosted should also support the IPv6 network stack along with the IPv4 network stack. Note that even if SF Oracle RAC supports IPv6, it cannot be configured to use IPv6 network addresses for its agents, because Oracle RAC does not support IPv6.

Installing the CP server using the installer

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

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

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

CP server setup uses a single system

Install and configure VCS to create a single-node VCS cluster.

Meet the following requirements for CP server:

- During installation, make sure to select all depots for installation. The VRTScps depot is installed only if you select to install all depots.
- During configuration, make sure to configure LLT and GAB.
- During configuration, set up the cluster in secure mode if you want secure communication between the CP server and the SF Oracle RAC cluster (application cluster).

See the *Veritas Cluster Server Installation Guide* for instructions on installing and configuring VCS.

Proceed to configure the CP server.

See " Configuring the CP server using the configuration utility" on page 111.

See "Configuring the CP server manually" on page 119.

CP server setup uses multiple systems

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

Meet the following requirements for CP server:

- During installation, make sure to select all depots for installation. The VRTScps depot is installed only if you select to install all depots.
- During configuration, set up the cluster in secure mode if you want secure communication between the CP server and the SF Oracle RAC cluster (application cluster).
  See "Preparing to configure the clusters in secure mode" on page 97.
- During configuration, configure disk-based fencing (scsi3 mode).

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

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

Configuring the CP server cluster in secure mode

You must configure security on the CP server only if you want to secure the communication between the CP server and the SF Oracle RAC cluster (CP client).

This step secures the HAD communication on the CP server cluster, and makes the authentication broker highly available.

Note: If you already configured Symantec Product Authentication Service (AT) during VCS configuration, you can skip this section.

To configure the CP server cluster in secure mode

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

  ```
  # installsfrac -security
  ```

  See "Preparing to configure the clusters in secure mode" on page 97.

Setting up shared storage for the CP server database

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

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

To set up shared storage for the CP server database

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

   For example:

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

2. Import the disk group if it's not already imported.

   For example:

   ```
   # vxdg import cps_dg
   ```

3 Create a mirrored volume over the disk group.

For example:

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

4 Create a file system over the volume.

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

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

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

Configuring the CP server using the configuration utility

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

Perform one of the following procedures:

For CP servers on single-node VCS cluster:	See "To configure the CP server on a single-node VCS cluster" on page 111.
For CP servers on an SFHA cluster:	See "To configure the CP server on an SFHA cluster" on page 115.

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

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

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

```
# /opt/VRTScps/bin/configure_cps.pl
```

3 Enter **1** at the prompt to configure CP server on a single-node VCS cluster.

The configuration utility then runs the following preconfiguration checks:

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

4 Enter the name of the CP server.

```
Enter the name of the CP Server: mycps1.symantecexample.com
```

5 Enter a valid virtual IP address on which the CP server process should depend on.

```
Enter a valid Virtual IP address on which
the CP Server process should depend on:
10.209.83.85
```

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

```
Enter a port number in range [49152, 65535], or
press <enter> for default port (14250):
```

7 Choose whether the communication between the CP server and the SF Oracle RAC clusters has to be made secure.

If you have not configured the CP server cluster in secure mode, enter **n** at the prompt.

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

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

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

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

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

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

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

9 Verify and confirm the CP server configuration information.

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

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

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

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

Configuring CP Server Service Group (CPSSG) for this cluster
-----------------------------------------------

NOTE: Please ensure that the supplied network interface is a
public NIC
```

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

```
Enter a valid network interface for virtual IP 10.209.83.85
on mycps1.symantecexample.com: lan0
```

12 Enter networkhosts information for the NIC resource.

```
Symantec recommends configuring NetworkHosts attribute to ensure
NIC resource to be online always.
Do you want to add NetworkHosts attribute for the NIC resource lan0 on
system mycps1? [y/n] : y
Enter a valid IP address to configure NetworkHosts for NIC lan0 on
system mycps1 : 10.209.83.86
Do you want to add another Network Host ?[y/n] : n
```

13 Enter the netmask for the virtual IP address. For example:

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

14 After the configuration process has completed, a success message appears. For example:

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

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

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

For example:

```
# hagrp -state CPSSG

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

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

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

For information about the CPSSG, refer to the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

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

See "Sample configuration files for CP server" on page 628.

To configure the CP server on an SFHA cluster

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

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

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

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

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

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

The configuration utility then runs the following preconfiguration checks:

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

5 Enter the name of the CP server.

```
Enter the name of the CP Server: mycps1.symantecexample.com
```

6 Enter a valid virtual IP address on which the CP server process should depend on.

```
Enter a valid Virtual IP address on which
the CP Server process should depend on:
10.209.83.85
```

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

```
Enter a port number in range [49152, 65535], or
press <enter> for default port (14250):
```

8 Choose whether the communication between the CP server and the SF Oracle RAC clusters has to be made secure.

If you have not configured the CP server cluster in secure mode, enter **n** at the prompt.

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

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

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

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

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

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

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

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

10 Verify and confirm the CP server configuration information.

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

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

11 The configuration utility proceeds with the configuration process, and creates a vxcps.conf configuration file on each node.

The following output is for one node:

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

Configuring CP Server Service Group (CPSSG) for this cluster
-----------------------------------------------
```

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

```
Is the name of NIC for virtual IP 10.209.83.85 same on all the systems?
[y/n] : y

NOTE: Please ensure that the supplied network interface is a
public NIC
```

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

```
Enter a valid interface for virtual IP 10.209.83.85
on all the systems : lan0
```

14 Enter networkhosts information for the NIC resource.

```
Symantec recommends configuring NetworkHosts attribute to ensure
NIC resource to be online always.
Do you want to add NetworkHosts attribute for the NIC resource lan0 on
system mycps1? [y/n] : y
Enter a valid IP address to configure NetworkHosts for NIC lan0 on
system mycps1 : 10.209.83.86
Do you want to add another Network Host ?[y/n] : n
```

15 Enter the netmask for the virtual IP address.

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

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

```
Enter the name of diskgroup for cps database :
cps_dg
```

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

```
Enter the name of volume created on diskgroup cps_dg :
cps_volume
```

18 After the configuration process has completed, a success message appears. For example:

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

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

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

For example:

```
# hagrp -state CPSSG

#Group   Attribute   System                      Value
CPSSG     State      mycps1.symantecexample.com   |ONLINE|
CPSSG     State      mycps2.symantecexample.com   |OFFLINE|
```

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

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

For information about the CPSSG, refer to the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

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

See "Sample configuration files for CP server" on page 628.

Configuring the CP server manually

Perform the following steps to manually configure the CP server.

To manually configure the CP server

1 Stop VCS on each node in the CP server cluster using the following command:

```
# hastop -local
```

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

See "Sample configuration files for CP server" on page 628.

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

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

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

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

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

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

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

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

5 Start VCS on all the cluster nodes.

```
# hastart
```

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

```
# hagrp -state CPSSG
```

Output similar to the following appears:

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

Verifying the CP server configuration

Perform the following steps to verify the CP server configuration.

To verify the CP server configuration

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

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

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

Chapter 8

Configuring SF Oracle RAC

This chapter includes the following topics:

- About configuring SF Oracle RAC
- Configuring the SF Oracle RAC components using the script-based installer
- Configuring SF Oracle RAC using the Web-based installer

About configuring SF Oracle RAC

You need to configure SF Oracle RAC when:

- You have completed installation of SF Oracle RAC on your systems.
- You want to reconfigure an existing SF Oracle RAC 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.

The configuration program provides you with menu options from which you can choose the configuration task.

During the configuration process, the installer performs the following tasks:

- Verifies the cluster information.
- Stops SF Oracle RAC processes.
- Starts SF Oracle RAC 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 Oracle RAC components using the script-based installer

Make sure that you have performed the necessary pre-configuration tasks if you want to configure the cluster in secure mode.

Start the `installsfrac` or `installer` program if you quit the installer after installation.

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 Oracle RAC, 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.

If you encounter issues during the configuration, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*, Chapter "Performance and troubleshooting" for information on resolving the issue.

To configure the SF Oracle RAC components

1. Log in as the superuser on any of the nodes in the cluster.
2. Start the configuration program.

SF Oracle RAC installer	Run the program:
	`# cd /opt/VRTS/install`
	`# ./installsfrac -configure galaxy nebula`

Common product installer	Run the program: `# ./installer -configure galaxy nebula` Choose **Veritas Storage Foundation for Oracle RAC** to configure SF Oracle RAC.

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

3 Enter **1** to select the option **Configure SF Oracle RAC sub-components**.

```
1)  Configure SF Oracle RAC sub-components
2)  SF Oracle RAC Installation and Configuration Checks
3)  Prepare to Install Oracle
4)  Install Oracle Clusterware/Grid Infrastructure and Database
5)  Post Oracle Installation Tasks
6)  Exit SF Oracle RAC Configuration
Choose option: [1-6,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 Oracle RAC on galaxy.
Do you want to resume this process? [y,n,q,?] (y) n
```

5 Configure the Veritas Cluster Server component to set up the SF Oracle RAC cluster.

See "Configuring the SF Oracle RAC cluster" on page 125.

6 Add VCS users.

See "Adding VCS users" on page 134.

7 Configure SMTP email notification.

See "Configuring SMTP email notification" on page 134.

8 Configure SNMP trap notification.

See "Configuring SNMP trap notification" on page 136.

9 Configure global clusters, if you chose to enable GCO during the installation.

See "Configuring global clusters" on page 138.

10 Stop the SF Oracle RAC resources.

See "Stopping and starting SF Oracle RAC processes" on page 139.

Configuring the SF Oracle RAC cluster

You must configure the Veritas Cluster Server component to set up the SF Oracle RAC cluster. You can configure a basic cluster with only the required components, or an advanced cluster with any or all the optional features that meet your configuration requirements.

Refer to the *Veritas Cluster Server Installation Guide* for more information.

Configuring the cluster name and ID

Enter the cluster information when the installer prompts you.

To configure the cluster

1. Review the configuration instructions that the installer presents.
2. Enter the unique cluster name and cluster ID.

```
Enter the unique cluster name: [q,?] rac_cluster101
Enter a unique Cluster ID number between 0-65535: [b,q,?] 7
```

Configuring private heartbeat links

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

The following procedure helps you configure LLT over Ethernet.

To configure private heartbeat links

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

Skip to step 5.

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

The installer discovers and lists the network interface cards. You can use either the standard interfaces or the aggregated interfaces (bonded NICs).

You must not enter the network interface card that is used for the public network (typically lan0.)

```
Enter the NIC for the first private heartbeat link on galaxy:
[b,q,?] lan1
lan1 has an IP address configured on it. It could be a
public NIC on galaxy.
Are you sure you want to use lan1 for the first private
heartbeat link? [y,n,q,b,?] (n) y
Would you like to configure a second private heartbeat link?
[y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat link on galaxy:
[b,q,?] lan2
lan2 has an IP address configured on it. It could be a
public NIC on galaxy.
Are you sure you want to use lan2 for the second private
heartbeat link? [y,n,q,b,?] (n) y
Would you like to configure a third private heartbeat link?
[y,n,q,b,?](n)
Do you want to configure an additional low priority heartbeat
link? [y,n,q,b,?] (n)
```

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

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

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

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

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

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

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

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

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

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

6 Verify and confirm the information that the installer summarizes.

Configuring the virtual IP of the cluster

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

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

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

To configure the virtual IP of the cluster

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

2 To configure virtual IP, enter `y` at the prompt.

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

Do one of the following:

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

```
Active NIC devices discovered on galaxy: lan0
Enter the NIC for Virtual IP of the Cluster to use on galaxy:
[b,q,?](lan0)
```

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 lan0 to be the public NIC used by all systems
[y,n,q,b,?] (y)
```

5 Enter the virtual IP address for the cluster.

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

6 Confirm the default netmask or enter another one:

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

7 Enter the NetworkHosts IP addresses that are separated with spaces for checking the connections.

```
Enter the NetworkHosts IP addresses, separated by
spaces: [b,q,?] 192.168.1.17
```

8 Verify and confirm the Cluster Virtual IP information.

```
Cluster Virtual IP verification:

      NIC: lan0
      IP: 192.168.1.16
      Netmask: 255.255.240.0

      NetworkHosts: 192.168.1.17

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

Configuring the cluster in secure mode

If you want to configure the cluster in secure mode, make sure that you meet the prerequisites for secure cluster configuration.

The installer provides different configuration modes to configure a secure cluster. Make sure that you completed the pre-configuration tasks for the configuration mode that you want to choose.

See "Preparing to configure the clusters in secure mode" on page 97.

To configure the cluster in secure mode

1 Choose whether to configure SF Oracle RAC to use Symantec Product Authentication Service.

```
Would you like to configure VCS to use Symantec Security
Services? [y,n,q] (n) y
```

- If you want to configure the cluster in secure mode, make sure you meet the prerequisites and enter **y**.
- If you do not want to configure the cluster in secure mode, enter **n**.
  You must add VCS users when the configuration program prompts.
  See "Adding VCS users" on page 134.

2 Select one of the options to enable security.

Before you choose any of the options, make sure that all the nodes in the cluster can successfully ping the root broker system.

```
Select the Security option you would like to perform [1-3,b,q,?] (1)

Security Menu
     1)  Configure security completely automatically
     2)  Provide AB credentials using BLOBs
     3)  Provide AB credentials without using BLOBs
     b)  Back to previous menu
```

Review the following configuration modes. Based on the configuration that you want to use, enter one of the following values:

`Option 1.` Automatic configuration

Based on the root broker you want to use, do one of the following:

- To use an external root broker:
  Enter the name of the root broker system when prompted.
  Requires remote access to the root broker. Make sure that all the nodes in the cluster can successfully ping the root broker system.
  Review the output as the installer verifies communication with the root broker system, checks vxatd process and version, and checks security domain.
- To configure one of the nodes as root broker:
  - Press Enter at the following installer prompt:

    ```
    If you already have an external
    RB(Root Broker) installed and configured, enter
    the RB name, or press Enter to skip: [b]
    ```

  - Choose the node that the installer must configure as root and authentication broker. The installer configures the other nodes as authentication brokers.
    At the installer prompt, you can choose the first node in the cluster to configure as RAB, or you can enter n to configure another node as RAB. For example:

    ```
    Do you want to configure <galaxy> as RAB,
    and other nodes as AB? [y,n,q,b] (y) n
    Enter the node name which you want to
    configure as RAB: nebula
    ```

`Option 2.` Semiautomatic configuration

Enter the path of the encrypted file (BLOB file) for each node when prompted.

Option 3. Manual configuration

Enter the following Root Broker information as the installer prompts you:

```
Enter root broker name: [b]
east.symantecexample.com
Enter root broker FQDN:  [b]
(symantecexample.com)
symantecexample.com
Enter the root broker domain name for the
Authentication Broker's identity:  [b]
root@east.symantecexample.com
Enter root broker port:  [b] 2821
Enter path to the locally accessible root hash [b]
(/var/tmp/installvcs-200910221810ROA/root_hash)
/var/tmp/installvcs-200910221810ROA/root_hash
```

Enter the following Authentication Broker information as the installer prompts you for each node:

```
Enter Authentication broker's identity on
galaxy [b]
(galaxy.symantecexample.com)
galaxy.symantecexample.com
Enter the password for the Authentication broker's
identity on galaxy:
Enter Authentication broker's identity on
nebula [b]
(nebula.symantecexample.com)
nebula.symantecexample.com
Enter the password for the Authentication broker's
identity on nebula:
```

3 After you provide the required information to configure the cluster in secure mode, the program prompts you to configure SMTP email notification.

Note that the installer does not prompt you to add VCS users if you configured the cluster in secure mode. However, you must add VCS users later.

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

Adding VCS users

If you have enabled Symantec Product Authentication Service, you do not need to add VCS users now. Otherwise, on systems operating under an English locale, you can add VCS users at this time.

To add VCS users

1. Review the required information to add VCS users.
2. Reset the password for the Admin user, if necessary.

```
Do you want to set the username and/or password for the Admin user
(default username = 'admin', password='password')? [y,n,q] (n) y
Enter the user name: [b,q,?] (admin)
Enter the password:
Enter again:
```

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

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

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

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

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

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

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

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

Configuring SMTP email notification

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

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

To configure SMTP email notification

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

2 Specify whether you want to configure the SMTP notification.

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

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

See "Configuring SNMP trap notification" on page 136.

3 Provide information to configure SMTP notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on galaxy: lan0
Enter the NIC for the VCS Notifier to use on galaxy:
[b,q,?] (lan0)
Is lan0 to be the public NIC used by all systems?
[y,n,q,b,?] (y)
```

- Enter the SMTP server's host name.

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

- Enter the email address of each recipient.

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

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

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

4 Add more SMTP recipients, if necessary.

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

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

Enter the full email address of the SMTP recipient
```

```
(example: user@yourcompany.com): [b,q,?] harriet@example.com

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

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

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

5 Verify and confirm the SMTP notification information.

```
NIC: lan0

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

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

Configuring SNMP trap notification

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

Note that you can also configure the notification after installation.

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

To configure the SNMP trap notification

1 Review the required information to configure the SNMP notification feature of VCS.

2 Specify whether you want to configure the SNMP notification.

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

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

See "Configuring global clusters" on page 138.

3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on galaxy: lan0
Enter the NIC for the VCS Notifier to use on galaxy:
[b,q,?] (lan0)
Is lan0 to be the public NIC used by all systems?
[y,n,q,b,?] (y)
```

- Enter the SNMP trap daemon port.

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

- Enter the SNMP console system name.

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

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

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

4 Add more SNMP consoles, if necessary.

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

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

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

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

5 Verify and confirm the SNMP notification information.

```
NIC: lan0

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

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

Configuring global clusters

If you had installed a valid HA/DR license, the installer provides you an option to configure this cluster as global cluster. If not, the installer proceeds with other set of questions for CVM and CFS.

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

See the *Veritas Cluster Server Administrator's Guide* for instructions to set up SF Oracle RAC global clusters.

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

To configure the global cluster option

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

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

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

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

3 Provide information to configure this cluster as global cluster.

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

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

4 Verify and confirm the configuration of the global cluster.

```
Global Cluster Option configuration verification:

NIC: lan0
IP: 192.168.1.16
Netmask: 255.255.240.0

NetworkHosts: 192.168.1.15

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

Creation of SF Oracle RAC configuration files

The program consolidates all the information gathered in the preceding configuration tasks and creates configuration files.

If you chose to configure the cluster in secure mode, the installer also configures the Symantec Product Authentication Service. Depending on the mode you chose to set up Authentication Service, the installer creates security principal or executes the encrypted file to create security principal on each node in the cluster. The installer creates the VxSS service group, creates Authentication Server credentials on each node in the cluster, and Web credentials for VCS users, and sets up trust with the root broker. Then, the installer proceeds to start SF Oracle RAC in secure mode.

Review the output as the configuration program creates security principal, starts VCS, creates VCS configuration files, and copies the files to each node.

Stopping and starting SF Oracle RAC processes

The installer stops and starts SF Oracle RAC processes and configures the SF Oracle RAC agents.

Note: To use aggregated interfaces that the installer has not discovered for private heartbeats, do not opt to start SF Oracle RAC.

To stop SF Oracle RAC processes

1 Enter **y** to stop SF Oracle RAC processes.

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

2 Review the output as the installer stops and starts the SF Oracle RAC processes.

Note that SF Oracle RAC configuration program starts I/O fencing feature in disabled mode. SF Oracle RAC requires you to configure and enable I/O fencing feature.

Configuring SF Oracle RAC using the Web-based installer

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

Note: If you want to reconfigure SF Oracle RAC, 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.

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

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

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

To configure SF Oracle RAC on a cluster

1 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 93.

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

Task	Configure a Product
Product	Veritas Storage Foundation for Oracle RAC

Click **Next**.

3 On the Select Systems page, enter the system names where you want to configure SF Oracle RAC, and click **Validate**.

Example: **galaxy nebula**

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

Click **Next** after the installer completes the system verification successfully.

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

Cluster Name	Enter a unique cluster name.
Cluster ID	Enter a unique cluster ID.
LLT Type	Select an LLT type from the list. You can choose to configure LLT over UDP or over Ethernet. If you choose **Auto detect over Ethernet**, the installer auto-detects the LLT links over Ethernet. Verify the links and click **Yes** in the Confirmation dialog box. Skip to step 6. If you click No, you must manually enter the details to configure LLT over Ethernet.
Number of Heartbeats	Choose the number of heartbeat links you want to configure.
Low Priority Heartbeat NIC	Select the check box if you want to configure a low priority link. The installer configures one heartbeat link as low priority link.
Unique Heartbeat NICs per system	For LLT over Ethernet, select the check box if you do not want to use the same NIC details to configure private heartbeat links on other systems. For LLT over UDP, this check box is selected by default.

Click **Next**.

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

For **LLT over Ethernet**:	Do the following: ■ If you are using the same NICs on all the systems, select the NIC for each private heartbeat link. ■ If you had selected **Unique Heartbeat NICs per system** on the Set Cluster Name/ID page, provide the NIC details for each system.
For **LLT over UDP**:	Select the NIC, Port, and IP address for each private heartbeat link. You must provide these details for each system.

Click **Next**.

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

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

If you want to perform this task later, click **No**. You can use the `installsfrac -security` command. Go to step 8.

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

Do not configure security services	Choose this option if you do not want to enable security. The installer takes you to the next page to configure optional features of SF Oracle RAC.
Configure security automatically	Choose this option to use an external root broker. Enter the name of the root broker that is already configured for your enterprise environment, and click **Validate**. The installer configures the cluster in secure mode.
Configure one node as RAB and the others as AB	Select the system that you want to configure as RAB node. The installer configures the cluster in secure mode.

Click **Next**.

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

Virtual IP	■ Select the **Configure Virtual IP** check box. ■ If each system uses a separate NIC, select the **Configure NICs for every system separately** check box. ■ Select the interface on which you want to configure the virtual IP. ■ Enter a virtual IP address and value for the netmask. Enter the value for the networkhosts.
VCS Users	■ Reset the password for the Admin user, if necessary. ■ Click **Add** to add a new user. Specify the user name, password, and user privileges for this user.

SMTP

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

SNMP

- Select the **Configure SNMP** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- If all the systems use the same NIC, select the NIC for the VCS Notifier to be used on all systems. If not, select the NIC to be used by each system.
- In the **SNMP Port** box, enter the SNMP trap daemon port: (162).
- In the **Console System Name** box, enter the SNMP console system name.
- In the **Event** list box, select the minimum security level of messages to be sent to each console.
- Click **Add** to add more SNMP consoles, if necessary.

GCO

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

See the *Veritas Storage Foundation for Oracle RAC Installation and Configuration Guide* for instructions to set up SF Oracle RAC global clusters.

- Select the **Configure GCO** check box.
- If each system uses a separate NIC, select the **Configure NICs for every system separately** check box.
- Select a NIC.
- Enter a virtual IP address and value for the netmask.
  Enter the value for the networkhosts.

Click **Next**.

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

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

11 Click **Next** to complete the process of configuring SF Oracle RAC.

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

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

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

Chapter 9

Configuring SF Oracle RAC clusters for data integrity

This chapter includes the following topics:

- Setting up disk-based I/O fencing using installsfrac program
- Setting up disk-based I/O fencing manually
- Setting up server-based I/O fencing using installsfrac program
- Setting up server-based I/O fencing manually

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

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

Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

To initialize disks as VxVM disks

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

```
# ioscan -nfC disk
# insf -e
```

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

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

- Use the interactive vxdiskadm utility to initialize the disks as VxVM disks. For more information see the *Veritas Volume Manager Administrator's Guide*.
- Use the `vxdisksetup` command to initialize a disk as a VxVM disk.

  ```
  vxdisksetup -i device_name
  ```

  The example specifies the CDS format:

  ```
  # vxdisksetup -i c2t13d0
  ```

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

Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See "Initializing disks as VxVM disks" on page 147.

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 149.

Checking shared disks for I/O fencing

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

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

The vxfentsthdw utility has additional options suitable for testing many disks. Review the options for testing the disk groups (`-g`) and the disks that are listed in a file (`-f`). You can also test disks without destroying data using the `-r` option.

See the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

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

- Verifying the Array Support Library (ASL)
  See "Verifying Array Support Library (ASL)" on page 149.
- Verifying that nodes have access to the same disk
  See "Verifying that the nodes have access to the same disk" on page 150.
- Testing the shared disks for SCSI-3
  See "Testing the disks using vxfentsthdw utility" on page 151.

Verifying Array Support Library (ASL)

Make sure that the Array Support Library (ASL) for the array that you add is installed.

To verify Array Support Library (ASL)

1 If the Array Support Library (ASL) for the array that you add is not installed, obtain and install it on each node before proceeding.

The ASL for the supported storage device that you add is available from the disk array vendor or Symantec technical support.

2 Verify that the ASL for the disk array is installed on each of the nodes. Run the following command on each node and examine the output to verify the installation of ASL.

```
# vxddladm listsupport all
```

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

```
# vxdisk scandisks
```

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

Verifying that the nodes have access to the same disk

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

To verify that the nodes have access to the same disk

1 Verify the connection of the shared storage for data to two of the nodes on which you installed SF Oracle RAC.

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/vx/rdmp/c1t1d0 path on node A and the /dev/vx/rdmp/c2t1d0 path on node B.

From node A, enter:

```
vxfenadm -i /dev/vx/rdmp/c1t1d0

Vendor id : EMC
Product id : SYMMETRIX
```

```
Revision : 5567
Serial Number : 42031000a
```

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

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

```
# vxfenadm -i /dev/vx/rdmp/c3t1d0

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

Testing the disks using vxfentsthdw utility

This procedure uses the /dev/vx/rdmp/c1t1d0 disk in the steps.

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

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

```
The disk /dev/vx/rdmp/c1t1d0 is ready to be configured for I/O Fencing on
node galaxy
```

For more information on how to replace coordinator disks, refer to the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

To test the disks using vxfentsthdw utility

1 Make sure system-to-system communication functions properly.

See "Setting up inter-system communication" on page 636.

2 From one node, start the utility.

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

```
# vxfentsthdw [-n]
```

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

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

```
******** WARNING!!!!!!!! ********
THIS UTILITY WILL DESTROY THE DATA ON THE DISK!!

Do you still want to continue : [y/n] (default: n) y
Enter the first node of the cluster: galaxy
Enter the second node of the cluster: nebula
```

4 Enter the names of the disks that you want to check. Each node may know the same disk by a different name.

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

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

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

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

ALL tests on the disk /dev/vx/rdmp/c1t1d0 have PASSED
The disk is now ready to be configured for I/O Fencing on node
galaxy
```

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

Configuring disk-based I/O fencing using installsfrac program

Note: The installer stops and starts SF Oracle RAC 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 Oracle RAC.

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

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

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

The installsfrac program starts with a copyright message and verifies the cluster information.

Note the location of log files which you can access in the event of any problem with the configuration process.

2 Confirm that you want to proceed with the I/O fencing configuration at the prompt.

The program checks that the local node running the script can communicate with remote nodes and checks whether SF Oracle RAC 5.1 Service Pack 1 is configured properly.

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

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

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

- If the check fails, configure and enable VxVM before you repeat this procedure.
- If the check passes, then the program prompts you for the coordinator disk group information.

5 Choose whether to use an existing disk group or create a new disk group to configure as the coordinator disk group.

The program lists the available disk group names and provides an option to create a new disk group. Perform one of the following:

- To use an existing disk group, enter the number corresponding to the disk group at the prompt.
  The program verifies whether the disk group you chose has an odd number of disks and that the disk group has a minimum of three disks.
- To create a new disk group, perform the following steps:
  - Enter the number corresponding to the **Create a new disk group** option.
    The program lists the available disks that are in the CDS disk format in the cluster and asks you to choose an odd number of disks with at least three disks to be used as coordinator disks.

Symantec recommends that you use three disks as coordination points for disk-based I/O fencing.

- Enter the numbers corresponding to the disks that you want to use as coordinator disks.
- Enter the disk group name.

6 Verify that the coordinator disks you chose meet the I/O fencing requirements.

You must verify that the disks are SCSI-3 PR compatible using the vxfentsthdw utility and then return to this configuration program.

See "Checking shared disks for I/O fencing" on page 149.

7 After you confirm the requirements, the program creates the coordinator disk group with the information you provided.

The program also does the following:

- Populates the /etc/vxfendg file with this disk group information
- Populates the /etc/vxfenmode file on each cluster node with the I/O fencing mode information and with the SCSI-3 disk policy information

8 Verify and confirm the I/O fencing configuration information that the installer summarizes.

9 Review the output as the configuration program does the following:

- Stops VCS and I/O fencing on each node.
- Configures disk-based I/O fencing and starts the I/O fencing process.
- Updates the VCS configuration file main.cf if necessary.
- Copies the /etc/vxfenmode file to a date and time suffixed file /etc/vxfenmode-*date-time*. This backup file is useful if any future fencing configuration fails.
- Starts VCS on each node to make sure that the SF Oracle RAC is cleanly configured to use the I/O fencing feature.

10 Review the output as the configuration program displays the location of the log files, the summary files, and the response files.

11 Configure the Coordination Point agent to monitor the coordinator disks.

See "Configuring Coordination Point agent to monitor coordination points" on page 180.

Setting up disk-based I/O fencing manually

Table 9-1 lists the tasks that are involved in setting up I/O fencing.

Table 9-1 Tasks to set up I/O fencing manually

Task	Reference
Initializing disks as VxVM disks	See "Initializing disks as VxVM disks" on page 147.
Identifying disks to use as coordinator disks	See "Identifying disks to use as coordinator disks" on page 148.
Checking shared disks for I/O fencing	See "Checking shared disks for I/O fencing" on page 149.
Setting up coordinator disk groups	See "Setting up coordinator disk groups" on page 155.
Creating I/O fencing configuration files	See "Creating I/O fencing configuration files" on page 156.
Modifying SF Oracle RAC configuration to use I/O fencing	See "Modifying VCS configuration to use I/O fencing" on page 157.
Configuring Coordination Point agent to monitor coordination points	See "Configuring Coordination Point agent to monitor coordination points" on page 180.
Starting SF Oracle RAC on all nodes	See "Starting SF Oracle RAC on all nodes" on page 158.
Verifying I/O fencing configuration	See "Verifying I/O fencing configuration" on page 160.

Setting up coordinator disk groups

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

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

Refer to the *Veritas Volume Manager Administrator's Guide* for details on how to create disk groups.

The following example procedure assumes that the disks have the device names c1t1d0, c2t1d0, and c3t1d0.

To create the vxfencoorddg disk group

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

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

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

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

3. Deport the coordinator disk group:

```
# vxdg deport vxfencoorddg
```

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

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

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

```
# vxdg deport vxfencoorddg
```

Creating I/O fencing configuration files

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

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

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

1 On each nodes, type:

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

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

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

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

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

3 To check the updated /etc/vxfenmode configuration, enter the following command on one of the nodes. For example:

```
# more /etc/vxfenmode
```

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

/etc/rc.config.d/vxfenconf

Modifying VCS configuration to use I/O fencing

After you add coordination points and configure I/O fencing, add the UseFence = SCSI3 cluster attribute to the VCS configuration file /etc/VRTSvcs/conf/config/main.cf. If you reset this attribute to UseFence = None, VCS does not make use of I/O fencing abilities while failing over service groups. However, I/O fencing needs to be disabled separately.

To modify VCS configuration to enable I/O fencing

1 Save the existing configuration:

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

2 Stop VCS on all nodes:

```
# hastop -all
```

3 If the I/O fencing driver vxfen is already running, stop the I/O fencing driver.

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

4 Make a backup copy of the main.cf file:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.orig
```

5 On one node, use vi or another text editor to edit the main.cf file. To modify the list of cluster attributes, add the UseFence attribute and assign its value as SCSI3.

```
cluster rac_cluster101(
UserNames = { admin = "cDRpdxPmHpzS." }
Administrators = { admin }
HacliUserLevel = COMMANDROOT
CounterInterval = 5
UseFence = SCSI3
)
```

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

6 Save and close the file.

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

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

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

For example, on each remaining node, enter:

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

Starting SF Oracle RAC on all nodes

You must start SF Oracle RAC on each node to bring up the cluster configuration with I/O fencing enabled.

Starting I/O fencing, VCS, CVM, and CFS

You must start I/O fencing, VCS, CVM, and CFS on all nodes in the cluster.

To start VCS, CVM, and CFS on a node

1 Start the I/O fencing driver. Run the following command on each node:

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

The vxfen startup script also invokes the `vxfenconfig` command, which configures the vxfen driver to start and use the coordinator disks that are listed in /etc/vxfentab.

2 With the configuration file in place on each system, start VCS, CVM, and CFS:

```
# hastart
```

Verifying GAB port membership

After setting up I/O fencing and starting VCS, CVM, and CFS on each node, verify GAB port membership.

See "Verifying GAB" on page 197.

To verify GAB port membership

- Run the `gabconfig -a` command.

  For example:

```
galaxy# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen  ada401 membership 01
Port b gen  ada40d membership 01
Port d gen  ada409 membership 01
Port f gen  ada41c membership 01
Port h gen  ada40f membership 01
Port o gen  ada406 membership 01

Port u gen  ada41a membership 01

Port v gen  ada416 membership 01
Port w gen  ada418 membership 01
```

Verifying the CVM group is online

Make sure the cvm group is in the online state.

To verify CVM group

1 On any node, run the following command to verify that the cvm group is online:

```
# hagrp -state cvm
```

2 On any node, run the following command to make sure CVM has started properly:

```
# vxclustadm nidmap
```

Verifying I/O fencing configuration

Verify from the vxfenadm output that the SCSI-3 disk policy reflects the configuration in the /etc/vxfenmode file.

To verify I/O fencing configuration

1 On one of the nodes, type:

```
# vxfenadm -d
```

Output similar to the following appears if the SCSI3 disk policy is dmp:

```
I/O Fencing Cluster Information:
================================

Fencing Protocol Version: 201
Fencing Mode: SCSI3
Fencing SCSI3 Disk Policy: dmp
Cluster Members:

   * 0 (galaxy)
   1 (nebula)

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

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

```
# vxfenconfig -l
```

Setting up server-based I/O fencing using installsfrac program

If SF Oracle RAC cluster is configured to run in secure mode, then verify that the configuration is correct before you configure CP server-based I/O fencing.

See "Verifying the security configuration on the SF Oracle RAC cluster to use CP server coordination point" on page 161.

See "Configuring server-based I/O fencing using the installsfrac program" on page 163.

Verifying the security configuration on the SF Oracle RAC cluster to use CP server coordination point

After configuring security using the `installsfrac -security` command, follow the procedure below on each SF Oracle RAC cluster node to confirm that security is correctly configured.

To verify the security configuration on SF Oracle RAC cluster to use CP server coordination point

1 Run the following command:

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

The following is an example of the command output:

```
Domain(s) Found 1

**************************

Domain Name HA_SERVICES@galaxy.symantec.com

Expiry Interval 0

**************************
```

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

```
HA_SERVICES@hostname.domainname
```

or

```
HA_SERVICES@hostname
```

3 There should not be duplicate entries for HA_SERVICES domain.

The following is an example of an incorrect configuration:

```
showdomains

Domain(s) Found :       3

************************************

Domain Name:    HA_SERVICES@galaxy.symantec.com

Domain Type:    vx

************************************

Domain Name:    broker@galaxy.symantec.com

Domain Type:    vx

************************************

Domain Name:    HA_SERVICES@galaxy

Domain Type:    vx

************************************
```

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

Configuring server-based I/O fencing using the installsfrac program

You can configure server-based I/O fencing for the SF Oracle RAC cluster using the installsfrac program.

With server-based fencing, you can have the coordination points in your configuration as follows:

- Combination of CP servers and SCSI-3 compliant coordinator disks
- CP servers only
  Symantec also supports server-based fencing with a single highly available CP server that acts as a single coordination point.

See "About planning to configure I/O fencing" on page 62.

See "Recommended CP server configurations" on page 65.

This section covers the following example procedures:

Mix of CP servers and coordinator disks	See "To configure server-based fencing for the SF Oracle RAC cluster (one CP server and two coordinator disks)" on page 164.
Single CP server	See "To configure server-based fencing for the SF Oracle RAC cluster (single CP server)" on page 169.

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

1. Depending on the server-based configuration model in your setup, make sure of the following:
   - CP servers are configured and are reachable from the SF Oracle RAC cluster. The SF Oracle RAC cluster is also referred to as the application cluster or the client cluster.
     See "Setting up the CP server" on page 106.
   - The coordination disks are verified for SCSI3-PR compliance.
     See "Checking shared disks for I/O fencing" on page 149.
2. Start the installsfrac program with `-fencing` option.

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

   The installsfrac program starts with a copyright message and verifies the cluster information.

   Note the location of log files which you can access in the event of any problem with the configuration process.
3. Confirm that you want to proceed with the I/O fencing configuration at the prompt.

   The program checks that the local node running the script can communicate with remote nodes and checks whether SF Oracle RAC 5.1 Service Pack 1 is configured properly.
4. Review the I/O fencing configuration options that the program presents. Type **1** to configure server-based I/O fencing.

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

5 Make sure that the storage supports SCSI3-PR, and answer y at the following prompt.

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

6 Provide the following details about the coordination points at the installer prompt:

- Enter the total number of coordination points including both servers and disks. This number should be at least 3.

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

- Enter the total number of coordinator disks among the coordination points.

```
Enter the total number of disks among these:
[b] (0) 2
```

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

- Enter the virtual IP addresses or host names of the virtual IP address for each of the CP servers. The installer assumes these values to be identical as viewed from all the application cluster nodes.

```
Enter the Virtual IP address/fully qualified host name
for the Co-ordination Point Server #1:
[b] 10.209.80.197
```

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

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

8 Provide the following coordinator disks-related details at the installer prompt:

- Enter the I/O fencing disk policy for the coordinator disks.

```
Enter fencing mechanism for the disk(s) (raw/dmp):
[b,q,?] raw
```

- Choose the coordinator disks from the list of available disks that the installer displays. Ensure that the disk you choose is available from all the SF Oracle RAC (application cluster) nodes.

The number of times that the installer asks you to choose the disks depends on the information that you provided in step 6. For example, if you had chosen to configure two coordinator disks, the installer asks you to choose the first disk and then the second disk:

```
Select disk number 1 for co-ordination point

1) c1t1d0
2) c2t1d0
3) c3t1d0

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

- If you have not already checked the disks for SCSI-3 PR compliance in step 1, check the disks now.
  The installer displays a message that recommends you to verify the disks in another window and then return to this configuration procedure.
  Press Enter to continue, and confirm your disk selection at the installer prompt.
- Enter a disk group name for the coordinator disks or accept the default.

```
Enter the disk group name for coordinating disk(s):
[b] (vxfencoorddg)
```

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

For example:

```
Total number of coordination points being used: 3
CP Server (Port):
    1. 10.209.80.197 (14250)
SCSI-3 disks:
    1. c1t1d0
    2. c2t1d0
Disk Group name for the disks in customized fencing: vxfencoorddg
Disk mechanism used for customized fencing: raw
```

The installer initializes the disks and the disk group and deports the disk group on the SF Oracle RAC (application cluster) node.

10 If the CP server is configured for security, the installer sets up secure communication between the CP server and the SF Oracle RAC (application cluster):

- Make sure that the security configuration in the application cluster and the CP server is the same. If CP server is configured for security, ensure that the application cluster also runs in secure mode.
- If the CP server is configured for security, perform the following steps:
  - Review the output as the installer verifies if the SF Oracle RAC (application cluster) nodes have already established trust with an AT root broker.
  - If the SF Oracle RAC (application cluster) nodes and the CP server use different AT root brokers, enter y at the installer prompt and provide the following information:
    - Hostname for the authentication broker for any one of the CP servers
    - Port number where the authentication broker for the CP server is listening for establishing trust
    - Hostname for the authentication broker for any one of the SF Oracle RAC (application cluster) nodes
    - Port number where the authentication broker for the SF Oracle RAC (application cluster) is listening for establishing trust

    After the installer establishes trust between the authentication brokers of the CP servers and the application cluster nodes, press Enter to continue.

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

```
CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: rac_cluster101
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
```

12 Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the `/etc/vxfenmode` file with the appropriate details in each of the application cluster nodes.

```
Updating client cluster information on CP Server 10.210.80.199

Adding the client cluster to the CP Server 10.210.80.199 .................. Done

Registering client node galaxy with CP Server 10.210.80.199.............. Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ......... Done
Adding cluster rac_cluster101 to the CPClient user on CP Server 10.210.80.199 ... Done

Registering client node nebula with CP Server 10.210.80.199 ............. Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ......... Done
Adding cluster rac_cluster101 to the CPClient user on CP Server 10.210.80.199 ... Done

Updating /etc/vxfenmode file on galaxy ................................. Done
Updating /etc/vxfenmode file on nebula ......... ........................ Done
```

See "About I/O fencing configuration files" on page 608.

13 Configure the CP agent on the SF Oracle RAC (application cluster).

```
Do you want to configure CP Agent on the client cluster? [y,n,q]
(y)

Enter a non-existing name for the service group for CP Agent:
[b] (vxfen)

Adding CP Agent via galaxy ........................ Done
```

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

15 Note the location of the configuration log files, summary files, and response files that the installer displays for later use.

To configure server-based fencing for the SF Oracle RAC cluster (single CP server)

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

   See "Setting up the CP server" on page 106.

2. Start the installsfrac program with `-fencing` option.

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

   The installsfrac program starts with a copyright message and verifies the cluster information.

   Note the location of log files which you can access in the event of any problem with the configuration process.

3. Confirm that you want to proceed with the I/O fencing configuration at the prompt.

   The program checks that the local node running the script can communicate with remote nodes and checks whether SF Oracle RAC 5.1 Service Pack 1 is configured properly.

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

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

5. Make sure that the storage supports SCSI3-PR, and answer y at the following prompt.

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

6. Enter the total number of coordination points as **1**.

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

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

7. Provide the following CP server details at the installer prompt:

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

```
Enter the Virtual IP address/fully qualified host name
for the Co-ordination Point Server #1:
[b] 10.209.80.197
```

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

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

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

For example:

```
Total number of coordination points being used: 1
CP Server (Port):
    1. 10.209.80.197 (14250)
```

9 If the CP server is configured for security, the installer sets up secure communication between the CP server and the SF Oracle RAC (application cluster):

- Make sure that the security configuration in the application cluster and the CP server is the same. If CP server is configured for security, ensure that the application cluster also runs in secure mode.
- If the CP server is configured for security, perform the following steps:
  - Review the output as the installer verifies if the SF Oracle RAC (application cluster) nodes have already established trust with an AT root broker.
  - If the SF Oracle RAC (application cluster) nodes and the CP server use different AT root brokers, enter y at the installer prompt and provide the following information:
    - Hostname for the authentication broker for any one of the CP servers
    - Port number where the authentication broker for the CP server is listening for establishing trust
    - Hostname for the authentication broker for any one of the SF Oracle RAC (application cluster) nodes
    - Port number where the authentication broker for the SF Oracle RAC (application cluster) is listening for establishing trust

After the installer establishes trust between the authentication brokers of the CP servers and the application cluster nodes, press Enter to continue.

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

```
CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: rac_cluster101
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
```

11 Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the `/etc/vxfenmode` file with the appropriate details in each of the application cluster nodes.

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

```
Updating client cluster information on CP Server 10.210.80.199

Adding the client cluster to the CP Server 10.210.80.199 .................. Done

Registering client node galaxy with CP Server 10.210.80.199.............. Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ......... Done
Adding cluster rac_cluster101 to the CPClient user on CP Server 10.210.80.199 ... Done

Registering client node nebula with CP Server 10.210.80.199 ............. Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ......... Done
Adding cluster rac_cluster101 to the CPClient user on CP Server 10.210.80.199 ... Done

Updating /etc/vxfenmode file on galaxy ................................. Done
Updating /etc/vxfenmode file on nebula ......... ....................... Done
```

See "About I/O fencing configuration files" on page 608.

12 Configure the CP agent on the SF Oracle RAC (application cluster).

```
Do you want to configure CP Agent on the client cluster? [y,n,q]
(y)

Enter a non-existing name for the service group for CP Agent:
[b] (vxfen)

Adding CP Agent via galaxy ....................... Done
```

13 Review the output as the installer stops and restarts VCS with the fencing processes on each application cluster node, and completes the I/O fencing configuration.

14 Note the location of the configuration log files, summary files, and response files that the installer displays for later use.

Setting up server-based I/O fencing manually

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

Table 9-2 Tasks to set up server-based I/O fencing manually

Action	Description
Preparing the CP servers for use by the SF Oracle RAC cluster	See "Preparing the CP servers manually for use by the SF Oracle RAC cluster" on page 172.
Modifying I/O fencing configuration files to configure server-based I/O fencing	See "Configuring server-based fencing on the SF Oracle RAC cluster manually" on page 176.
Modifying SF Oracle RAC configuration to use I/O fencing	See "Modifying VCS configuration to use I/O fencing" on page 157.
Configuring Coordination Point agent to monitor coordination points	See "Configuring Coordination Point agent to monitor coordination points" on page 180.
Verifying the server-based I/O fencing configuration	See "Verifying server-based I/O fencing configuration" on page 182.

Preparing the CP servers manually for use by the SF Oracle RAC cluster

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

Table 9-3 displays the sample values used in this procedure.

Table 9-3 Sample values in procedure

CP server configuration component	Sample name
CP server	mycps1.symantecexample.com
Node #1 - SF Oracle RAC cluster	galaxy

Table 9-3 Sample values in procedure *(continued)*

CP server configuration component	Sample name
Node #2 - SF Oracle RAC cluster	nebula
Cluster name	rac_cluster101
Cluster UUID	{f0735332-1dd1-11b2}

To manually configure CP servers for use by the SF Oracle RAC cluster

1 Determine the cluster name and uuid on the SF Oracle RAC cluster.

For example, issue the following commands on one of the SF Oracle RAC cluster nodes (galaxy):

```
# grep cluster /etc/VRTSvcs/conf/config/main.cf

cluster rac_cluster101

# cat /etc/vx/.uuids/clusuuid

{f0735332-1dd1-11b2}
```

2 Use the `cpsadm` command to check whether the SF Oracle RAC cluster and nodes are present in the CP server.

For example:

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

ClusName  UUID                  Hostname(Node ID) Registered
rac_cluster101  {f0735332-1dd1-11b2} galaxy(0)         0
rac_cluster101  {f0735332-1dd1-11b2} nebula(1)         0
```

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

For detailed information about the `cpsadm` command, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide.*

3 Add the SF Oracle RAC cluster and nodes to each CP server.

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

```
# cpsadm -s mycps1.symantecexample.com -a add_clus\
 -c rac_cluster101  -u {f0735332-1dd1-11b2}

Cluster rac_cluster101 added successfully
```

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

```
# cpsadm -s mycps1.symantecexample.com -a add_node\
 -c rac_cluster101 -u {f0735332-1dd1-11b2} -h galaxy -n0

Node 0 (galaxy) successfully added
```

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

```
# cpsadm -s mycps1.symantecexample.com -a add_node\
 -c rac_cluster101 -u {f0735332-1dd1-11b2} -h nebula -n1

Node 1 (nebula) successfully added
```

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

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

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

Username/Domain Type  Cluster Name / UUID         Role

_HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com/vx
                      rac_cluster101/{f0735332-1dd1-11b2} Operator

_HA_VCS_nebula@HA_SERVICES@nebula.symantec.com/vx
                      rac_cluster101/{f0735332-1dd1-11b2} Operator
```

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

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

5 Add the users to the CP server.

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

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

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

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

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

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

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

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

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

For example, issue the following command on the CP server (mycps1.symantecexample.com) for SF Oracle RAC cluster rac_cluster101 with two nodes galaxy and nebula:

```
# cpsadm -s mycps1.symantecexample.com -a\
add_clus_to_user -c rac_cluster101\
 -u {f0735332-1dd1-11b2}\
 -e _HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com\
 -f cps_operator -g vx

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

# cpsadm -s mycps1.symantecexample.com -a\
add_clus_to_user -c rac_cluster101\
 -u {f0735332-1dd1-11b2}\
 -e _HA_VCS_nebula@HA_SERVICES@nebula.symantec.com\
 -f cps_operator -g vx

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

Configuring server-based fencing on the SF Oracle RAC cluster manually

The configuration process for the client or SF Oracle RAC cluster to use CP server as a coordination point requires editing the `/etc/vxfenmode` file.

You need to edit this file to specify the following information for your configuration:

- Fencing mode
- Fencing mechanism
- Fencing disk policy (if applicable to your I/O fencing configuration)
- Appropriate value for the security configuration
- CP server or CP servers
- Coordinator disk group (if applicable to your I/O fencing configuration)

Note: Whenever coordinator disks are used as coordination points in your I/O fencing configuration, you must create a disk group (vxfendg). You must specify this disk group in the `/etc/vxfenmode` file.

See "Setting up coordinator disk groups" on page 155.

The customized fencing framework also generates the `/etc/vxfentab` file which has security setting and the coordination points (all the CP servers and disks from disk group specified in `/etc/vxfenmode` file).

To configure server-based fencing on the SF Oracle RAC cluster manually

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

   `/etc/rc.config.d/vxfenconf`

   You must change the values of the VXFEN_START and the VXFEN_STOP environment variables to 1.

2. Use a text editor to edit the `/etc/vxfenmode` file values to meet your configuration specifications.

   If your server-based fencing configuration uses a single highly available CP server as its only coordination point, make sure to add the `single_cp=1` entry in the `/etc/vxfenmode` file.

   The following sample file output displays what the `/etc/vxfenmode` file contains:

   See "Sample vxfenmode file output" on page 177.

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

   For example:

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

Sample vxfenmode file output

The following sample file output displays

```
#
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
```

```
vxfen_mode=customized

# vxfen_mechanism determines the mechanism for customized I/O
# fencing that should be used.
#
# available options:
# cps      - use a coordination point server with optional script
#            controlled scsi3 disks
#
vxfen_mechanism=cps

#
# scsi3_disk_policy determines the way in which I/O Fencing
# communicates with the coordination disks. This field is
# required only if customized coordinator disks are being used.
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
scsi3_disk_policy=dmp

# security when enabled uses secure communication to the cp server
# using VxAT (Veritas Authentication Service)
# available options:
# 0 - don't use Veritas Authentication Service for cp server
#   communication
# 1  - use Veritas Authentication Service for cp server
#   communication
security=1

#
# Specify 3 or more odd number of coordination points in this file,
# one in each row. They can be all-CP servers, all-SCSI-3 compliant
# coordinator disks, or a combination of CP servers and SCSI-3
# compliant coordinator disks. Please ensure that the CP server
# coordination points are numbered sequentially and in the same
# order on all the cluster nodes.
#
# Coordination Point Server(CPS) is specified as:
#
#  cps<number>=<Virtual IP/ Virtual hostname of cp server> in
# square brackets ([]), followed by ":" and CPS port number.
```

```
#
# Examples:
# cps1=[192.168.0.23]:14250
# cps2=[mycps.company.com]:14250
#
# SCSI-3 compliant coordinator disks are specified as:
#
#  vxfendg=<coordinator disk group name>
# Example:
#  vxfendg=vxfencoorddg
#
# Examples of different configurations:
#  1. All CP server coordination points
# cps1=
# cps2=
# cps3=
#
# 2. A combination of CP server and a disk group having two SCSI-3
# coordinator disks
# cps1=
# vxfendg=
# Note: The disk group specified in this case should have two disks
#
# 3. All SCSI-3 coordinator disks
# vxfendg=
# Note: The disk group specified in case should have three disks
#
```

Table 9-4 defines the vxfenmode parameters that must be edited.

Table 9-4 vxfenmode file parameters

vxfenmode File Parameter	Description
vxfen_mode	Fencing mode of operation. This parameter must be set to “customized”.
vxfen_mechanism	Fencing mechanism. This parameter defines the mechanism that is used for fencing. If one of the three coordination points is a CP server, then this parameter must be set to “cps”.
scsi3_disk_policy	Configure the vxfen module to use either DMP devices, "dmp" or the underlying raw character devices, "raw". **Note:** The configured disk policy is applied on all the nodes.

Table 9-4 vxfenmode file parameters *(continued)*

vxfenmode File Parameter	Description
security	Security parameter 1 indicates that Symantec Product Authentication Service is used for CP server communications. Security parameter 0 indicates that communication with the CP server is made in non-secure mode. The default security value is 1. **Note:** Symantec only supports a configuration where both the CP server and client sides have the same security setting. The security setting on both sides must be either enabled or disabled.
cps1, cps2, cps3, or vxfendg	Coordination point parameters. Enter either the Virtual IP address or FQHN (whichever is accessible) of the CP server. **Note:** Whenever coordinator disks are used in an I/O fencing configuration, a disk group has to be created (vxfendg) and specified in the /etc/vxfenmode file. Additionally, the customized fencing framework also generates the /etc/vxfentab file which specifies the security setting and the coordination points (all the CP servers and the disks from disk group specified in /etc/vxfenmode file).
single_cp	Value 1 for single_cp parameter indicates that the server-based fencing uses a single highly available CP server as its only coordination point. Value 0 for single_cp parameter indicates that the server-based fencing uses at least three coordination points.

Configuring Coordination Point agent to monitor coordination points

The following procedure describes how to manually configure the Coordination Point agent to monitor coordination points (CP server or SCSI-3 disks).

To configure Configuration Point agent to monitor coordination points

1. Ensure that your SF Oracle RAC cluster has been properly installed and configured with fencing enabled.
2. Create a parallel service group vxfen and add a coordpoint resource to the vxfen service group using the following commands:

```
# haconf -makerw
# hagrp -add vxfen
# hagrp -modify vxfen SystemList galaxy 0 nebula 1
# hagrp -modify vxfen AutoFailOver 0
# hagrp -modify vxfen Parallel 1
# hagrp -modify vxfen SourceFile "./main.cf"
# hares -add coordpoint CoordPoint vxfen
# hares -modify coordpoint FaultTolerance 1
# hares -modify coordpoint Enabled 1
# haconf -dump -makero
```

3 Verify the status of the agent on the SF Oracle RAC cluster using the `hares` commands. For example:

```
# hares -state coordpoint
```

The following is an example of the command and output:

```
# hares -state coordpoint

# Resource    Attribute   System   Value
coordpoint   State        galaxy   ONLINE
coordpoint   State        nebula   ONLINE
```

4 Access the engine log to view the agent log. The agent log is written to the engine log.

The agent log contains detailed Coordination Point agent monitoring information; including information about whether the Coordination Point agent is able to access all the coordination points, information to check on which coordination points the Coordination Point agent is reporting missing keys, etc.

To view all such information in the engine log, change the dbg level for that node using the following commands:

```
# haconf -makerw

# hatype -modify Coordpoint LogDbg 10

# haconf -dump -makero
```

The agent log can now be viewed at the following location:

/var/VRTSvcs/log/engine_A.log

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

Verifying server-based I/O fencing configuration

Follow the procedure described below to verify your server-based I/O fencing configuration.

To verify the server-based I/O fencing configuration

1 Verify that the I/O fencing configuration was successful by running the `vxfenadm` command.

For example, run the following command:

```
# vxfenadm -d
```

Note: For troubleshooting any server-based I/O fencing configuration issues, refer to the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

---

2 Verify that I/O fencing is using the specified coordination points by running the `vxfenconfig` command.

For example, run the following command:

```
# vxfenconfig -l
```

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

Chapter 10

Performing post-installation and configuration tasks

This chapter includes the following topics:

- About enabling LDAP authentication for clusters that run in secure mode
- Configuring Veritas Volume Replicator
- Verifying SF Oracle RAC installation using VCS configuration file
- Verifying LLT, GAB, and cluster operation
- Running VRTSexplorer to diagnose issues in the cluster

About enabling LDAP authentication for clusters that run in secure mode

Symantec Product Authentication Service (AT) supports LDAP (Lightweight Directory Access Protocol) user authentication through a plug-in for the authentication broker. AT supports all common LDAP distributions such as Sun Directory Server, Netscape, OpenLDAP, and Windows Active Directory.

For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain.

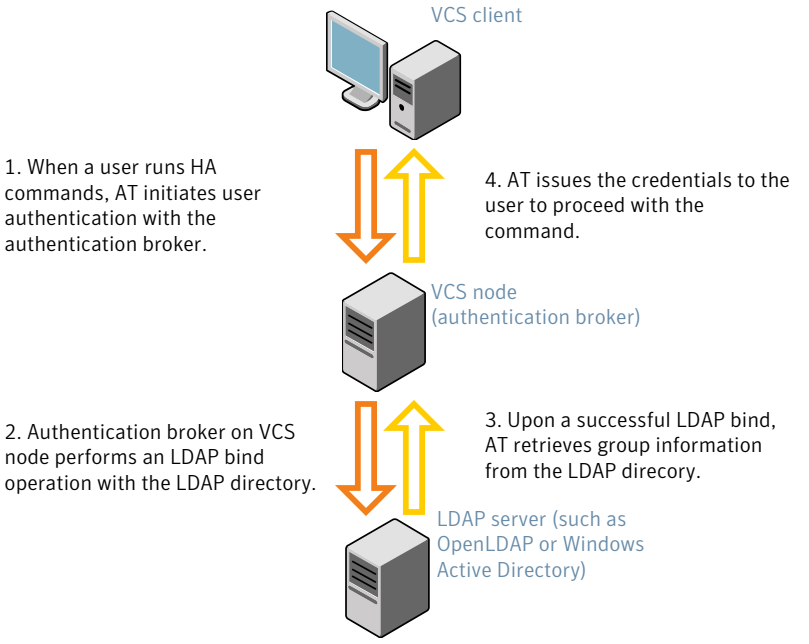
See "Enabling LDAP authentication for clusters that run in secure mode" on page 187.

If you have not already added VCS users during installation, you can add the users later.

See the *Veritas Cluster Server Administrator's Guide* for instructions to add VCS users.

Figure 10-1 depicts the SF Oracle RAC cluster communication with the LDAP servers when clusters run in secure mode.

Figure 10-1 Client communication with LDAP servers



See the *Symantec Product Authentication Service Administrator's Guide.*

The LDAP schema and syntax for LDAP commands (such as, ldapadd, ldapmodify, and ldapsearch) vary based on your LDAP implementation.

Before adding the LDAP domain in Symantec Product Authentication Service, note the following information about your LDAP environment:

- The type of LDAP schema used (the default is RFC 2307)
  - UserObjectClass (the default is posixAccount)
  - UserObject Attribute (the default is uid)
  - User Group Attribute (the default is gidNumber)
  - Group Object Class (the default is posixGroup)
  - GroupObject Attribute (the default is cn)

- Group GID Attribute (the default is gidNumber)
- Group Membership Attribute (the default is memberUid)

- URL to the LDAP Directory
- Distinguished name for the user container (for example, UserBaseDN=ou=people,dc=comp,dc=com)
- Distinguished name for the group container (for example, GroupBaseDN=ou=group,dc=comp,dc=com)

Enabling LDAP authentication for clusters that run in secure mode

The following procedure shows how to enable the plug-in module for LDAP authentication. This section provides examples for OpenLDAP and Windows Active Directory LDAP distributions.

Before you enable the LDAP authentication, complete the following steps:

- Make sure that the cluster runs in secure mode.

  ```
  # haclus -value SecureClus
  ```

  The output must return the value as 1.

- Make sure that the AT version is 5.0.32.0 or later.

  ```
  # /opt/VRTSat/bin/vssat showversion
  vssat version: 5.0.32.0
  ```

See the `vssat.1m` and the `atldapconf.1m` manual pages.

To enable OpenLDAP authentication for clusters that run in secure mode

1 Add the LDAP domain to the AT configuration using the `vssat` command.

The following example adds the LDAP domain, MYENTERPRISE:

```
# /opt/VRTSat/bin/vssat addldapdomain \
--domainname "MYENTERPRISE.symantecdomain.com"\
--server_url "ldap://my_openldap_host.symantecexample.com"\
--user_base_dn "ou=people,dc=symantecdomain,dc=myenterprise,dc=com"\
--user_attribute "cn" --user_object_class "account"\
--user_gid_attribute "gidNumber"\
--group_base_dn "ou=group,dc=symantecdomain,dc=myenterprise,dc=com"\
--group_attribute "cn" --group_object_class "posixGroup"\
--group_gid_attribute "member"\
--admin_user "cn=manager,dc=symantecdomain,dc=myenterprise,dc=com"\
--admin_user_password "password" --auth_type "FLAT"
```

2 Verify that you can successfully authenticate an LDAP user on the SF Oracle RAC nodes.

You must have a valid LDAP user ID and password to run the command. In the following example, authentication is verified for the MYENTERPRISE domain for the LDAP user, vcsadmin1.

```
galaxy# /opt/VRTSat/bin/vssat authenticate
--domain ldap:MYENTERPRISE.symantecdomain.com
--prplname vcsadmin1 --broker galaxy:2821

Enter password for vcsadmin1: ##########

authenticate
----------------------
----------------------

Authenticated User vcsadmin1
----------------------
```

3 Add the LDAP user to the main.cf file.

```
# haconf makerw
# hauser -add "CN=vcsadmin1/CN=people/\
DC=symantecdomain/DC=myenterprise/\
DC=com@myenterprise.symantecdomain.com" -priv Administrator
# haconf -dump -makero
```

If you want to enable group-level authentication, you must run the following command:

```
# hauser -addpriv \
ldap_group@ldap_domain AdministratorGroup
```

4 Verify that the main.cf file has the following lines:

```
# cat /etc/VRTSvcs/conf/config/main.cf
...
...
cluster rac_cluster101 (
  SecureClus = 1
  Administrators = {
    "CN=vcsadmin1/CN=people/DC=symantecdomain/DC=myenterprise/
    DC=com@myenterprise.symantecdomain.com" }
  AdministratorGroups = {
    "CN=symantecusergroups/DC=symantecdomain/DC=myenterprise/
    DC=com@myenterprise.symantecdomain.com " }
  )
...
...
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=myenterprise.symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh or ksh), run the following commands:

```
# export VCS_DOMAIN=myenterprise.symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
galaxy     Attribute  RUNNING
nebula     Attribute  RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the SF Oracle RAC node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.

To enable Windows Active Directory authentication for clusters that run in secure mode

1 Run the LDAP configuration tool atldapconf using the -d option. The -d option discovers and retrieves an LDAP properties file which is a prioritized attribute list.

```
# /opt/VRTSat/bin/atldapconf -d
-s domain_controller_name_or_ipaddress
-u domain_user -g domain_group
```

For example:

```
# /opt/VRTSat/bin/atldapconf -d -s 192.168.20.32 \
-u Administrator -g "Domain Admins"
Search User provided is invalid or Authentication is required to
proceed further.
Please provide authentication information for LDAP server.

Username/Common Name: symantecdomain\administrator
Password:

Attribute file created.
```

2 Run the LDAP configuration tool atldapconf using the -c option. The -c option creates a CLI file to add the LDAP domain.

```
# /opt/VRTSat/bin/atldapconf -c -d windows_domain_name
```

For example:

```
# /opt/VRTSat/bin/atldapconf -c -d symantecdomain.com
Attribute list file not provided, using default AttributeList.txt.
CLI file name not provided, using default CLI.txt.

CLI for addldapdomain generated.
```

3 Run the LDAP configuration tool atldapconf using the -x option. The -x option reads the CLI file and executes the commands to add a domain to the AT.

```
# /opt/VRTSat/bin/atldapconf -x
```

4 List the LDAP domains to verify that the Windows Active Directory server integration is complete.

```
# /opt/VRTSat/bin/vssat listldapdomains

Domain Name :          symantecdomain.com
Server URL :           ldap://192.168.20.32:389
SSL Enabled :          No
User Base DN :         CN=people,DC=symantecdomain,DC=com
User Object Class :    account
User Attribute :       cn
User GID Attribute :   gidNumber
Group Base DN :        CN=group,DC=symantecdomain,DC=com
Group Object Class :   group
Group Attribute :      cn
Group GID Attribute :  cn
Auth Type :            FLAT
Admin User :
Admin User Password :
Search Scope :         SUB
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh or ksh), run the following commands:

```
# export VCS_DOMAIN=symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
galaxy     Attribute  RUNNING
nebula     Attribute  RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the SF Oracle RAC 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 Veritas 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 Oracle RAC, 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 *Veritas 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-5-2-3728  Starting Communication daemon: [OK]
VxVM VVR  V-5-4-2415 Starting VRAS daemon: [OK]
VxVM VVR  V-5-4-2415 Starting VxRSyncd daemon: [OK]
```

Verifying SF Oracle RAC 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 Oracle RAC installation and before the Oracle 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 not automatically present; you must manually add it after the installation.
- If you configured the cluster in secure mode, the main.cf includes the VxSS service group and “SecureClus = 1” cluster attribute.

For more information on the configuration file:

See “About VCS configuration file ” on page 605.

Verifying LLT, GAB, and cluster operation

Verify the operation of LLT, GAB, and the cluster using the VCS commands.

To verify LLT, GAB, and cluster operation

1. Log in to any node in the cluster as superuser.
2. Make sure that the PATH environment variable is set to run the VCS commands.
3. Verify LLT operation.

   See “Verifying LLT” on page 195.
4. Verify GAB operation.

   See “Verifying GAB” on page 197.
5. Verify the cluster operation.

   See “Verifying the cluster” on page 198.

Verifying LLT

Use the `lltstat` command to verify that links are active for LLT. If LLT is configured correctly, this command shows all the nodes in the cluster. The command also returns information about the links for LLT for the node on which you typed the command.

Refer to the `lltstat(1M)` manual page for more information.

To verify LLT

1. Log in as superuser on the node galaxy.
2. Run the `lltstat` command on the node galaxy to view the status of LLT.

   ```
   lltstat -n
   ```

   The output on galaxy resembles:

   ```
   LLT node information:
       Node             State           Links
       *0 galaxy          OPEN           2
        1 nebula          OPEN           2
   ```

   Each node has two links and each node is in the OPEN state. The asterisk (*) denotes the node on which you typed the command.

   If LLT does not operate, the command does not return any LLT links information: If only one network is connected, the command returns the following LLT statistics information:

   ```
   LLT node information:
       Node                State    Links
      * 0 galaxy           OPEN        2
        1 nebula           OPEN        2
        2 saturn           OPEN        1
   ```

3. Log in as superuser on the node nebula.
4. Run the `lltstat` command on the node nebula to view the status of LLT.

   ```
   lltstat -n
   ```

   The output on nebula resembles:

   ```
   LLT node information:
       Node             State           Links
        0 galaxy          OPEN           2
       *1 nebula          OPEN           2
   ```

5 To view additional information about LLT, run the `lltstat -nvv` command on each node.

For example, run the following command on the node galaxy in a two-node cluster:

```
lltstat -nvv active
```

The output on galaxy resembles:

```
Node          State      Link    Status      Address
*0 galaxy      OPEN
                         lan1 UP     08:00:20:93:0E:34
                         lan2 UP     08:00:20:93:0E:38
1 nebula       OPEN
                         lan1 UP     08:00:20:8F:D1:F2
                         lan2 DOWN
```

The command reports the status on the two active nodes in the cluster, galaxy and nebula.

For each correctly configured node, the information must show the following:

- A state of OPEN
- A status for each link of UP
- A MAC address for each link

However, the output in the example shows different details for the node nebula. The private network connection is possibly broken or the information in the `/etc/lltab` file may be incorrect.

6 To obtain information about the ports open for LLT, type `lltstat -p` on any node.

For example, type `lltstat -p` on the node galaxy in a two-node cluster:

```
lltstat -p
```

The output resembles:

```
LLT port information:
  Port  Usage       Cookie
  0     gab          0x0
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
  7     gab          0x7
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
```

```
63    gab          0x1F
      opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
      connects:    0 1
```

Verifying 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 SF Oracle RAC 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
d	Oracle Disk Manager (ODM)
f	Cluster File System (CFS)
h	Veritas Cluster Server (VCS: High Availability Daemon)
o	VCSMM driver
u	Cluster Volume Manager (CVM) (to ship commands from slave node to master node) Port u in the `gabconfig` output is visible with CVM protocol version >= 100.
v	Cluster Volume Manager (CVM)
w	vxconfigd (module for CVM)

For more information on GAB, refer to the *Veritas 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  ada401 membership 01

  Port b gen  ada40d membership 01

  Port d gen  ada409 membership 01
  Port f gen  ada41c membership 01
  Port h gen  ada40f membership 01

  Port o gen  ada406 membership 01

  Port u gen  ada41a membership 01

  Port v gen  ada416 membership 01
  Port w gen  ada418 membership 01
  ```

Verifying the cluster

Verify the status of the cluster using the `hastatus` command. This command returns the system state and the group state.

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

Refer to the *Veritas Cluster Server Administrator's Guide* for a description of system states and the transitions between them.

To verify the cluster

1 To verify the status of the cluster, type the following command:

```
hastatus -summary
```

The output resembles:

```
-- SYSTEM STATE
-- System               State                Frozen

A  galaxy                RUNNING               0
A  nebula                RUNNING               0

-- GROUP STATE
-- Group           System         Probed   AutoDisabled    State

B  cvm             galaxy          Y        N               ONLINE
B  cvm             nebula          Y        N               ONLINE

B  VxSS            galaxy          Y        N               ONLINE
B  VxSS            nebula          Y        N               ONLINE
```

Note that the VxSS service group is displayed only if you have configured the cluster in secure mode.

2 Review the command output for the following information:

- The system state
  If the value of the system state is RUNNING, the cluster is successfully started.
- The cvm group state
  In the sample output, the group state lists the cvm group, which is ONLINE on both the nodes galaxy and nebula.

Verifying the cluster nodes

Verify the information of the cluster systems using the `hasys -display` command. The information for each node in the output should be similar.

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

Refer to the *Veritas Cluster Server Administrator's Guide* for information about the system attributes for VCS.

To verify the cluster nodes

- On one of the nodes, type the `hasys -display` command:

```
hasys -display
```

The example shows the output when the command is run on the node galaxy. The list continues with similar information for nebula (not shown) and any other nodes in the cluster.

```
#System    Attribute             Value

galaxy     AgentsStopped         0

galaxy     AvailableCapacity     100

galaxy     CPUBinding            BindTo None CPUNumber 0

galaxy     CPUThresholdLevel     Critical 90 Warning 80 Note 70
                                 Info 60

galaxy     CPUUsage              0

galaxy     CPUUsageMonitoring    Enabled 0 ActionThreshold 0
                                 ActionTimeLimit 0 Action NONE
                                 NotifyThreshold 0 NotifyTimeLimit 0

galaxy     Capacity              100

galaxy     ConfigBlockCount      141

galaxy     ConfigCheckSum        33975

galaxy     ConfigDiskState       CURRENT

galaxy     ConfigFile            /etc/VRTSvcs/conf/config

galaxy     ConfigInfoCnt         0

galaxy     ConfigModDate         Wed 14 Oct 2009 17:22:48

galaxy     ConnectorState        Down

galaxy     CurrentLimits

galaxy     DiskHbStatus

galaxy     DynamicLoad           0

galaxy     EngineRestarted       0

galaxy     EngineVersion         5.1.10.0

galaxy     FencingWeight         0
```

```
galaxy    Frozen                0
galaxy    GUIIPAddr
galaxy    HostUtilization       CPU 0 Swap 0
galaxy    LLTNodeId             0
galaxy    LicenseType           DEMO
galaxy    Limits
galaxy    LinkHbStatus
galaxy    LoadTimeCounter       0
galaxy    LoadTimeThreshold     600
galaxy    LoadWarningLevel      80
galaxy    NoAutoDisable         0
galaxy    NodeId                0
galaxy    OnGrpCnt              1
galaxy    ShutdownTimeout
galaxy    SourceFile            ./main.cf
galaxy    SwapThresholdLevel    Critical 90 Warning 80 Note 70
                                Info 60
galaxy    SysInfo               HP-UX:galaxy,U,B.11.31,ia64
galaxy    SysName               galaxy
galaxy    SysState              RUNNING
galaxy    SystemLocation
galaxy    SystemOwner
galaxy    TFrozen               0
galaxy    TRSE                  0
galaxy    UpDownState           Up
galaxy    UserInt               0
galaxy    UserStr
```

```
galaxy     VCSFeatures            DR

galaxy     VCSMode                VCS_RAC
```

Running VRTSexplorer to diagnose issues in the cluster

Perform this step if you encounter issues in your cluster environment that require professional support.

VRTSexplorer, also known as Veritas Explorer, is a tool provided by Symantec to gather system and configuration information from a node to diagnose or analyze issues in the cluster. The utility is located at `/opt/VRTSspt/VRTSexplorer`.

Note: The utility collects only technical information such as the server configuration and installed Veritas products information required to troubleshoot issues. No user data is collected by the utility. For more details on the information that is collected by the utility, refer to the README located in the `/opt/VRTSspt/VRTSexplorer` directory.

To run the utility:

```
# cd /opt/VRTSspt/VRTSexplorer
# ./VRTSexplorer
```

For information on various command options, see `VRTSexplorer` (1M).

If you find issues in the cluster that require professional help, run the utility and send the compressed tar file output to Symantec Technical Support to resolve the issue.

Section 3

Upgrade of SF Oracle RAC

- Chapter 11. Preparing to upgrade to SF Oracle RAC 5.1 SP1
- Chapter 12. Performing a full upgrade to SF Oracle RAC 5.1 SP1
- Chapter 13. Performing a phased upgrade to SF Oracle RAC 5.1 SP1
- Chapter 14. Upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1
- Chapter 15. Migrating from single instance Storage Foundation for Oracle HA to SF Oracle RAC
- Chapter 16. Performing post-upgrade tasks

Chapter 11

Preparing to upgrade to SF Oracle RAC 5.1 SP1

This chapter includes the following topics:

- About upgrading SF Oracle RAC
- About types of upgrade
- Supported upgrade paths
- Preparing to upgrade to SF Oracle RAC 5.1 SP1
- Pre-upgrade tasks for migrating the SFDB repository database

About upgrading SF Oracle RAC

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

For the supported types of upgrade:

See "About types of upgrade" on page 206.

For the supported upgrade paths:

See "Supported upgrade paths" on page 206.

Note: SF Oracle RAC software must be at the same version across all nodes in an SF Oracle RAC cluster after the upgrade, that is 5.1 Service Pack 1.

About types of upgrade

Table 11-1 lists the supported types of upgrade.

Table 11-1 Types of upgrade

Type of upgrade	Method of upgrade	Procedures
Full upgrade	Veritas script-based installation programs ■ Interactive mode ■ Non-interactive mode using response files	Complete the following steps: ■ Preparing to upgrade See "Preparing to upgrade to SF Oracle RAC 5.1 SP1" on page 208. ■ Upgrading to SF Oracle RAC 5.1 SP1 See the chapter *Performing a full upgrade to SF Oracle RAC 5.1 SP1*. ■ Completing post-upgrade tasks See the chapter "Performing post-upgrade tasks".
Phased upgrade	Combination of manual steps and the Veritas script-based installation programs	Complete the steps in the chapter *Performing a phased upgrade to SF Oracle RAC 5.1 SP1*.

Supported upgrade paths

Table 11-2 lists the supported upgrade paths.

Table 11-2 Supported upgrade paths

From SF Oracle RAC version	To SF Oracle RAC version	Supported upgrade type
3.5 and later versions on HP-UX 11i(including updates on 3.5)	5.1 SP1	**Note:** SF Oracle RAC does not support direct upgrades from version 3.5. You need to first upgrade to version 4.1, then upgrade to SF Oracle RAC 5.1 SP1. For instructions on upgrading to version 4.1, see the *Veritas Storage Foundation 4.1 for Oracle RAC Installation and Configuration Guide*. Contact Technical Support to obtain the software media or to download the software for version 4.1.
SF Oracle RAC 4.1 and later versions on HP-UX 11iv2 (including maintenance packs and rolling patches on 4.1)	5.1 SP1	Full or phased upgrade
SF Oracle RAC 5.0 and later versions on HP-UX 11iv2 (including maintenance packs and rolling patches on 5.0)	5.1 SP1	Full or phased upgrade
SF Oracle RAC 5.0 and later versions on HP-UX 11iv3 (including maintenance packs and rolling patches on 5.0)	5.1 SP1	Full or phased upgrade
SF Oracle RAC 5.0.1 and later versions on HP-UX 11iv3 (including maintenance packs and rolling patches on 5.0.1)	5.1 SP1	Full or phased upgrade

Preparing to upgrade to SF Oracle RAC 5.1 SP1

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, CVMTypes.cf, CFSTypes.cf, OracleTypes.cf, OracleASMTypes.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
   # 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 \
   /var/tmp/PrivNIC.cf.save
   # cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf \
   /var/tmp/MultiPrivNIC.cf.save
   ```

3. Stop all applications that use VxFS or VxVM disk groups, whether local or CFS.

   If the applications are under VCS control:

   ```
   # hagrp -offline grp_name -any
   ```

   If the applications are not under VCS control:

   Use native application commands to stop the application.

4. For Oracle RAC 9i, log in as Oracle user on each node and stop `gsd`:

   ```
   $ $ORACLE_HOME/bin/gsdctl stop
   ```

5. For Oracle RAC 10g and Oracle RAC 11g:

   Stop all Oracle RAC resources.

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

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

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

```
# hagrp -offline group_name -any
```

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
# hagrp -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:

```
$ srvctl modify database -d db-name -y manual
```

7 Unmount the non-system files on the VxFS file system, which is not under VCS control.

```
# mount -v |grep vxfs

# 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
```

8 Stop VCS on all nodes:

```
# hastop -all
```

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 5.1 SP1.

10 Perform the following steps only if you are upgrading from HP-UX 11i v2:

- If the cluster-wide attribute “UseFence” is set to SCSI3, then reset the value to NONE in the /etc/VRTSvcs/conf/config/main.cf file.

- On each node, edit the /etc/vxfenmode file to configure I/O fencing in disabled mode.

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

Note: If you upgrade from SF Oracle RAC 4.1 on HP-UX 11iv2, create `/etc/vxfenmode` file and populate it as above.

- On each node, change LLT_START=0 in the file /etc/rc.config.d/lltconf.
- On each node, remove the following device files:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
# rm -f /dev/lmx
# rm -f /dev/vcsmm
```

Pre-upgrade tasks for migrating the SFDB repository database

If you plan to continue using checkpoints or SmartTier for Oracle policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, you must migrate the SFDB repository database to 5.1 Service Pack 1.

If you are upgrading from 5.1 to 5.1 Service Pack 1, no upgrade steps are required for the SFDB tools.

Note: The Sfua_Base repository resource group will be removed from the main.cf file. It is not required as a separate service group for SF Oracle RAC 5.1 Service Pack 1.

Perform the following before upgrading SF Oracle RAC.

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 carried over after upgrading. You must create a new Database Flashsnap clone database after upgrading to 5.1 Service Pack 1.

Chapter 12

Performing a full upgrade to SF Oracle RAC 5.1 SP1

This chapter includes the following topics:

- About full upgrades
- Upgrading to SF Oracle RAC 5.1 SP1

About full upgrades

A full upgrade involves upgrading all the nodes in the cluster at the same time. The cluster remains unavailable for the duration of the upgrade.

You can perform the upgrade using one of the following Veritas script-based installation programs:

- Common product installer (`installer`)

  The common product installer provides menu options for installing and configuring multiple Veritas products.
- SF Oracle RAC installation script (`installsfrac`)

  The SF Oracle RAC installation script provides menu options for installing and configuring SF Oracle RAC.

Note: If you obtained SF Oracle RAC from an electronic download site, you must use the product installer (`installsfrac`) instead of the common product installer (`installer`).

You can also perform a full upgrade using a response file. You can create a response file using the response file template or customize an installer-generated response file.

Note: After you upgrade to version 5.1 SP1 from version 5.1 or related 5.1 rolling patches, Symantec recommends that you do not roll back to version 5.1 or corresponding rolling patches.

For more information about response files:

See "About response files" on page 371.

Upgrading to SF Oracle RAC 5.1 SP1

Perform the steps in the following procedure to upgrade to SF Oracle RAC 5.1 SP1.

Note: If you are upgrading from SF Oracle RAC versions 3.5, 3.5 Update 3, and 3.5 Update 4, you need to first upgrade to version 4.1, then upgrade to SF Oracle RAC 5.1 SP1. For instructions on upgrading to version 4.1, see the *Veritas Storage Foundation 4.1 for Oracle RAC Installation and Configuration Guide*.

Contact Technical Support to obtain the software media or to download the software for version 4.1.

To upgrade to SF Oracle RAC 5.1 SP1

1. Upgrade the operating system, if required.

   See "Upgrading the HP-UX operating system" on page 215.

   For instructions, see the operating system documentation.

2. Upgrade to SF Oracle RAC 5.1 SP1.

   See "Upgrading SF Oracle RAC using the Veritas script-based installation program" on page 216.

   You can also perform a silent upgrade:

   See "Upgrading SF Oracle RAC using a response file" on page 218.

3. Relink the SF Oracle RAC libraries with Oracle.

   See "Relinking Oracle RAC libraries with the SF Oracle RAC libraries" on page 257.

4. Bring the Oracle database service group online.

   - If the Oracle database is managed by VCS:

     ```
     # hagrp -online oracle_group -sys node_name
     ```

- If the Oracle database is not managed by VCS:

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

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

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

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
# hagrp -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:

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

8 Complete other post-upgrade steps.

For instructions, see the chapter *Performing post-upgrade tasks* in this document.

9 For upgrade scenarios that involve Oracle RAC 9i, start `gsd` as the Oracle user:

```
$ $ORACLE_HOME/bin/gsdctl start
```

10 Upgrade Oracle RAC.

For instructions, see the chapter *Upgrading Oracle RAC* in this document.

11 If you want to upgrade CP server systems that use VCS or SFHA to 5.1 SP1, make sure that you upgraded all application clusters to version 5.1 SP1. Then, upgrade VCS or SFHA on the CP server systems.

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

Upgrading the HP-UX operating system

If you are on an unsupported version of the operating system, you need to upgrade it to HP-UX B.11.31.1009, HP-UX 11i Version 3 September 2010 Operating Environments Update Release or later.

If you are upgrading the operating system from HP-UX 11i v2, make sure that you choose the following depots along with the HP-UX 11i v3 September 2010 OEUR release depots:

- Base-VxFS-50
- Base-VxTools-50
- Base-VxVM-50

To upgrade the operating system from HP-UX 11i v2, run the update-ux command specifying the Veritas depots along with the HP-UX operating system depots:

```
# swinstall -s  os_path Update-UX
# update-ux -s os_path HPUX11i-DC-OE \
Base-VxFS-50 Base-VxTools-50 Base-VxVM-50
```

where os_path is the full path of the directory containing the operating system depots.

To upgrade the operating system from HP-UX 11i v3, run the update-ux command as follows:

```
# update-ux -s os_path HPUX11i-DC-OE
```

where os_path is the full path of the directory containing the operating system depots.

For detailed instructions on upgrading the operating system, see the operating system documentation.

Upgrading SF Oracle RAC using the Veritas script-based installation program

Use one of the following Veritas script-based sinstallation programs to upgrade SF Oracle RAC: installer or installsfrac

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 5.1 SP1 depots on the nodes.
- Starts SF Oracle RAC 5.1 SP1 on all the nodes.
- Displays the location of the log files, summary file, and response file.

Note: If you upgrade to version 5.1 SP1 from version 5.1 or related 5.1 rolling patches, Symantec recommends that you do not roll back to version 5.1 or corresponding rolling patches.

To upgrade to SF Oracle RAC 5.1 SP1 using the installsfrac program

1 Start the installation program using one of the following ways:

SF Oracle RAC installer	Navigate to the directory that contains the installation program. The program is located in the product directory. Run the program: `# ./installsfrac galaxy nebula`
Common product installer	Navigate to the directory that contains the installation program. Run the program: `# ./installer galaxy nebula` From the opening Selection Menu, choose **G** for "**Upgrade a Product**." From the displayed list of products, choose **Veritas Storage Foundation for Oracle RAC**.

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

2 Enter **3** to install all the SF Oracle RAC depots.

Before you select an option, you can view the list of depots that are installed for each option by choosing option 4.

```
1)  Install minimal required Veritas Storage Foundation for Oracle RAC
    depots
2)  Install recommended Veritas Storage Foundation for Oracle RAC
    depots
3)  Install all Veritas Storage Foundation for Oracle RAC
    depots
4)  Display depots to be installed for each option
Select the depots to be installed on all systems? [1-4,q,?] (2) 3
```

The installer verifies the systems for compatibility.

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

3 Press **Enter** to continue with the upgrade.

Depending on the installation option selected, the installer displays the list of depots that will be installed and prompts for the stoppage of SF Oracle RAC processes before the upgrade.

4 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 SF Oracle RAC processes and shuts down SF Oracle RAC on all nodes in the cluster. It uninstalls the existing SF Oracle RAC packages on the cluster and installs SF Oracle RAC 5.1 SP1 packages.

5 Enable fencing:

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

6 Restart each node in the cluster.

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

7 Complete the remaining tasks to finish the upgrade:

See "Upgrading to SF Oracle RAC 5.1 SP1" on page 214.

Upgrading SF Oracle RAC using a response file

You can upgrade from SF Oracle RAC version 4.1 MP2 and later using a response file.

Perform the steps in the following procedure to upgrade to SF Oracle RAC 5.1 SP1 using a response file.

To upgrade SF Oracle RAC using a response file

1 Upgrade the operating system, if required.

For instructions, see the operating system documentation.

2 Create a response file using one of the available options.

Note: Make sure that you replace the host names in the response file with the names of the systems that you plan to upgrade.

For information on various options available for creating a response file:

See "About response files" on page 371.

For response file variable definitions:

See "Response file variables to upgrade SF Oracle RAC" on page 219.

For a sample response file:

See "Sample response file for upgrading SF Oracle RAC" on page 221.

3 Navigate to the directory containing the SF Oracle RAC installation program.

4 Start the installation:

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

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

5 Restart the nodes in the cluster:

```
# shutdown -r now
```

6 Complete the post-upgrade steps.

See the chapter "Performing post-upgrade tasks" in this document.

Response file variables to upgrade SF Oracle RAC

Table 12-1 lists the response file variables that you can define to upgrade SF Oracle RAC.

Table 12-1 Response file variables specific to upgrading SF Oracle RAC

Variable	List or Scalar	Description
CFG{opt}{upgrade}	Scalar	Upgrades SF Oracle RAC depots. (Required)

Table 12-1 Response file variables specific to upgrading SF Oracle RAC *(continued)*

Variable	List or Scalar	Description
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)
CFG{opt}{systems}	List	List of systems on which the product is to be upgraded. (Required)
CFG{prod}	Scalar	Defines the product to be upgraded. (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{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{patchpath}	Scalar	Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems. (Optional)
CFG{opt}{pkgpath}	Scalar	Defines a location, typically an NFS mount, from which all remote systems can install product depots. The location must be accessible from all target systems. (Optional)

Table 12-1 Response file variables specific to upgrading SF Oracle RAC *(continued)*

Variable	List or Scalar	Description
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the depots that are needed during the install. The default location is /var/tmp. (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 *logpath* location. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *remsh* must be used instead of ssh as the communication method between systems. (Optional)

Sample response file for upgrading SF Oracle RAC

The following sample response file upgrades SF Oracle RAC to version 5.1 Service Pack 1 on nodes, galaxy and nebula.

```
our  %CFG;

$CFG{accepteula}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{opt}{patchupgrade}=1;
$CFG{prod}="SFRAC51";
$CFG{systems}=[ qw(galaxy nebula)];
$CFG{vcs_allowcomms}=1;

1;
```

Chapter 13

Performing a phased upgrade to SF Oracle RAC 5.1 SP1

This chapter includes the following topics:

- About phased upgrade
- Performing phased upgrade of SF Oracle RAC from version 5.0

About phased upgrade

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

Note: You can perform a phased upgrade only if the Oracle RAC binaries are present on the local file system.

SF Oracle RAC supports phased upgrade of the cluster from the following versions:

- Version 5.0x on HP-UX 11i v3
- Version 4.x on HP-UX 11i v2
- Version 5.0x on HP-UX 11i v2

Caution: There is a potential for dependency problems between product components that no longer match when upgrading part of a cluster at a time. Follow the phased upgrade procedures carefully to avoid these problems.

Note: There will be some downtime involved. Review the procedures and carefully plan your downtime before proceeding with any steps. The sample procedures assume that Oracle RAC binaries are installed on local file systems for each node in the cluster.

The examples in the procedures assume a four-node SF Oracle RAC cluster with the nodes *galaxy* and *nebula* constituting the first half of the cluster and the nodes *jupiter* and *mercury* constituting the second half of the cluster.

Performing phased upgrade of SF Oracle RAC from version 5.0

Table 13-1 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 13-1 Summary of phased upgrade

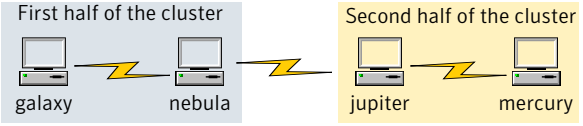
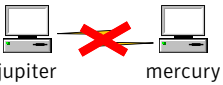
First half of the cluster	Second half of the cluster
SF Oracle RAC cluster before the upgrade:  	
STEP 1: Perform the following pre-upgrade steps: ■ Switch failover applications. ■ Stop all parallel applications. See "Step 1: Performing pre-upgrade tasks on the first half of the cluster" on page 225. **STEP 2**: Upgrade SF Oracle RAC. See "Step 2: Upgrading the first half of the cluster" on page 228.	The second half of the cluster is up and running.

Table 13-1 Summary of phased upgrade *(continued)*

First half of the cluster	Second half of the cluster
The first half of the cluster is not running. 	**STEP 3**: Perform the following pre-upgrade steps: ■ Stop all parallel and failover applications. ■ Stop SF Oracle RAC. See "Step 3: Performing pre-upgrade tasks on the second half of the cluster" on page 229. **The downtime starts now.**
STEP 4: Perform the following post-upgrade steps: ■ Start SF Oracle RAC. ■ Start all applications. See "Step 4: Performing post-upgrade tasks on the first half of the cluster" on page 231. **The downtime ends here.**	The second half of the cluster is not running. 
The first half of the cluster is up and running. 	**STEP 5**: Upgrade SF Oracle RAC. See "Step 5: Upgrading the second half of the cluster" on page 233. **STEP 6**: Perform the following post-upgrade steps: ■ Start SF Oracle RAC. ■ Start all applications. See "Step 6: Performing post-upgrade tasks on the second half of the cluster" on page 234.
The phased upgrade is complete and both the first and the second half of the cluster are running. 	

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, OracleASMTypes.cf, , PrivNIC.cf, MultiPrivNIC.cf, /etc/lltab, /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 \
   /var/tmp/PrivNIC.cf.save
   # cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf \
   /var/tmp/MultiPrivNIC.cf.save
   ```

2. Stop all applications that are not configured under VCS. Use native application commands to stop the application.

3. If you plan to continue using checkpoints 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 5.1 Service Pack 1.

   See "Pre-upgrade tasks for migrating the SFDB repository database" on page 210.

4. Stop the Oracle database:

   - 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:

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

   - If the Oracle RAC instance is managed by VCS:

     ```
     # hagrp -offline oracle_group -sys galaxy
     # hagrp -offline oracle_group -sys nebula
     ```

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:

```
# haconf -makerw
# hagrp -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:

```
$ srvctl modify database -d db-name -y manual
```

6 Unmount the non-system VxFS and CFS file systems that are not managed by VCS.

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

```
# mount -v | grep vxfs

# fuser -cu /mount_point
```

■ Unmount the non-system VxFS or CFS file system:

```
# umount /mount_point
```

7 If you created local VxFS mount points on VxVM volumes and added them to `/etc/fstab`, comment out the mount point entries in the file.

8 Stop the parallel service groups and switch over failover service groups:

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

9 Verify that only ports a, b, d, and o are open:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   79c302 membership 0123
Port b gen   79c307 membership 0123
Port d gen   79c306 membership 0123
Port o gen   79c304 membership 0123
```

10 Perform the following steps only if you are upgrading from HP-UX 11i v2:

- If the cluster-wide attribute “UseFence” is set to SCSI3, then reset the value to NONE in the /etc/VRTSvcs/conf/config/main.cf file.
- On each node, edit the /etc/vxfenmode file to configure I/O fencing in disabled mode.

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

Note: If you upgrade from SF Oracle RAC 4.1 on HP-UX 11iv2, create `/etc/vxfenmode` file and populate it as above.

- On each node, remove the following device files:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
# rm -f /dev/lmx
# rm -f /dev/vcsmm
```

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/lltab` file to prevent LLT from starting automatically when the node starts:

```
$ mv /etc/lltab /etc/lltab.save
```

2. Upgrade the operating system, if required.

See “Upgrading the HP-UX operating system” on page 215.

3. Rename the `/etc/lltab` file to its original name:

```
$ mv /etc/lltab.save /etc/lltab
```

4. 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.

5 Upgrade SF Oracle RAC:

```
# ./installsfrac galaxy nebula
```

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.

6 Change the `/etc/rc.config.d/lltconf` file to prevent LLT from starting automatically after reboot by setting the LLT_START attribute to 0:

```
LLT_START=0
```

7 For phased upgrades from HP-UX 11iv2, enable fencing:

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

8 Uncomment the VxFS mount point entries in the `/etc/fstab` file.

9 Restart the nodes:

```
# shutdown -r now
```

You may see some errors in the system log file when the nodes restart. This is because LLT is disabled. Ignore these messages.

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. Use native application commands to stop the application.

2 If you plan to continue using checkpoints 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 5.1 Service Pack 1.

See "Pre-upgrade tasks for migrating the SFDB repository database" on page 210.

3 Stop the Oracle database:

- 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:

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

- If the Oracle RAC instance is managed by VCS:

```
# hagrp -offline oracle_group -sys jupiter
# hagrp -offline oracle_group -sys mercury
```

Note: The downtime starts now.

4 Unmount the non-system VxFS or CFS file systems that are not managed by VCS.

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

```
# mount -v | grep vxfs

# fuser -cu /mount_point
```

- Unmount the non-system VxFS file system:

```
# umount /mount_point
```

5 If you created local VxFS mount points on VxVM volumes and added them to `/etc/fstab`, comment out the mount point entries in the file.

6 Stop VCS:

```
# hastop -local
```

7 Stop the following SF Oracle RAC modules: Fencing, ODM, VCSMM, VCS, GAB, LMX, and LLT

```
# /opt/VRTS/bin/vcsmmconfig -U
# /sbin/init.d/odm stop
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule odm=unused
# kcmodule vcsmm=unused
# kcmodule vxglm=unused
# kcmodule vxgms=unused
# lmxconfig -U
# kcmodule lmx=unused
# kcmodule gab=unused
# lltconfig -U
# kcmodule llt=unused
```

8 Perform the following steps only if you are upgrading from HP-UX 11i v2:

- If the cluster-wide attribute "UseFence" is set to SCSI3, then reset the value to NONE in the /etc/VRTSvcs/conf/config/main.cf file.
- On each node, edit the /etc/vxfenmode file to configure I/O fencing in disabled mode.

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

Note: If you upgrade from SF Oracle RAC 4.1 on HP-UX 11iv2, create `/etc/vxfenmode` file and populate it as above.

- On each node, remove the following device files:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
# rm -f /dev/lmx
# rm -f /dev/vcsmm
```

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. Change `/etc/rc.config.d/lltconf` to start LLT on the nodes by setting the LLT_START attribute to 1:

   ```
   LLT_START=1
   ```

2. On the first half of the cluster, force GAB to form a cluster.

   ```
   # gabconfig -x
   ```

3. On the first half of the cluster, start SF Oracle RAC:

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

   ```
   # ./installsfrac -start galaxy nebula
   ```

   Verify that the GAB ports a, b, d, o and h appear in the `gabconfig -a` command output.

4. Upgrade VxVM disk group version.

   See "Upgrading VxVM disk group version" on page 262.

5. Upgrade disk layout version.

   See "Upgrading disk layout versions" on page 262.

6. Relink the SF Oracle RAC libraries with Oracle.

   See "Relinking Oracle RAC libraries with the SF Oracle RAC libraries" on page 257.

7. Bring the Oracle database service group online.

   If the Oracle database is managed by VCS:

   ```
   # hagrp -online oracle_group -sys node_name
   ```

   If the Oracle database is not managed by VCS:

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

Note: The downtime ends here.

---

8 On the first half of the cluster, manually mount the VxFS or CFS file systems that are not managed by VCS.

9 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.

See "Upgrading the HP-UX operating system" on page 215.

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

```
$ mv /etc/llttab.save /etc/llttab
```

4 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.

5 On the second half of the cluster, upgrade SF Oracle RAC:

```
# ./installsfrac jupiter mercury
```

6 For phased upgrades from HP-UX 11iv2, enable fencing:

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

7 Uncomment the VxFS mount point entries in the `/etc/fstab` file.

8 Restart the nodes:

When the nodes in the second half of the cluster come up, all the GAB ports a, b, d, o, h, u, v, w and f will be online. All the CFS mount service groups also come online automatically.

```
# shutdown -r now
```

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. Relink the SF Oracle RAC libraries with Oracle.

   See "Relinking Oracle RAC libraries with the SF Oracle RAC libraries" on page 257.

2. Bring the Oracle database service group online.

   If the Oracle database is managed by VCS:

   ```
   # hagrp -online oracle_group -sys node_name
   ```

   If the Oracle database is not managed by VCS:

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

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
     # hagrp -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:

     ```
     $ srvctl modify database -d db-name -y AUTOMATIC
     ```

4. Manually mount the VxFS and CFS file systems that are not managed by VCS.
5. Start all applications that are not managed by VCS. Use native application commands to start the applications.
6. Set or change the product license level, if required.

   See "Setting or changing the product license level" on page 261.

7. Migrate the SFDB repository database.

   See "Post upgrade tasks for migrating the SFDB repository database" on page 263.

8 Verify the cluster.

See "Verifying the cluster" on page 270.

9 If you want to upgrade CP server systems that use VCS or SFHA to 5.1 SP1, make sure that you upgraded all application clusters to version 5.1 SP1. Then, upgrade VCS or SFHA on the CP server systems.

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

Chapter 14

Upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1

This chapter includes the following topics:

- About upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1
- Upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1

About upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1

You can upgrade from earlier versions of the following Storage Foundation products to SF Oracle RAC 5.1 SP1:

- Storage Foundation High Availability
- Storage Foundation Cluster File System

Note: The installer does not support direct upgrade from earlier versions of Storage Foundation products, such as Storage Foundation Cluster File System 5.0, to SF Oracle RAC 5.1 SP1. You must first upgrade to version 5.1 Service Pack 1 of the installed product, then install SF Oracle RAC 5.1 SP1.

Upgrading from Storage Foundation products to SF Oracle RAC 5.1 SP1

Perform the steps in the following procedure to upgrade Storage Foundation products to SF Oracle RAC 5.1 SP1.

To upgrade Storage Foundation products to SF Oracle RAC 5.1 SP1

1. If you are running an earlier version of the product, upgrade to version 5.1 Service Pack 1 of the product.

   For instructions, see the installation guide of the product.

2. Install SF Oracle RAC 5.1 SP1.

   See "About installing SF Oracle RAC " on page 87.

3. When you are prompted to configure SF Oracle RAC, enter **y** at the prompt:

   ```
   Would you like to configure SF Oracle RAC on galaxy? [y,n,q] (n) y
   ```

   The program menu is displayed.

4. Select the option **Configure SF Oracle RAC sub-components**.

   ```
   1)  Configure SF Oracle RAC sub-components
   2)  SF Oracle RAC Installation and Configuration Checks
   3)  Prepare to Install Oracle
   4)  Install Oracle Clusterware/Grid Infrastructure and Database
   5)  Post Oracle Installation Tasks
   6)  Exit SF Oracle RAC Configuration

   Choose option: [1-6,q] (1)
   ```

   If VCS is configured in your environment, the installation program detects the VCS configuration.

   Note: Do not reconfigure VCS when you are prompted by the installation program:

   ```
   Do you want to re-configure VCS? [y,n,q] (n)
   ```

   The installation program creates the VCS configuration file and the `/etc/vcsmmtab` file and starts all processes.

5 Verify that all GAB ports are up and running.

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen    29d01  membership 01
Port b gen    29d0f  membership 01
Port d gen    29d07  membership 01
Port f gen    29d17  membership 01
Port h gen    29d11  membership 01
Port o gen    29d12  membership 01
Port u gen    71520b membership 01
Port v gen    29d13  membership 01
Port w gen    29d15  membership 01
```

6 Restart ODM on all nodes. This will start ODM in clustered mode.

```
# /sbin/init.d/odm stop
# /sbin/init.d/odm start
```

7 If fencing is not configured, configure fencing.

For instructions, see the chapter *Configuring SF Oracle RAC clusters for data integrity* in this document.

8
- If you have neither single-instance Oracle nor Oracle RAC running in your environment, install Oracle RAC.
  For instructions, see the chapter *Installing and configuring Oracle RAC* in this document.
- If you have a single-instance Oracle database in your environment, migrate the database to Oracle RAC.
  For instructions, see the chapter *Migrating from single instance Storage Foundation for Oracle HA to SF Oracle RAC* in this document.

Chapter 15

Migrating from single instance Storage Foundation for Oracle HA to SF Oracle RAC

This chapter includes the following topics:

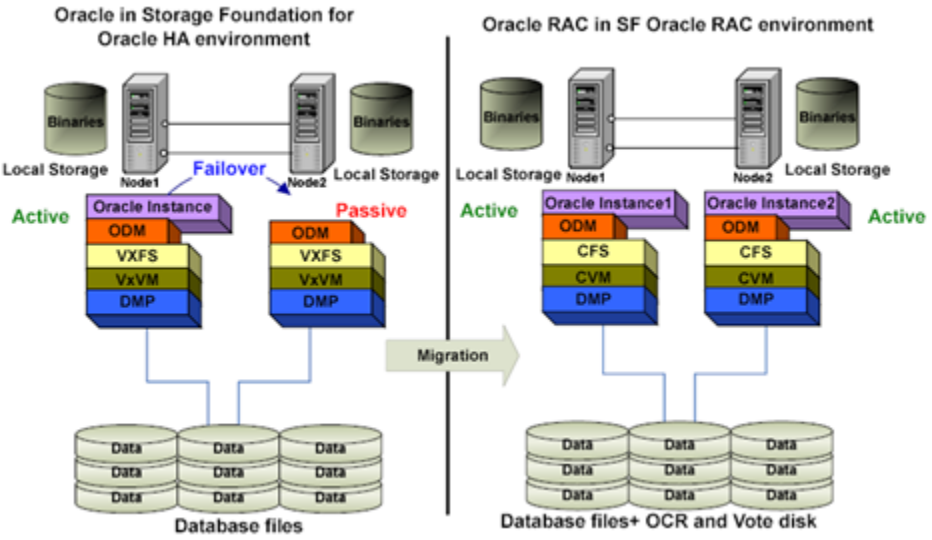
- Migration overview
- Migration requirements
- Before you migrate
- Migrating to SF Oracle RAC 5.1 SP1
- Sample configuration files

Migration overview

This chapter provides instructions for migrating from Veritas Storage Foundation for Oracle High Availability to Veritas Storage Foundation for Oracle RAC (SF Oracle RAC).

Figure 15-1 illustrates the migration from Storage Foundation for Oracle HA to SF Oracle RAC.

Figure 15-1 Migration from Storage Foundation for Oracle HA to SF Oracle RAC



Sample configuration before and after migration

Table 15-1 describes a sample existing configuration in a Storage Foundation for Oracle HA database environment.

Table 15-1 Configuration in a Storage Foundation for Oracle HA database environment

Host name	Instance name	Database name	Oracle home	Database file storage
galaxy	dbrac	dbrac	/u01/app/oracle/product/*release*/dbhome_1 where *release* is 10.2.0 or 11.1.0 depending on the Oracle RAC version	Shared storage using VxFS
nebula	dbrac	dbrac	/u01/app/oracle/product/*release*/dbhome_1 where *release* is 10.2.0 or 11.1.0 depending on the Oracle RAC version	Shared storage using VxFS

Table 15-2 describes a sample configuration in an SF Oracle RAC database environment.

Table 15-2 Configuration in an SF Oracle RAC environment

Host name	Instance name	Database name	Oracle home	Database file storage	OCR and voting disk
galaxy	dbrac1	dbrac	/u01/app/oracle/product/*release*/dbhome_1 where *release* is 10.2.0, 11.1.0, or 11.2.0 depending on the Oracle RAC version	Shared storage using CFS	Reside on CVM or CFS
nebula	dbrac2	dbrac	/u01/app/oracle/product/*release*/dbhome_1 where *release* is 10.2.0, 11.1.0, or 11.2.0 depending on the Oracle RAC version	Shared storage using CFS	Reside on CVM or CFS

Migration requirements

Make sure that you meet the following requirements before migrating to SF Oracle RAC:

- Storage Foundation for Oracle HA version 5.1 Service Pack 1 is installed on the systems.
- Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 is installed on the systems.

Before you migrate

Before you migrate to SF Oracle RAC, complete the following tasks:

- Set up the single instance Storage Foundation for Oracle database with the following configuration:
  - Storage Foundation for Oracle HA installed on all nodes
  - Oracle binaries installed on each node
  - Oracle database created on shared storage using Veritas File System (VxFS)
- Back up the existing database before the migration.

Migrating to SF Oracle RAC 5.1 SP1

Perform the following steps to migrate from Storage Foundation for Oracle HA to SF Oracle RAC.

1. Migrate Storage Foundation for Oracle HA to SF Oracle RAC.

   See "Migrating Storage Foundation for Oracle HA to SF Oracle RAC" on page 244.

2. Migrate single instance Oracle database to Oracle RAC database.

   See "Migrating a single instance Oracle database to Oracle RAC database" on page 245.

3. Complete the post-migration tasks.

   See "Completing post-migration tasks" on page 249.

Migrating Storage Foundation for Oracle HA to SF Oracle RAC

Perform the following steps to migrate from Storage Foundation for Oracle HA to SF Oracle RAC.

To migrate from Storage Foundation for Oracle HA to SF Oracle RAC

1 Log in as a superuser.

2 Back up the existing Storage Foundation for Oracle database HA resource configuration:

```
# cp -rp /etc/VRTSvcs/conf/config config.old
```

3 Take the database service groups offline:

```
# hagrp -offline group_name -any
```

4 If the VxFS file systems are not managed by VCS, unmount them :

```
# umount mount_point
```

5 Stop all the other VCS service groups.

To view the current state of the service groups:

```
# hagrp -state
```

To stop each group:

```
# hagrp -offline servicegroup -sys node_name
```

6 Freeze the VCS service groups:

```
# haconf -makerw
# hagrp -freeze servicegroup -persistent
# haconf -dump -makero
```

7 Stop VCS on all nodes:

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

8 Install and configure SF Oracle RAC.

For information on installing and configuring SF Oracle RAC, see *Section 2: Installation and configuration of SF Oracle RAC* in this guide.

9 Unfreeze the VCS service groups:

```
# haconf -makerw
# hagrp -unfreeze servicegroup -persistent
# haconf -dump -makero
```

Migrating a single instance Oracle database to Oracle RAC database

Complete the steps in the following procedure for migrating a single instance Oracle database to the Oracle RAC database.

To migrate a single instance Oracle database to Oracle RAC database

1 Install Oracle Clusterware.

For information on installing Oracle Clusterware, see *Section 4: Installation and upgrade of Oracle RAC* in this guide.

2 Import the single instance Storage Foundation for Oracle database HA storage disk group in shared mode:

```
# vxdg –s import oradatadg
```

where oradatadg is a disk group in the Storage Foundation for Oracle database HA environment.

In an Oracle RAC environment, all instances concurrently access a single database. Thus, all datafiles, control files, SPFILE, redo log files and archive log files must reside on shared storage.

3 Mount the file system in cluster mode on all nodes:

```
# mount -F vxfs -o cluster,largefiles\
/dev/vx/dsk/oradatadg/oradatavol /oradata
```

where oradata is a file system in the Storage Foundation for Oracle database HA environment.

4 Before relinking the Oracle database binaries with the Veritas libraries run the following commands:

On PA-RISC systems:

```
# rm $ORACLE_HOME/lib/libskgxn2.sl
# ln -s /opt/nmapi/nmapi2/lib/pa20_64/libnmapi2.sl \
$ORACLE_HOME/lib/libskgxn2.sl
```

On Itanium systems:

```
# rm $ORACLE_HOME/lib/libskgxn2.so
# ln -s /opt/nmapi/nmapi2/lib/hpux64/libnmapi2.so \
$ORACLE_HOME/lib/libskgxn2.so
```

5 Relink Oracle binaries with Veritas libraries.

See "Relinking Oracle RAC libraries with the SF Oracle RAC libraries" on page 257.

6 Start the database as an Oracle user from any one of the nodes in the cluster using SQLPLUS:

```
$ export ORACLE_SID=dbrac
$ export ORACLE_HOME=/oracle/db11g
$ /oracle/db11g/bin/sqlplus "/as sysdba"
```

where dbrac is a database in the Storage Foundation for Oracle database HA environment.

7 Add redo logs. Each instance requires its own redo thread. The following example assumes a two node configuration, with galaxy and nebula as the nodes in the cluster. The existing redo thread will be used by galaxy.

To add a new redo thread, log on to nebula as Oracle user and run the following commands:

```
SQL> alter database add logfile thread 2
    group 4 ('/oradata/dbrac/redo04.log') size 50M REUSE;
Database altered

SQL> alter database add logfile thread 2
   group 5 ('/oradata/dbrac/redo05.log') size 50M REUSE;
Database altered.

SQL> alter database add logfile thread 2
   group 6 ('/oradata/dbrac/redo06.log') size 50M REUSE;
Database altered
```

8 Enable redo log thread.While enabling, it may be designated as a public thread or a private thread:

```
SQL> ALTER DATABASE ENABLE PUBLIC THREAD 2;
OR
SQL> ALTER DATABASE ENABLE PRIVATE THREAD 2;
```

9 Add UNDO tablespaces for each additional instance:

```
SQL> create undo tablespace UNDOTBS2 datafile\
'/oradata/dbrac/undotbs02.dbf' size 500M autoextend on;
```

10 Create the cluster views needed for Oracle RAC:

```
SQL> @?/rdbms/admin/catclust
```

11 If you are using an SPFILE, create a PFILE from it:

```
SQL> create pfile='/tmp/initORA.ora' from spfile
```

12 Edit the Oracle initialization parameter file `/tmp/initORA.ora` to include cluster parameters:

```
*.cluster_database_instances=2
*.cluster_database=TRUE
dbrac1.instance_name=dbrac1
dbrac2.instance_name=dbrac2
dbrac1.instance_number=1
dbrac2.instance_number=2
dbrac1.thread=1
dbrac2.thread=2
dbrac1.undo_tablespace='UNDOTBS1'
dbrac2.undo_tablespace='UNDOTBS2'
dbrac1.local_listener= 'LISTENER_GALAXY'
dbrac2.local_listener= 'LISTENER_NEBULA'
dbrac1.remote_listener= 'LISTENERS_DBRAC'
dbrac2.remote_listener= 'LISTENERS_DBRAC'
```

13 Start the Oracle initialization parameter file:

```
SQL> connect / as sysdba
SQL> shutdown immediate
SQL> startup pfile='/tmp/initORA.ora'
```

14 If the database starts successfully using the Oracle initialization parameter file, create an spfile in a shared location:

```
SQL> create spfile='sharedlocation/spfiledbrac.ora'\
 from pfile='/tmp/initORA.ora'
```

15 On each node create a link in $ORACLE_HOME/dbs to the shared spfile directory.

For galaxy:

```
cd $ORACLE_HOME/dbs
ln -s sharedlocation/spfiledbrac.ora spfiledbrac1.ora
```

For nebula:

```
cd $ORACLE_HOME/dbs
ln -s sharedlocation/spfiledbrac.ora spfiledbrac2.ora
```

16 Add the database and instances to the cluster registry:

```
# srvctl add database -d dbrac -o $ORACLE_HOME
# srvctl add instance -d dbrac -i dbrac1 -n galaxy
# srvctl add instance -d dbrac -i dbrac2 -n nebula
```

17 Stop and start the database:

```
$ srvctl stop database -d dbrac
$ srvctl start database -d dbrac
```

18 For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

Configure Oracle listener using Oracle Net Configuration Assistant (NETCA).

Note: The NETCA utility requires xterm capability.

```
$ export DISPLAY=localhost:0.0
$ ORACLE_HOME/bin/netca
```

The NETCA utility starts Oracle listener on both nodes.

This completes the migration of the single-instance Oracle database to an Oracle RAC configuration.

Completing post-migration tasks

Perform the steps in the following procedure to complete the migration process. The examples in the procedures assume a two-node SF Oracle RAC cluster with the nodes galaxy and nebula.

To complete the post-migration tasks:

1 For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

Copy the file `tnsnames.ora` to the directory `$ORACLE_HOME/network/admin`on all nodes. A sample `tnsnames.ora` file is given below:

```
DBRAC =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = galaxy-vip)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = nebula-vip)(PORT = 1521))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = dbrac)
    )
  )
DBRAC1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = galaxy-vip)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = dbrac)
      (INSTANCE_NAME = dbrac1)
    )
  )
DBRAC2 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = nebula-vip)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = dbrac)
      (INSTANCE_NAME = dbrac2)
    )
  )
LISTENERS_DBRAC =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = galaxy-vip)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = nebula-vip)(PORT = 1521))
        )
```

For Oracle RAC 11g Release 2, see the Oracle documentation to update the `tnsnames.ora` file.

2 Optional: Add services to a database and assign them to instances. You can create services manually or by using the Database Configuration Assistant (DBCA) utility.

In Real Application Clusters (RAC), a service can span one or more instances and facilitate real workload balancing based on real transaction performance. You can control the instances in your cluster that are allocated to different services at different times.

To create the services manually:

```
# srvctl add service -d dbrac -s ORA_TAF -r dbrac1, dbrac2
```

3 Configure the CSSD, PrivNIC or MultiPrivNIC and Oracle resource agents in the VCS configuration file.

For more information see *Section 4: Installation and upgrade of Oracle RAC* in this guide.

4 Depending on your deployment needs you may perform the following optional tasks:

- Update the application (database client) configuration to connect to Oracle RAC database (if required) and to take advantage of Oracle RAC features like load balancing and scalability.
- Update the VCS configuration file for any additional resources, which were present in the VCS configuration prior to the migration process.

Migrating Storage Foundation for Databases (SFDB) objects from single instance Oracle to Oracle RAC

After migrating from Storage Foundation HA to Storage Foundation for Oracle RAC, the Storage Foundation for Databases (SFDB) objects created in a single instance Oracle environment will not be available in the Oracle RAC environment.

To re-create the SFDB repository

1 After migrating from Storage Foundation HA to Storage Foundation for Oracle RAC, run `dbed_update`.

2 Re-create the SFDB objects that existed in the Storage Foundation HA environment. They will now be supported for SFRAC.

For information on configuring SFDB objects, see the *Storage Foundation: Storage and Availability Management for Oracle Databases* guide.

Sample configuration files

This section illustrates sample configurations for the following files:

VCS configuration file	See "VCS configuration file for Storage Foundation for Oracle HA" on page 252.
Oracle initialization parameter file	See "Oracle initialization parameter file for Storage Foundation for Oracle HA" on page 253.
tnsnames.ora	See "tnsnames.ora for Storage Foundation for Oracle HA" on page 254.
listener.ora	See "listener.ora for Storage Foundation for Oracle HA" on page 254.

VCS configuration file for Storage Foundation for Oracle HA

The sample VCS configuration file for Storage Foundation for Oracle HA is as follows:

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

cluster tyur (
 UserNames = { admin = bQRjQLqNRmRRpZRlQO }
 Administrators = { admin }
 )

system galaxy (
 )

system nebula (
 )

group sfora (
 SystemList = { galaxy = 0, nebula = 1 }
 AutoStartList = { galaxy, nebula }
 )

 DiskGroup oradatadg (
  Critical = 0
```

```
 DiskGroup = oradatadg
 )

Mount oradatamnt (
 Critical = 0
 MountPoint = "/oradata"
 BlockDevice = "/dev/vx/dsk/oradatadg/datavol"
 FSType = vxfs
 FsckOpt = "-y"
 )

Oracle oradb (
 Critical = 0
 Sid = dbrac
 Owner = oracle
 Home = "/oracle/db11g"
 )
oradatamnt requires oradatadg
oradb requires oradatamnt
```

Oracle initialization parameter file for Storage Foundation for Oracle HA

The sample Oracle initialization parameter file for Storage Foundation for Oracle HA is as follows:

```
dbrac.__db_cache_size=1375731712
dbrac.__java_pool_size=16777216
dbrac.__large_pool_size=16777216
dbrac.__oracle_base='/oracle/db11g'\
#ORACLE_BASE set from environment
dbrac.__pga_aggregate_target=1224736768
dbrac.__sga_target=1811939328
dbrac.__shared_io_pool_size=0
dbrac.__shared_pool_size=385875968
dbrac.__streams_pool_size=0
*.audit_file_dest='/oracle/db11g/admin/dbrac/adump'
*.audit_trail='none'
*.compatible='11.1.0.0.0'
*.control_files='/oradata/dbrac/control01.ctl',
'/oradata/dbrac/control02.ctl',
'/oradata/dbrac/control03.ctl'
*.db_block_size=8192
```

```
*.db_domain=''
*.db_name='dbrac'
*.diagnostic_dest='/oracle/db11g'
*.dispatchers='(PROTOCOL=TCP) (SERVICE=dbracXDB)'
*.log_archive_dest_1='LOCATION=/oradata/archive'
*.log_archive_format='%t_%s_%r.dbf'
*.memory_target=3036676096
*.open_cursors=300
*.processes=150
*.remote_login_passwordfile='EXCLUSIVE'
*.undo_tablespace='UNDOTBS1'
```

tnsnames.ora for Storage Foundation for Oracle HA

The sample tnsnames.ora for Storage Foundation for Oracle HA is as follows:

```
Host : galaxy
DBRAC =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = galaxy)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = dbrac)
    )
  )

Host : Nebula
DBRAC =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = nebula)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = dbrac)
    )
  )
```

listener.ora for Storage Foundation for Oracle HA

The sample listener.ora for Storage Foundation for Oracle HA is as follows:

```
Host : galaxy


LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = galaxy)(PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )

Host : Nebula

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = nebula)(PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )
```

Chapter 16

Performing post-upgrade tasks

This chapter includes the following topics:

- Relinking Oracle RAC libraries with the SF Oracle RAC libraries
- Setting or changing the product license level
- Changing permissions for Storage Foundation for Databases
- Upgrading disk layout versions
- Upgrading VxVM disk group version
- Post upgrade tasks for migrating the SFDB repository database
- Configuring Powerfail Timeout after upgrade
- Converting from QuickLog to Multi-Volume support
- Verifying the cluster

Relinking Oracle RAC libraries with the SF Oracle RAC libraries

You must relink the Oracle RAC libraries with the SF Oracle RAC libraries after upgrading SF Oracle RAC.

The steps vary depending on the version of Oracle RAC in use before the upgrade:

- If you upgraded from an SF Oracle RAC version running Oracle RAC 10g Release 2 or Oracle RAC 11g:

See "To relink Oracle RAC 10g Release 2 or Oracle RAC 11g using the installer" on page 258.

- If you upgraded from an SF Oracle RAC version running Oracle RAC 9i or Oracle RAC 10g Release 1 or if you want to relink the libraries manually for later versions of Oracle RAC:
  See "To relink the Oracle RAC libraries with SF Oracle RAC libraries manually" on page 259.

Note: You must upgrade the database to a supported version after you complete the post-upgrade tasks.

To relink Oracle RAC 10g Release 2 or Oracle RAC 11g using the installer

1 Run the `installsfrac` installer:

```
# cd /opt/VRTS/install
# ./installsfrac -configure galaxy nebula
```

2 Enter **5** to select the option **Post Oracle Installation Tasks**.

```
1)  Configure SF Oracle RAC sub-components
2)  SF Oracle RAC Installation and Configuration Checks
3)  Prepare to Install Oracle
4)  Install Oracle Clusterware/Grid Infrastructure and Database
5)  Post Oracle Installation Tasks
6)  Exit SF Oracle RAC Configuration
Choose option: [1-6,q] (1) 5
```

3 Select the option **Relink Oracle Database Binary**.

```
1)  Configure CSSD agent
2)  Relink Oracle Database Binary
3)  Exit SF Oracle RAC Configuration
b)  Back to previous menu
Choose option: [1-3,b,q] (1) 2
```

4 Provide the following information:

```
Enter Oracle UNIX user name: [b] (oracle)
Enter Oracle UNIX group name: [b] (oinstall)
Enter absolute path of Oracle Clusterware/Grid Infrastructure
Home directory: [b]
Enter absolute path of Oracle Database Home directory: [b]
```

The installer detects the Oracle version.

5 Enter **y** to proceed with relinking.

```
Do you want to continue? [y,n,q] (y)
```

Perform the steps in the following procedure if you upgraded nodes running Oracle RAC 9i or Oracle RAC 10g Release 1 or if you want to relink the libraries manually.

To relink the Oracle RAC libraries with SF Oracle RAC libraries manually

1 On each node, shut down the Oracle service group:

```
# hagrp -offline oracle_grp -sys system_name
```

2 On each node, run the following command as the oracle user to link Oracle with the Veritas IPC, VCSMM, and ODM libraries:

```
$ /opt/VRTSvcs/rac/bin/linkrac oracle_version
```

Replace oracle_version with one of the following values depending on the version you installed:

- 9i (for Oracle RAC 9i)
- 10gR1 (for Oracle RAC 10g Release 1)
- 10gR2 (for Oracle RAC 10g Release 2)
- 11gR1 (for Oracle RAC 11g Release 1)
- 11gR2 (for Oracle RAC 11g Release 2)

Note: If the Oracle binaries are on a cluster file system, perform this step on only one node. If the Oracle binaries are on a local file system of each cluster node, run the command to link Oracle with Vertitas libraries on each cluster node.

If your system uses a bundled C compiler or a compiler other than the ANSI C compiler, you can safely ignore such warnings as:

```
(Bundled) cc: warning 922: "+Oshortdata=8" is unsupported in the
bundled compiler, ignored.
```

Refer to Oracle Metalink Document ID 66442.1 for more information.

Search on: 66442.1 FAQ about C Compiler Issues on HP-UX.

3 On each node, start the Oracle service group:

```
# hagrp -online oracle_grp -sys system_name
```

4 After starting the Oracle instance, confirm Oracle uses the Veritas libraries. Examine the Oracle alert file, `alert_$ORACLE_SID.log`, for the following lines:

```
Oracle instance running with ODM: VERITAS 5.0 ODM Library,
Version 1.0
cluster interconnect IPC version:VERITAS IPC
'5.0.31.5' 09:13:36 Jun 25 2009
```

Note: If Oracle binaries are on a local file system of each cluster node, examine the Oracle alert file on each of the cluster nodes.

If you see the following message in the `alert_$ORACLE_SID.log` file

```
cluster interconnect IPC version string is not available
Oracle interface version information 2.4
cluster IPC library version information 2.2
```

Perform the following steps:

- Stop the database on all the nodes (for instances under VCS control):

  ```
  # hagrp -offline oracle_grp -sys system_name
  ```

  Stop the database on all the nodes (for instances not under VCS control):

  ```
  # srvctl stop database -d database_name
  ```

- For Oracle RAC 9i/Oracle RAC 10g Release 1: Export the IPC_LIB_PATH variable:
  On HP-UX (IA) for Oracle RAC 9i:

  ```
  $ export IPC_LIB_PATH=/opt/VRTSvcs/rac/lib/hpux64/\
  libskgxp<oracleversion>_ver24_64.sl
  ```

  On HP-UX (PA) for Oracle RAC 9i:

```
$ export IPC_LIB_PATH=/opt/VRTSvcs/rac/lib/pa20_64/\
libskgxp<oracleversion>_ver24_64.sl
```

On HP-UX (IA) for Oracle RAC 10g Release 1:

```
$ export IPC_LIB_PATH=/opt/VRTSvcs/rac/lib/hpux64/\
libskgxp<oracleversion>_ver25_64.sl
```

On HP-UX (PA) for Oracle RAC 10g Release 1:

```
$ export IPC_LIB_PATH=/opt/VRTSvcs/rac/lib/pa20_64/\
libskgxp<oracleversion>_ver25_64.sl
```

where *<oracleversion>* is 9 (for Oracle RAC 9i) or 10 (for Oracle RAC 10g)

- Repeat step 2 and step 3.

Setting or changing the product license level

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

After you upgrade, perform one of the following steps:

- Obtain a valid license key and run the `vxlicinst` command to add it to your system.
- Use the `vxkeyless` command to update the license keys to the keyless license model.

For more information and instructions, see the chapter *Licensing SF Oracle RAC*.

Changing permissions for Storage Foundation for Databases

Change the permissions on the `/opt/VRTSdbed` directory and reset owner and group settings as appropriate. This is necessary to ensure that the Veritas Storage Foundation for Oracle commands work correctly.

To chang permissions for Storage Foundation for Databases

1 Change permissions for the `/opt/VRTSdbed` directory:

```
# chmod 550 /opt/VRTSdbed
```

2 Reset the owner to user "oracle" and the group to "dba":

```
# chown oracle:dba /opt/VRTSdbed
```

Upgrading disk layout versions

In this release, you can create and mount only file systems with disk layout Version 6, Version 7, and Version 8. No prior versions can be created or mounted.

Use the `vxfsconvert` or `vxupgrade` utilities to upgrade older disk layout versions to disk layout Version 8.

See the `vxfsconvert` or `vxupgrade` man pages.

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

Upgrading 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 160.

Run the following command on the master node to upgrade the disk group version:

```
# vxdg -T 160 upgrade diskgroup_name
```

The default Cluster Volume Manager protocol version is 100 and does not need to be upgraded.

Run the following command to verify the CVM protocol version:

```
# /opt/VRTS/bin/vxdctl protocolversion
```

If the protocol version is not 100, run the following command to upgrade the version:

```
# /opt/VRTS/bin/vxdctl upgrade
```

Post upgrade tasks for migrating the SFDB repository database

To continue using the checkpoints or tering policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, you must perform one of the following procedures after upgrading SF Oracle RAC to 5.1 Service Pack 1:

- After you upgrade from 5.0.x and before you migrate SFDB:
  See "After upgrading from 5.0.x and before migrating SFDB" on page 268.
- Migrating from a 5.0 SFDB repository database
- Migrating from a 4.x SFDB repository database
- Upgrading without migrating existing Database Storage Checkpoints and SmartTier parameters

Migrating from a 5.0 repository database to 5.1 Service Pack 1

Perform the following on one node only.

To migrate from a 5.0 repository database to 5.1 Service Pack 1

1. When upgrading SFDB tools from the previous release in an HP Service Guard environment, first verify that the `cmviewcl` command can be executed by a non-root user.
2. Rename the startup script NO_S*vxdbms3 to S*vxdbms3.

   See "After upgrading from 5.0.x and before migrating SFDB" on page 268.
3. As root, set the Oracle group permission for various directories used by Oracle on one node:

   ```
   # /opt/VRTSdbed/common/bin/sfua_db_config
   ```
4. As root, dump out the old Sybase ASA repository. If you are using SFHA or SF Oracle RAC, you only need to this on one node.

   ```
   # /opt/VRTSdbed/migrate/sfua_rept_migrate
   ```
5. On the same node that you ran `sfua_rept_migrate` run the following command as Oracle user. For each Oracle instance, migrate the old repository data to the SQLite repository.

   ```
   $ dbed_update -S $ORACLE_SID -H $ORACLE_HOME
   ```

6 By default, the repository is created on the filesystem which contains the Oracle SYSTEM tablespace. If you need an alternative repository path, first verify the following requirements:

- Repository path has to be a directory writable by Oracle user.
- The repository must be accessible by all nodes. You can put it in a CFS file system, or put it in a resource group under VCS control so it can be failed over together with the Oracle database.
- The update commands will not be able to verify accessibility of the repository path and will fail if you have not set up the path correctly.

To create an alternate repository path:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME -R \
Alternate_path
```

7 If you are using Database Flashsnap for off-host processing, and if you have a repository on the secondary host that you need to migrate: perform the previous steps on the secondary host.

If you do not have a repository that you need to migrate from 5.0:

As root, set the Oracle group permission for various directories used by Oracle:

```
# /opt/VRTSdbed/common/bin/sfua_db_config
```

8 On the primary host, edit your snapplans to remove the "SNAPSHOT_DG=SNAP_*" parameter and add “SNAPSHOT_DG_PREFIX=SNAP_*". The parameter can be any PREFIX value and not necessarily "SNAP_*".

For example:

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.pdx.symantec.com
PRIMARY_DG=system1_data
SNAPSHOT_DG=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.pdx.symantec.com
PRIMARY_DG=judge_data
SNAPSHOT_DG_PREFIX=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

9 On the primary host, revalidate your snapshots using the following command:

```
$ /opt/VRTS/bin/dbed_vmchecksnap -S $ORACLE_SID \
 -H $ORACLE_HOME -f SNAPPLAN -o validate
```

This completes the migration of the repository for Database Storage Checkpoints and Database Tiered Storage parameters.

To begin using the Storage Foundation for Databases (SFDB) tools:

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

Migrating from a 4.x repository database to 5.1 Service Pack 1

If you are upgrading Database Storage Checkpoints or Database FlashSnap information created in SF Oracle RAC 4.x, you can migrate to `/var/vx/vxdba` to save space under the root partition. Migrating to `/var/vx/vxdba` is optional. However, if you do not perform this migration, you cannot remove any file or directory from `/etc/vx/vxdba` to ensure proper operation.

To migrate from /etc/vx/vxdba to /var/vx/vxdba

1 Copy the `/etc/vx/vxdba` directory and contents to `/var/vx/vxdba`.

```
# cp -rp /etc/vx/vxdba /var/vx/vxdba
```

2 Remove /etc/vx/vxdba.

```
# rm -rf /etc/vx/vxdba
```

3 Link the two directories.

```
# ln -s /var/vx/vxdba /etc/vx/vxdba
```

To upgrade the SFDB tools from 4.x to 5.1 Service Pack 1

1
```
# /opt/VRTSdbed/common/bin/sfua_db_config
```

2 On one node, as Oracle user, for each Oracle instance, migrate the old repository data to SQLite repository.

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME
```

3 By default, the repository is created on the filesystem which contains the Oracle SYSTEM tablespace. If you need an alternative repository path, first verify the following requirements:

- The SFDB repository path has to be a directory writable by Oracle user.

- The repository must be accessible by all nodes. You can put it in a resource group under VCS control so it can be failed over together with the Oracle database.
- The update commands will not be able to verify accessibility of the repository path and will fail if you have not set up the path correctly.

To create an alternate repository path:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME -R \
Alternate_path
```

4 On the primary host, edit your snapplans to remove the "SNAPSHOT_DG=SNAP_*" parameter and add “SNAPSHOT_DG_PREFIX=SNAP_*". The parameter can be any PREFIX value and not necessarily "SNAP_*".

For example:

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=4.0
PRIMARY_HOST=host1
SECONDARY_HOST=host1
PRIMARY_DG=PRODdg
SNAPSHOT_DG=SNAP_PRODdg
ORACLE_SID=PROD
ARCHIVELOG_DEST=/prod_ar
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
```

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=4.0
PRIMARY_HOST=host1
SECONDARY_HOST=host1
PRIMARY_DG=PRODdg
SNAPSHOT_DG_PREFIX=SNAP_PRODdg
ORACLE_SID=PROD
ARCHIVELOG_DEST=/prod_ar
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
```

5 If you are using Database Flashsnap for off-host processing, and if you have a repository on the secondary host that you need to migrate: perform steps 1-4 on the secondary host.

If you do not have a repository that you need to migrate from 4.x:

As root, set the Oracle group permission for various directories used by Oracle on one node:

```
# /opt/VRTSdbed/common/bin/sfua_db_config
```

6 On the primary host, revalidate your snapshots using the following command:

```
$ /opt/VRTS/bin/dbed_vmchecksnap -S $ORACLE_SID \
 -H $ORACLE_HOME -f SNAPPLAN -o validate
```

This completes the migration of the SFDB repository.

To begin using the Storage Foundation for Databases (SFDB) tools:

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

After upgrading from 5.0.x and before migrating SFDB

When upgrading from SF Oracle RAC version 5.0 or 5.0.1 to SF Oracle RAC 5.1 Service Pack 1 the S*vxdbms3 startup script is renamed to NO_S*vxdbms3. The S*vxdbms3 startup script is required by `sfua_rept_migrate`. Thus when `sfua_rept_migrate` is run, it is unable to find the S*vxdbms3 startup script and gives the error message:

```
/sbin/rc3.d/S*vxdbms3 not found
SFORA sfua_rept_migrate ERROR V-81-3558 File:  is missing.
SFORA sfua_rept_migrate ERROR V-81-9160 Failed to mount repository.
```

To prevent S*vxdbms3 startup script error

- Rename the startup script NO_S*vxdbms3 to S*vxdbms3.

When upgrading SFDB tools from the previous release in an HP Service Guard environment, first verify that the `cmviewcl` command can be executed by a non-root user. This permission change must be done before executing SFDB upgrade commands.

Configuring Powerfail Timeout after upgrade

When you install SF Oracle RAC, SF Oracle RAC configures Powerfail Timeout (PFTO) using tunable parameters. Starting with SF Oracle RAC 5.0.1, the Powerfail Timeout (PFTO) has the following default values:

- disabled for devices using the HP-UX native multi-pathing
- enabled for devices using DMP

After installation, you can override the defaults, if required. You can explicitly enable or disable PFTO for native multi-pathing devices and DMP devices.

When you upgrade from SF Oracle RAC release 5.0 or earlier, SF Oracle RAC does not preserve any user-defined PFTO values. After the upgrade, the PFTO default values apply to all devices. If you want to use the device settings from the previous release, you must set the desired value explicitly. For example, in an SF Oracle RAC 5.0 installation, you have set the PFTO state to enabled for a native multi-pathing device. After you upgrade from SF Oracle RAC 5.0 to SF Oracle RAC 5.1SP1, the native device is set to the default value, which is disabled. In order to use PFTO, you must explicitly enable the PFTO on that device.

When you upgrade from SF Oracle RAC release 5.0.1 to a higher version, SF Oracle RAC preserves the PFTO state for the devices. After the upgrade, the PFTO values are set to the same values that the device had before the upgrade. For example, in an SF Oracle RAC 5.0.1 installation, you have set the PFTO state to enabled for a native multi-pathing device. After you upgrade from SF Oracle RAC 5.0.1 to SF Oracle RAC 5.1SP1, the native device is set to enabled.

For more information about controlling Powerfail Timeout, see the *Veritas Volume Manager Administrator's Guide*.

Converting from QuickLog to Multi-Volume support

The 4.1 release of the Veritas File System is the last major release to support QuickLog. The Version 6 or Version 7 disk layout does not support QuickLog. The functionality provided by the Veritas Multi-Volume Support (MVS) feature replaces most of the functionality provided by QuickLog.

The following procedure describes how to convert from QuickLog to MVS. Unlike QuickLog, which allowed logging of up to 31 VxFS file systems to one device, MVS allows intent logging of only one file system per device. Therefore, the following procedure must be performed for each file system that is logged to a QuickLog device if Version 6 or Version 7 disk layout is used.

The QuickLog device did not need to be related to the file system. For MVS, the log volume and the file system volume must be in the same disk group.

To convert Quicklog to MVS

1. Select a QuickLog-enabled file system to convert to MVS and unmount it.

   ```
   # umount myfs
   ```

2. Detach one of the QuickLog volumes from the QuickLog device that the file system had been using. This volume will be used as the new intent log volume for the file system.

   ```
   # qlogdetach -g diskgroup log_vol
   ```

3. Create the volume set.

   ```
   # vxvset make myvset myfs_volume
   ```

4. Mount the volume set.

   ```
   # mount -F vxfs /dev/vx/dsk/rootdg/myvset /mnt1
   ```

5. Upgrade the volume set's file system to Version 6 or Version 7 disk layout.

   For example:

   ```
   # vxupgrade -n 6 /mnt1
   ```

6. Add the log volume from step 2 to the volume set.

   ```
   # vxvset addvol myvset log_vol
   ```

7. Add the log volume to the file system. The size of the volume must be specified.

   ```
   # fsvoladm add /mnt1 log_vol 50m
   ```

8. Move the log to the new volume.

   ```
   # fsadm -o logdev=log_vol,logsize=16m /mnt1
   ```

Verifying the cluster

The installer performs the following checks on each node during the process:

- Verifies that SF Oracle RAC is installed.
- Verifies whether the Oracle process daemon (oprocd) is running or not.

- If Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1 is installed, verifies that LLT and Oracle Clusterware uses the same node IDs for each node in the cluster.
- Verifies that the Veritas libraries (VCS IPC, ODM, and VCSMM) are linked with the Oracle RAC libraries. The VCS IPC check is skipped if Oracle RAC 11g is installed.
- Verifies whether the tunables for LLT/LMX/VCSMM tunables are set correctly.
- Verifies that the CSSD resource is configured under the CVM service group.
- Verifies whether the specified Oracle user has read permissions on the /etc/llttab and /etc/llthosts files.
- Verifies that LLT and Oracle Clusterware/Grid Infrastructure have the same view of the number of nodes in the cluster.
- Verifies that the Oracle RAC database version is the same on all nodes in the cluster. The check fails if the version or patchset information varies across nodes.

For information on resolving issues that you may encounter during the checks, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*, Chapter: Troubleshooting SF Oracle RAC, Section: Troubleshooting installation and configuration check failures.

The installer skips the following checks when LLT is configured over UDP:

- LLT links' full duplex setting
- LLT link jumbo frame setting (MTU)
- LLT links' cross connection
- LLT links' speed and auto negotiation settings

Run the SF Oracle RAC installer to verify the functional health of the cluster.

To verify the cluster

1 Start the SF Oracle RAC installer:

```
# cd /opt/VRTS/install

# ./installsfrac -configure galaxy nebula
```

2 Select the option **SF Oracle RAC Installation and Configuration Checks**.

```
1)  Configure SF Oracle RAC sub-components
2)  SF Oracle RAC Installation and Configuration Checks
3)  Prepare to Install Oracle
4)  Install Oracle Clusterware/Grid Infrastructure and Database
5)  Post Oracle Installation Tasks
6)  Exit SF Oracle RAC Configuration
Choose option: [1-6,q] (1) 2
```

3 Enter **y** to confirm that Oracle RAC is installed on the nodes.

4 Enter the full path of the Oracle Clusterware/Grid Infrastructure home directory.

Note: The installer tries to discover the location of the Oracle Clusterware/Grid Infrastructure home directory from the Oracle inventory. If the installer discovers the information, you are not prompted for this information.

The installer verifies the path information and re-prompts if the path is incorrect.

5 Enter the full path of the Oracle RAC database home directory.

Note: The installer tries to discover the location of the Oracle RAC database home directory from the Oracle inventory. If the installer discovers the information, you are not prompted for this information.

The installer verifies the path information.

6 Enter the Oracle user name.

The installer displays the location of the temporary log file and starts the verification process.

Section 4

Installation and upgrade of Oracle RAC

- Chapter 17. Before installing Oracle RAC
- Chapter 18. Installing Oracle RAC
- Chapter 19. Performing Oracle RAC post-installation tasks
- Chapter 20. Upgrading Oracle RAC

Chapter 17

Before installing Oracle RAC

This chapter includes the following topics:

- About preparing to install Oracle RAC
- Preparing to install Oracle RAC using the SF Oracle RAC installer or manually

About preparing to install Oracle RAC

Use one of the following ways to perform the pre-installation tasks:

SF Oracle RAC installer	The SF Oracle RAC installer provides a menu-driven command line interface to step you through the pre-installation tasks. **Note:** Some of the pre-installation steps are not supported by the SF Oracle RAC installer and must be done manually as described in the manual procedures.
Manual	You need to perform the pre-installation tasks manually as described in the manual procedures.
Response file	You can pre-configure the systems for Oracle RAC installation using an SF Oracle RAC response file. The SF Oracle RAC response file in tandem with the Oracle RAC response files simplify the process of automating and standardizing Oracle RAC installations. **Note:** You can use the response file to automate only those pre-configuration tasks that are supported by the SF Oracle RAC installer. For instructions, see the chapter "Installing Oracle RAC using a response file" in this document.

The examples in this chapter assume a two-node cluster comprising the nodes galaxy and nebula.

Before installing Oracle RAC, review the Oracle installation manuals and the appropriate Oracle support Web sites.

Note: Some of the pre-installation tasks, wherever indicated in the document, must be done in accordance with the instructions in the Oracle installation manuals. The instructions for these tasks are not provided in this document.

Preparing to install Oracle RAC using the SF Oracle RAC installer or manually

This section provides instructions for both manual as well as SF Oracle RAC installer-based procedures.

To prepare to install Oracle RAC

1. Identify the public virtual IP addresses for use by Oracle.

   See "Identifying the public virtual IP addresses for use by Oracle" on page 277.

2. Set the kernel parameters.

   See "Setting the kernel parameters" on page 278.

3. Verify that the user nobody exists.

   See "Verifying the user "nobody" exists" on page 278.

4. Launch the SF Oracle RAC installer.

   See "Launching the SF Oracle RAC installer" on page 278.

5. Create Oracle user and groups.

   See "Creating users and groups for Oracle RAC" on page 279.

6. Create the storage for OCR and voting disk.

   See "Creating storage for OCR and voting disk " on page 282.

7. Configure the private network for Oracle RAC.

   See "Configuring private IP addresses for Oracle RAC" on page 295.

8. Create the Oracle Clusterware/Grid Infrastructure and Oracle database home directories manually.

   See "Creating Oracle Clusterware/Grid Infrastructure and Oracle database home directories manually" on page 308.

9. Set up Oracle user equivalence on all nodes.

   See "Setting up user equivalence" on page 323.

10 Set privileges for the DBA user.

See "Setting privileges for the DBA user" on page 323.

11 Verify the cluster configuration before the installation to ensure that there are no issues that may prevent a successful installation.

See "Verifying the systems for Oracle RAC installation" on page 324.

Identifying the public virtual IP addresses for use by Oracle

Identify separate public virtual IP addresses for each node in the cluster. Oracle requires one public virtual IP address for the Oracle listener process on each node. Public virtual IP addresses are used by client applications to connect to the Oracle database. Oracle Clusterware/Grid Infrastructure manages the virtual IP addresses.

The IP address and the corresponding host name should be registered in the domain name service (DNS). Alternatively, an entry for the virtual IP address and virtual public name can be placed in the `/etc/hosts` file as shown in the following example:

```
10.182.79.239 galaxy-vip
10.182.79.240 nebula-vip
```

The `/etc/hosts` file on each node of the cluster should have these entries.

Oracle recommends that the public node name for the virtual IP address be in the following format *hostname-vip*. For example, galaxy-vip.

Note: The public node name (in other words, the alias for the virtual IP address) for the nodes must be different from the host's current fully qualified domain name (FQDN).

For Oracle RAC 11g Release 2: Additionally, you need a Single Client Access Name (SCAN) registered in Enterprise DNS that resolves to three IP addresses (recommended) using a round robin algorithm or at least one IP address. The IP addresses must be on the same subnet as your public network in the cluster. SCAN provides a single name for clients to access an Oracle database running in a cluster.

Note: The virtual IP addresses that are used for SCAN IP resolution must be on the same subnet. Oracle RAC does not support their configuration on different subnets.

Setting the kernel parameters

Set the kernel parameter values to meet Oracle RAC deployment requirements. The Oracle Universal Installer (OUI) verifies the settings at the time of installation to ensure that they satisfy the minimum requirements. The Oracle RAC installation fails if the kernel parameters are not configured properly. The settings can also be tuned to optimize system performance.

For instructions and guidelines, see the Oracle Metalink document: 169706.1

Restart the nodes for the new values to take effect.

Verifying the user "nobody" exists

To verify the user "nobody" exists on each system in the cluster:

```
# id nobody
uid=65534(nobody) gid=65533(nobody) groups=65533(nobody),65534(nogroup)
```

If the user does not exist, create the user:

```
# groupadd -g 65533 nobody
# useradd -g 65533 -u 65533 nobody
```

Note: Make sure that the user ID and group ID are the same across the nodes in your cluster.

Launching the SF Oracle RAC installer

The following procedure describes the steps to launch the SF Oracle RAC installer for performing the Oracle RAC pre-installation tasks.

To launch the SF Oracle RAC installer

1. Log in as the root user on any one node and start the SF Oracle RAC installer:

   ```
   # cd /opt/VRTS/install

   # ./installsfrac -configure galaxy nebula
   ```

   The program displays the Symantec copyright information as well as the location of the installation logs.

2. Review the installer instructions and press **Enter** to proceed. From the configuration program menu, select **Prepare to Install Oracle**.

3. Select the pre-installation task you want to perform.

- Enter **1** to select the option **Create Oracle User and Group**:
  See "Creating users and groups for Oracle RAC" on page 279.
- Enter **2** to select the option **Create Storage for OCR and voting disk**:
  See "Creating storage for OCR and voting disk " on page 282.
- Enter **3** to select the option **Oracle Network Configuration**:
  See "Configuring private IP addresses for Oracle RAC" on page 295.

Creating users and groups for Oracle RAC

Depending on the Oracle RAC version, create the required users and groups.

Create the following groups and users for Oracle RAC 10g Release 2/ Oracle RAC 11g Release 1:

- Oracle Inventory group
- dba group
- Oracle user

Create the following groups and users for Oracle RAC 11g Release 2:

- Oracle Inventory group
- dba group
- Oracle grid user
- Oracle user

Create additional users and groups as required by Oracle. Before creating Oracle users and groups, see the Oracle documentation.

You must assign Oracle Inventory as the primary group and dba as the secondary group. Oracle requires secondary groups for identifying operating system accounts that have database administrative (SYSDBA) privileges and for those accounts that have limited sets of database administrative (SYSOPER) privileges. Create the groups on all systems and assign the Oracle user to these groups.

Use one of the following ways to create the Oracle user and groups:

Using the SF Oracle RAC installer	See "Creating Oracle user and groups using the SF Oracle RAC installer" on page 280.
Manual	See "Creating the Oracle user and groups manually" on page 281.

Creating Oracle user and groups using the SF Oracle RAC installer

This procedure provides instructions for creating Oracle user and groups using the SF Oracle RAC installer.

To create Oracle user and groups on all nodes in the cluster

1. From the SF Oracle RAC installer menu, enter **1** to select the option **Create Oracle User and Group**.
2. Provide the following information for creating the Oracle user and groups: user name, group name, user ID, group ID, and the full path of the Oracle user home directory.

   The user ID and group ID must not be in use on any node in the cluster. The installer suggests unused values, which you may use or change as required. The configuration program assigns the same values on all the nodes.

   Note: If you are configuring GCO, then the user IDs and group IDs of all nodes on both the primary and secondary clusters must be the same. While configuring the user ID and group ID values on the secondary site, make sure that they are identical to the values used at the primary site.

   ```
   Enter Oracle UNIX user name: [b] oracle
   Enter Oracle UNIX group name: [b] oinstall
   Enter Oracle user's ID (numerical):  [b] (1165) 1000
   Enter Oracle group's ID (numerical):  [b] (1165) 1000
   Enter absolute path of Oracle user's Home directory: [b] /home/oracle
   ```

   If the specified user name does not exist on any node in the cluster, the following prompt is displayed:

   ```
   User oracle does not exist on any node. Do you want to create it
   with the information provided [y,n,q] (y)
   ```

   Enter **y** to create the Oracle user with the information provided.

3 Enter the information to create secondary groups, "dba" and "oper".

The secondary group "oper" is optional.

```
Do you want to create a secondary group
for Oracle user? [y,n,q,b,?] (n) y
Enter Oracle UNIX group name:  [b] (dba, oper etc.) dba
Enter Oracle group's ID (numerical): [b] (1996) 1001

    Creating secondary group dba for
    Oracle user oracle on galaxy ..... Done
    Creating secondary group dba for
    Oracle user oracle on nebula ..... Done
Do you want to create another secondary group
for Oracle user? [y,n,q,b,?] (n)
```

4 Create a password for the oracle user on each node:

```
# passwd oracle
```

5 For Oracle RAC 11g Release 2: Repeat the above steps to create the grid user.

```
Enter Oracle UNIX user name: [b] grid
Enter Oracle UNIX group name: [b] (oinstall)
Enter Oracle user's ID (numerical):  [b] (1168) 1001
Enter Oracle group's ID (numerical):  [b] (1000)
Enter absolute path of Oracle user's Home directory: [b] /home/grid
```

Creating the Oracle user and groups manually

Perform this step only if you plan to configure the database storage management repository during the configuration of SF Oracle RAC.

Depending on the Oracle RAC version, create the necessary Oracle groups and users. Be sure to assign the same group ID, user ID, and home directory for the user on each system.

Note: When you create the user and group, make sure that you specify a user and group ID that is not in use.

To create the operating system Oracle user and group on each system

1 Create the 'oinstall' group on each system.

```
# groupadd -g 1000 oinstall

# groupadd -g 1001 dba
```

2 Create the Oracle user and the user home directory on each system:

```
# useradd -g oinstall -u 1000 \
-G dba -m -d /home/oracle oracle
```

3 For Oracle RAC 11g Release 2: Create the grid user and the user home directory on each system:

```
# useradd -g oinstall -u 1001 \
-G dba -m -d /home/grid grid
```

Creating storage for OCR and voting disk

Create appropriate storage for Oracle Cluster Registry (OCR) and the voting disk depending on the version of Oracle RAC.

Oracle RAC 10g Release 2/ Oracle RAC 11g Release 1	The OCR and the voting disk can reside on CVM raw volumes or in directories in a cluster file system.
Oracle RAC 11g Release 2	The OCR and the voting disk can reside on ASM or in directories in a cluster file system. **Note:** You can use CVM raw volumes to create ASM disk groups.

Use one of the following ways to create the storage:

SF Oracle RAC installer	See "Creating storage for OCR and voting disk using the installer" on page 283.
Manual	See "Creating storage for OCR and voting disk manually" on page 288.

You need to create CVM volumes or a CFS mount point for database file storage later in the installation process:

Creating storage for OCR and voting disk using the installer

The SF Oracle RAC installer enables you to create OCR and voting disk storage on CVM raw volumes or on a clustered file system. After creating the storage, the installer adds the storage configuration to VCS for high availability.

If you are creating the OCR and voting disk storage on CVM raw volumes, the installer performs the following tasks:

- Creates CVM volume mirrors for OCR and voting disk
- Creates the OCR and voting disk volumes and sets the ownership
- Starts the volumes
- Adds the CVMVolDg resource to the VCS configuration in the cvm group so that the volumes are brought online automatically when the node starts
- Brings the CVMVoIDg resource online

If you are creating the OCR and voting disk storage on CFS, the installer performs the following tasks:

- Creates CVM volume mirrors for OCR and voting disk
- Creates the OCR and voting disk volumes and sets the ownership
- Starts the volumes
- Creates the mount point and mounts it on all the nodes
- Sets the ownership for the CFS mount point
- Adds the CFSMount and CVMVolDg resources to the VCS configuration in the cvm group so that the resources are brought online automatically when the node starts
- Brings the CFSMount and CVMVoIDg resources online

To create storage for OCR and voting disk using the SF Oracle RAC installer

1 From the SF Oracle RAC installer menu, enter **2** to select the option **Create Storage for OCR and Voting disk**.

The following menu displays:

```
1)  Create Oracle User and Group
2)  Create Storage for OCR and Voting disk
3)  Oracle Network Configuration
4)  Exit SF Oracle RAC Configuration
b)  Back to previous menu
Choose option: [1-4,b,q] (1) 2
```

2 Enter **y** to create the storage.

```
Do you want the installer to assist you in creating disk groups,
volumes and file systems for Oracle? (Mirroring enabled
by default) [y,n,q] (n) y
```

If you want to create the storage manually, enter **n**. The installer displays instructions for creating the storage manually. You may skip the remaining steps.

3 Select an appropriate option for the disk group.

```
1)  Create a disk group
2)  Use an existing disk group
b)  Back to previous menu
Choose option: [1-2,b,q]
```

- If you choose to create a disk group, the installer displays the list of existing disks that do not belong to any disk group. Specify the disks (by entering the serial numbers displayed next to the disk names) that you want to use to create the disk group.
  Enter the name of the disk group.

  ```
  Enter the disk group name:  [b] (ocrvotedg)
  ```

- If you choose to use an existing disk group, the installer displays the existing disk groups that contain at least two disks for mirroring.

4 Review and confirm the configuration information displayed:

```
CVM Master node: galaxy
Selected disks (including mirroring):
   1. Disk_2
   2. Disk_3
Disk group name: ocrvotedg
Is this information correct? [y,n,q] (y)
```

The installer initializes the disk groups.

5 Choose the type of storage.

- To create the storage on CVM raw volumes
  See "Creating the OCR and voting disk storage on CVM raw volumes" on page 285.
- To create the storage on CFS:
  See "Creating the OCR and voting disk storage on CFS" on page 286.

Creating the OCR and voting disk storage on CVM raw volumes

Perform the steps in the following procedure to create the storage for OCR and voting disk on CVM raw volumes.

Note: For Oracle RAC 11g Release 2, you may create CVM raw volumes to create ASM disk groups that may be used to store the OCR and voting disk information.

To create the OCR and voting disk storage on CVM raw volumes

1 Enter **1** to select the option **CVM raw volumes**.

```
1  CVM Raw Volume
2  Clustered File System
b  Back to previous menu
Select the storage scheme to be used: [1-2,b,q] 1
```

2 Enter the name and size of the volume on which you want to store OCR information.

```
Enter the volume name for OCR:  [b] (ocrvol)
Enter the volume size for OCR (in MB):  [b] (320)
```

3 Enter the name and size of the volume on which you want to store voting disk information.

```
Enter the volume name for Vote:  [b] (votevol)
Enter the volume size for Vote (in MB):  [b] (320)
```

4 Enter the Oracle UNIX user name.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
Enter Oracle UNIX user name:  [b] oracle
```

For Oracle RAC 11g Release 2:

```
Enter Oracle UNIX user name:  [b] grid
```

5 Enter the Oracle UNIX group name.

```
Enter Oracle UNIX group name:  [b] (oinstall)
```

6 Press **Return** to continue.

7 Review and confirm the configuration information. The installer creates the volumes and brings the corresponding resources online.

Press **Return** to continue.

8 Verify that the resource is online on all nodes in the cluster.

Note: It takes a few minutes for the CVMVolDg resource to come online.

```
# hares -state ocrvote_voldg_ocrvotedg
```

Creating the OCR and voting disk storage on CFS

Perform the steps in the following procedure to create the storage for OCR and voting disk on CFS.

To create the OCR and voting disk storage on CFS

1 Enter **2** to select the option **CFS Mounted**.

```
1  CVM Raw Volume
2  Clustered File System
b  Back to previous menu
Select the storage scheme to be used: [1-2,b,q] 2
```

2 Enter the name and size of the volume on which you want to store OCR and voting disk information.

```
Enter the volume name for OCR and Voting disk: [b] (ocrvotevol)
Enter the volume size for OCR and Voting disk (in MB): [b] (640)
```

3 Enter the Oracle UNIX user name.

The Oracle UNIX user name was previously set up when you performed the pre-installation task of creating Oracle user and group.

```
Enter Oracle UNIX user name:  [b] oracle
```

4 Enter the Oracle UNIX group name.

The Oracle UNIX group name was previously set up when you performed the pre-installation task of creating Oracle user and group.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
Enter Oracle UNIX group name: [b] (oinstall)
```

For Oracle RAC 11g Release 2:

```
Enter Oracle UNIX group name: [b] (oinstall)
```

5 Press **Return** to continue.

6 Review and confirm the configuration information. The installer creates and starts the volumes on all nodes in the cluster.

7 Enter the CFS mount point for OCR and voting disk information.

```
Enter the mount point location for CFS (common for all the nodes) [b]
(/ocrvote)
```

The installer creates the CFS mount points and sets the ownership. Press **Return** to continue.

8 Verify that the ocrvote_mnt_ocrvotedg and ocrvote_voldg_ocrvotedg resources are online on all nodes in the cluster:

Note: It takes a few minutes for the CVMVolDg resource to come online.

```
# hares -state ocrvote_mnt_ocrvotedg

# hares -state ocrvote_voldg_ocrvotedg
```

Creating storage for OCR and voting disk manually

Use one of the following storage options to create the OCR and voting disk storage:

CVM raw volumes	See "To create OCR and voting disk volumes on raw volumes" on page 288.
CFS	See "To create the storage for OCR and voting disks on CFS" on page 289.

Note: Whether you create volumes or file system directories, you can add them to the VCS configuration to make them highly available.

To create OCR and voting disk volumes on raw volumes

1 Log in as the root user.

2 Determine the CVM master:

```
# vxdctl -c mode
```

3 On the master node, create a shared disk group:

```
# vxdg -s init ocrvotedg Disk_2 Disk_3
```

4 Set the activation mode for the disk group on all the nodes.

```
# vxdg -g ocrvotedg set activation=sw
```

5 Create mirrored volumes in the shared group for OCR and voting disk:

```
# vxassist -g ocrvotedg make ocrvol 300M nmirrors=2

# vxassist -g ocrvotedg make votevol 300M nmirrors=2
```

6 Set the ownership for the volumes:

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# vxedit -g ocrvotedg set group=oinstall user=oracle mode=660
ocrvol
# vxedit -g ocrvotedg set group=oinstall user=oracle mode=660
votevol
```

For Oracle RAC 11g Release 2:

```
# vxedit -g ocrvotedg set group=oinstall user=grid mode=660
ocrvol
# vxedit -g ocrvotedg set group=oinstall user=grid mode=660
votevol
```

7 Start the volume:

```
# vxvol -g ocrvotedg startall
```

8 Add the storage resources to the VCS configuration to make them highly available.

See "Adding the storage resources to the VCS configuration" on page 290.

To create the storage for OCR and voting disks on CFS

1 Determine the CVM master:

```
# vxdctl -c mode
```

2 On the master node, create a shared VxVM disk group:

```
# vxdg -s init ocrvotedg Disk_2 Disk_3
```

3 Set the activation mode for the disk group on all the nodes.

```
# vxdg -g ocrvotedg set activation=sw
```

4 From the CVM master node, start the disk group:

```
# vxvol -g ocrvotedg startall
```

5 From the CVM master, create a mirrored volume `ocrvotevol`:

```
# vxassist -g ocrvotedg make ocrvotevol 640M nmirrors=2
```

6 From the CVM master, create a file system with the volume `ocrvotevol`.

```
# mkfs -F vxfs /dev/vx/rdsk/ocrvotedg/ocrvotevol
```

7 Start the volume:

```
# vxvol -g ocrvotedg startall
```

8 On each system, create a directory `/ocrvote`:

```
# mkdir /ocrvote
```

9 On each system, mount the directory `/ocrvote`:

```
# mount -F vxfs -o cluster /dev/vx/dsk/ocrvotedg/ocrvotevol
/ocrvote
```

10 From any system, change permissions on `/ocrvote`:

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# chown -R oracle:oinstall /ocrvote
```

For Oracle RAC 11g Release 2:

```
# chown -R grid:oinstall /ocrvote
```

11 Add the storage resources to the VCS configuration to make them highly available.

See "Adding the storage resources to the VCS configuration" on page 290.

Adding the storage resources to the VCS configuration

The type of storage resource you add to the VCS configuration depends on whether you chose to create the OCR and voting disk storage on raw volumes or CFS. If you chose to create the storage on raw volumes, you need to add a CVMVolDg resource to the VCS configuration. If you chose to create the storage on CFS, you need to add the CVMVolDg and CFSMount resources to the VCS configuration.

Depending on the type of storage, follow the steps in one of the following procedures to add the storage resources to the VCS configuration using the command line interface (CLI):

For storage resources on CVM raw volumes	See "To add the storage resources created on raw volumes to the VCS configuration" on page 293.
For storage resources on CFS	See "To add the storage resources created on CFS to the VCS configuration" on page 291.

Note: Set the attribute "Critical" to "0" for all the resources in the cvm service group. This ensures that critical CVM and CFS resources are always online.

To add the storage resources created on CFS to the VCS configuration

1 Change the permissions on the VCS configuration file:

```
# haconf -makerw
```

2 Configure the CVM volumes under VCS:

```
# hares -add ocrvote_voldg_ocrvotedg CVMVolDg cvm

# hares -modify ocrvote_voldg_ocrvotedg Critical 0

# hares -modify ocrvote_voldg_ocrvotedg CVMDiskGroup ocrvotedg

# hares -modify ocrvote_voldg_ocrvotedg CVMVolume -add ocrvotevol

# hares -modify ocrvote_voldg_ocrvotedg CVMActivation sw
```

3 Set up the file system under VCS:

```
# hares -add ocrvote_mnt_ocrvotedg CFSMount cvm

# hares -modify ocrvote_mnt_ocrvotedg Critical 0

# hares -modify ocrvote_mnt_ocrvotedg MountPoint "/ocrvote"

# hares -modify ocrvote_mnt_ocrvotedg BlockDevice  \
"/dev/vx/dsk/ocrvotedg/ocrvotevol"

# hares -modify ocrvote_mnt_ocrvotedg
```

4 Link the parent and child resources:

```
# hares -link ocrvote_voldg_ocrvotedg cvm_clus

# hares -link ocrvote_mnt_ocrvotedg ocrvote_voldg_ocrvotedg

# hares -link ocrvote_mnt_ocrvotedg vxfsckd
```

5 Enable the resources:

```
# hares -modify ocrvote_voldg_ocrvotedg Enabled 1

# hares -modify ocrvote_mnt_ocrvotedg Enabled 1

# haconf -dump -makero
```

6 Verify the configuration of the ocrvote_mnt_ocrvotedg and ocrvote_voldg_ocrvotedg resources in main.cf.

```
CFSMount ocrvote_mnt_ocrvotedg (
               Critical = 0
               MountPoint = "/ocrvote"
               BlockDevice = "/dev/vx/dsk/ocrvotedg/ocrvotevol"
               MountOpt= "mincache=direct"
               )
CVMVolDg ocrvote_voldg_ocrvotedg (
              Critical = 0
              CVMDiskGroup = ocrvotedg
              CVMVolume = { ocrvotevol }
              CVMActivation = sw
              )
ocrvote_mnt_ocrvotedg requires ocrvote_voldg_ocrvotedg
ocrvote_mnt_ocrvotedg requires vxfsckd
ocrvote_voldg_ocrvotedg requires cvm_clus
```

7 Bring the ocrvote_mnt_ocrvotedg and ocrvote_voldg_ocrvotedg resources online on all systems in the cluster:

```
# hares -online ocrvote_voldg_ocrvotedg -sys sys_name

# hares -online ocrvote_mnt_ocrvotedg -sys sys_name
```

Verify that the resources are online on all systems in the cluster:

```
# hares -state ocrvote_voldg_ocrvotedg

# hares -state ocrvote_mnt_ocrvotedg
```

To add the storage resources created on raw volumes to the VCS configuration

1 Change the permissions on the VCS configuration file:

```
# haconf -makerw
```

2 Configure the CVM volumes under VCS:

```
# hares -add ocrvote_voldg_ocrvotedg CVMVolDg cvm

# hares -modify ocrvote_voldg_ocrvotedg Critical 0

# hares -modify ocrvote_voldg_ocrvotedg CVMDiskGroup ocrvotedg

# hares -modify ocrvote_voldg_ocrvotedg CVMVolume -add ocrvol

# hares -modify ocrvote_voldg_ocrvotedg CVMVolume -add votevol

# hares -modify ocrvote_voldg_ocrvotedg CVMActivation sw
```

3 Link the parent and child resources:

```
# hares -link ocrvote_voldg_ocrvotedg cvm_clus
```

4 Enable the resources:

```
# hares -modify ocrvote_voldg_ocrvotedg Enabled 1

# haconf -dump -makero
```

5 Verify the configuration of the ocrvote_voldg_ocrvotedg resource in main.cf.

```
CVMVolDg ocrvote_voldg_ocrvotedg (
              Critical = 0
              CVMDiskGroup = ocrvotedg
              CVMVolume = { ocrvol, votevol }
              CVMActivation = sw
              )
ocrvote_voldg_ocrvotedg requires cvm_clus
```

6 Bring the ocrvote_voldg_ocrvotedg resource online on all systems in the cluster:

```
# hares -online ocrvote_voldg_ocrvotedg -sys sys_name
```

Verify that the resource is online on all systems in the cluster:

```
# hares -state ocrvote_voldg_ocrvotedg
```

Setting CVM disk policies for OCR, voting disk, and data disk groups

Table 17-1 describes the CVM disk policies you need to set for Oracle Cluster Registry (OCR), voting disk, and data disk groups.

Table 17-1 Disk group fail policy for OCR, voting disk, and data disk groups

Disk group	Policy setting
OCR and voting disk	`leave` If the disk groups containing the OCR and voting disk uses the default policy setting (`dgdisable`), and the CVM master node looses connectivity to the storage, then a cluster-wide panic results. The CVM master node disables the corresponding disk group after a storage loss and prevents access to volumes from any cluster node. This in turn prevents the slave nodes from performing I/O operations to shared volumes even though issues with storage may be confined to the master node. If Oracle's clusterware is unable to perform I/O operations to voting disks, the corresponding node is panicked and evicted from the cluster. Setting the policy to `leave` for the disk group ensures that only the node which loses connectivity to the storage is panicked.
Data disk groups	`leave` If the disk groups containing the Oracle data uses the default policy setting (`dgdisable`), and if one of the nodes in the cluster looses connectivity to the storage, then the disk group is disabled across the cluster. This causes the database to freeze on all nodes in the cluster. Setting the policy to `leave` for the disk group ensures that only the node which loses connectivity to the storage is panicked.

Note: Symantec strongly recommends retaining the default setting (`global`) for the disk detach policy. For other disk detach policy options, see the *Veritas Volume Manager Administrator's Guide*.

To set the disk policies for OCR, voting disk, and data disk groups

1 Log into the CVM master node as the root user.

2 Set the disk group fail policy as follows:

```
# vxdg -g dg_name set dgfailpolicy=leave
```

Configuring private IP addresses for Oracle RAC

Private IP addresses are required by Oracle RAC to provide communication between the cluster nodes. Depending on your private network configuration, you may need one or more IP addresses. You can configure the private IP addresses for high availability using the PrivNIC or MultiPrivNIC agents.

Note: IPv6 addresses are not supported in this release.

Table 17-2 lists the available options for configuring the private network for Oracle RAC. Use one of the following options to configure the private network.

Table 17-2 Options for configuring the private network for Oracle RAC

Option	Description
PrivNIC configuration	Perform this configuration if you plan to: ■ Use a common IP address for Oracle Clusterware/Grid Infrastructure heartbeat and Oracle RAC database cache fusion and you plan to configure the IP address for high availability using the PrivNIC agent. ■ Or, in the case of Oracle RAC 10g Release 2, use VCSIPC/LMX/LLT for Oracle RAC database cache fusion (you need an IP address only for Oracle Clusterware heartbeat in this scenario) and you plan to configure the IP address for high availability using the PrivNIC agent. For instructions: See "Configuring the private IP address and PrivNIC resource" on page 296.

Table 17-2 Options for configuring the private network for Oracle RAC *(continued)*

Option	Description
MultiPrivNIC configuration	Perform this configuration if you plan to: ■ Use an IP address on each node for Oracle Clusterware/Grid Infrastructure heartbeat ■ And, use one or more IP addresses on each node for Oracle database cache fusion ■ And, configure the IP addresses for high availability using the MultiPrivNIC agent For instructions: See "Configuring the private IP address information and MultiPrivNIC resource" on page 300.

Configuring the private IP address and PrivNIC resource

You need to configure the following information:

- An IP address on each node
  If you plan to install Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1, the IP addresses configured must be added to the `/etc/hosts` file (using the SF Oracle RAC installer or manually) on all the nodes before installing Oracle Clusterware/Grid Infrastructure.
- The PrivNIC agent for failing over IP addresses in the event of link failures.
  The Oracle Clusterware/Grid Infrastructure interconnects need to be protected against NIC failures and link failures. The installer discovers the existing private NICs on which LLT is configured. For maximum failover options, all available LLT links are used for PrivNIC configuration.

Use one of the following ways to configure the PrivNIC and private IP address information:

SF Oracle RAC installer	See "Configuring the private IP address and PrivNIC using the SF Oracle RAC installer" on page 296.
Manual	See "Configuring the private IP address and PrivNIC resource manually" on page 299.

Configuring the private IP address and PrivNIC using the SF Oracle RAC installer

The SF Oracle RAC installer performs the following tasks:

- Backs up the /etc/hosts file and adds the IP address information to the file (only if you specified that the installer update the file).
- Adds the PrivNIC resource in the CVM group.

Perform the steps in the following procedure to configure the PrivNIC and private IP address using the installer.

To configure the PrivNIC and private IP address information

1 From the SF Oracle RAC menu, enter **3** to select the option **Oracle Network Configuration**.

```
1)  Create Oracle User and Group
2)  Create Storage for OCR and Voting disk
3)  Oracle Network Configuration
4)  Exit SF Oracle RAC Configuration
b)  Back to previous menu
Choose option: [1-4,b,q] (1) 3
```

2 Enter **1** to select the option **Configure private IP addresses (PrivNIC Configuration)**.

```
1)  Configure private IP addresses (PrivNIC Configuration)
2)  Configure private IP addresses (MultiPrivNIC Configuration)
3)  Exit SF Oracle RAC Configuration
b)  Back to previous menu
Choose option: [1-3,b,q] (1) 1
```

The installer discovers available LLT links and PrivNIC resources.

If PrivNIC resources exist, you can choose to delete and reconfigure the resources using the installer.

Note: The installer only removes the corresponding PrivNIC resources from the configuration file. You must manually disassociate the IP addresses from the corresponding network interfaces and remove the IP addresses from the /etc/hosts file.

---

3 Enter the name for the PrivNIC resource.

```
Enter the PrivNIC resource name: [b] (ora_priv)
```

4 Enter **y** to modify the priority of the PrivNIC interfaces.

Note: The priority you set determines the interface that the PrivNIC agent chooses during failover.

```
Do you want to update the priority of the PrivNIC
interfaces? [y,n,q] (n) y
```

5 Set the interface priority in decreasing order. The PrivNIC agent will assign the highest priority to the first interface specified in the list.

```
Enter the interface name in the decreasing priority order,
separated by a space: [b] (lan2 lan3) lan3 lan2
```

6
- Enter **y** to add the IP addresses to the `/etc/hosts` file.
- Enter **n** if you choose to add the IP addresses to the file manually. Go to step 8.

7 Perform this step only if you enabled the installer to add the IP address to the /etc/hosts file in the previous step.

Provide the private IP address and the private node name for the IP address that must be added to the file.

Note: All IP addresses must be in the same subnet, failing which Oracle Clusterware/Grid Infrastructure will not be able to communicate properly across the nodes.

If the private IP address entries are already present in the /etc/hosts file on one of nodes in the cluster, the installer does not update the file with the specified IP addresses on any of the nodes in the cluster.

```
Enter the private IP for galaxy: [b] 192.168.12.1
Enter Hostname alias for the above IP address: [b] galaxy-priv
Enter the private IP for nebula: [b] 192.168.12.2
Enter Hostname alias for the above IP address: [b] nebula-priv
```

Go to step 9.

8 Perform this step only if you have chosen to add the IP address to the /etc/hosts file manually.

Enter the private IP address information.

```
Enter the private IP for galaxy: [b] 192.168.12.1
Enter the private IP for nebula: [b] 192.168.12.2
```

9 Enter the netmask information for the private network:

```
Enter the Netmask for private network: [b] (255.255.255.0)
```

The SF Oracle RAC installer now displays the configuration information.

10 Enter **y** to review and confirm the configuration information. The installer adds the PrivNIC resources to the VCS configuration and updates the /etc/hosts file (if you chose an installer-based update).

11 If you chose to add the IP address information to the /etc/hosts file manually, proceed to update the file as described in the following procedure.

See "Adding private IP addresses to the /etc/hosts file manually" on page 306.

12 Verify the PrivNIC configuration updates made by the program in the main.cf file.

See "Verifying the VCS configuration for PrivNIC and MultiPrivNIC" on page 307.

Configuring the private IP address and PrivNIC resource manually

Perform the steps in the following procedure to configure the private IP address and PrivNIC resource manually. Configure the PrivNIC resource in the VCS group where you have configured the OCR and voting disk resources.

The sample procedure creates the PrivNIC resource in the cvm group. The PrivNIC agent plumbs the IP address to the specified network interface.

To configure the private IP address and PrivNIC resource manually

1 Log in as the root user on one of the nodes in the cluster.

2 Change the cluster configuration to read-write mode:

```
# haconf -makerw
```

3 Create the PrivNIC resource and add the resource to the cvm group:

```
# hares -add ora_priv PrivNIC cvm
```

4 Modify the PrivNIC resource:

```
# hares -modify ora_priv Critical 0
# hares -local ora_priv Device
# hares -local ora_priv Address
# hares -modify ora_priv \
Device -add lan1 0 -sys galaxy
# hares -modify ora_priv \
Device -add lan2 1 -sys galaxy
# hares -modify ora_priv \
Address 192.168.12.1 -sys galaxy
# hares -modify ora_priv \
Device -add lan1 0 -sys nebula
# hares -modify ora_priv \
Device -add lan2 1 -sys nebula
# hares -modify ora_priv \
Address 192.168.12.2 -sys nebula
# hares -modify ora_priv \
NetMask 255.255.255.0
# hares -modify ora_priv Enabled 1
```

5 Change the cluster configuration to read-only mode:

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

Configuring the private IP address information and MultiPrivNIC resource

You need to configure the following information:

- An IP address on each node for Oracle Clusterware/Grid Infrastructure heartbeats
- One or more IP addresses on each node for the Oracle database
- The MultiPrivNIC agent for failing over IP addresses in the event of link failures.
  The Oracle Clusterware/Grid Infrastructure interconnects need to be protected against NIC failures and link failures. The MultiPrivNIC agent protects the links against failures, if multiple links are available. The installer discovers the existing private NICs on which LLT is configured. For maximum failover options, all available LLT links are used for MultiPrivNIC configuration.

If you plan to use Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1, the IP addresses configured must be added to the `/etc/hosts` file (using the SF Oracle

RAC installer or manually) on all the nodes before installing Oracle Clusterware/Grid Infrastructure.

Use one of the following ways to configure the MultiPrivNIC and private IP address information:

SF Oracle RAC installer	See "Configuring the MultiPrivNIC and private IP address information using the SF Oracle RAC installer" on page 301.
Manual	See "Configuring MultiPrivNIC and private IP addresses manually " on page 304.

Configuring the MultiPrivNIC and private IP address information using the SF Oracle RAC installer

Perform the steps in the following procedure to configure the MultiPrivNIC and private IP address using the installer.

The installer performs the following tasks:

- Backs up the /etc/hosts file and adds the IP address information to the file (only if you specified that the installer update the file).
- Adds the MultiPrivNIC resource in the CVM group.

To configure the MultiPrivNIC and private IP address information using the installer

1 From the SF Oracle RAC menu, enter **3** to select the option **Oracle Network Configuration**.

```
1)  Create Oracle User and Group
2)  Create Storage for OCR and Voting disk
3)  Oracle Network Configuration
4)  Exit SF Oracle RAC Configuration
b)  Back to previous menu
Choose option: [1-4,b,q] (1) 3
```

2 Enter **2** to select the option **Configure private IP addresses (MultiPrivNIC Configuration)**.

```
1)  Configure private IP addresses (PrivNIC Configuration)
2)  Configure private IP addresses (MultiPrivNIC Configuration)
3)  Exit SF Oracle RAC Configuration
b)  Back to previous menu
Choose option: [1-3,b,q] (1) 2
```

The installer discovers available LLT links and MultiPrivNIC resources. If MultiPrivNIC resources exist, you can choose to delete and reconfigure the resources using the installer.

Note: The installer only removes the corresponding MultiPrivNIC resources from the configuration file. You must manually disassociate the IP addresses from the corresponding network interfaces and remove the IP addresses from the /etc/hosts file.

---

3 Enter the name for the MultiPrivNIC resource.

```
Enter the MultiPrivNIC resource name: [b] (ora_mpriv) multi_priv
```

4
- Enter **y** to add the IP addresses to the `/etc/hosts` file.
- Enter **n** if you choose to add the IP addresses to the file manually. Go to step 6.

5 Perform this step only if you enabled the installer to add the IP address to the /etc/hosts file in the previous step.

Provide the private IP address and the private node name for the IP addresses that must be added to the file. When you do not want to enter information at the prompts, enter **x**.

Note: The IP addresses used for a particular NIC on all nodes of a cluster must be in the same subnet. This subnet must be different from the subnets for the IP addresses on other NICs. Otherwise, Oracle Clusterware/Grid Infrastructure and UDP IPC will not be able to communicate properly across the nodes.

If the private IP address entries are already present in the /etc/hosts file on one of the nodes in the cluster, the installer does not update the file with the specified IP addresses on any of the nodes in the cluster.

```
Enter IP addresses for galaxy for lan1 separated by space: [b,q,?]
192.168.12.1
Enter Hostname aliases for the above IP addresses
separated by space: [b,q,?] galaxy-priv
Enter IP addresses for galaxy for lan2
separated by space: [b,q,?] 192.168.2.1
Enter Hostname aliases for the above IP addresses
separated by space: [b,q,?]  galaxy-priv1
Enter IP addresses for nebula for lan1
separated by space: [b,q,?] 192.168.12.2
Enter Hostname aliases for the above IP addresses
separated by space: [b,q,?] nebula-priv
Enter IP addresses for nebula for lan2
separated by space: [b,q,?] 192.168.2.2
Enter Hostname aliases for the above IP addresses
separated by space: [b,q,?] nebula-priv1
```

Go to step 7.

6 Perform this step only if you have chosen to add the IP address to the /etc/hosts file manually.

Enter the private IP address information.

```
Enter IP addresses for galaxy for lan1
separated by space: [b,q,?] 192.168.12.1
Enter IP addresses for galaxy for lan2
separated by space: [b,q,?] 192.168.2.1
Enter IP addresses for nebula for lan1
separated by space: [b,q,?] 192.168.12.2
Enter IP addresses for nebula for lan2
separated by space: [b,q,?] 192.168.2.2
```

7 Enter the netmask information for the private network:

```
Enter the Netmask for private network: [b] (255.255.255.0)
```

The SF Oracle RAC installer displays the configured parameters.

8 Enter **y** to review and confirm the configuration information. The installer adds the MultiPrivNIC resources and updates the /etc/hosts file (if you chose installer-based update).

9 If you chose to add the IP address information to the /etc/hosts file manually, proceed to update the file as described in the following procedure.

See "Adding private IP addresses to the /etc/hosts file manually" on page 306.

10 Verify the MultiPrivNIC configuration updates made by the program in the main.cf file.

See "Verifying the VCS configuration for PrivNIC and MultiPrivNIC" on page 307.

Configuring MultiPrivNIC and private IP addresses manually

Perform the steps in the following procedure to configure MultiPrivNIC and private IP addresses for Oracle Clusterware/Grid Infrastructure and UDP IPC manually. Configure the MultiPrivNIC resource in the VCS group where you have configured the OCR and voting disk resources.

Make sure that the number of links are the same for every node. For example, in the following configuration, if the lan1 and lan2 links fail, the MultiPrivNIC agent fails over the IP addresses to the lan3 link on galaxy; On nebula, the absence of a third link results in the agent failing over the link to lan1, which is already down. This results in loss of communication between the nodes and causes Oracle Clusterware/Grid Infrastructure to reboot the cluster.

```
MultiPrivNIC multi_priv (
          Critical = 0
          Device@galaxy = {lan1 = 0, lan2 = 1, lan3 = 2}
          Device@nebula = {lan1 = 0, lan2 = 1}
          Address@galaxy = {"192.168.12.1" = 0,"192.168.2.1" = 1}
          Address@nebula = {"192.168.12.2" = 0,"192.168.2.2" = 1}
          NetMask = "255.255.255.0"
          )
```

Note: Avoid configurations where the number of links differ between the nodes.

The sample procedure creates the MultiPrivNIC resource in the cvm group. The MultiPrivNIC agent plumbs the IP addresses to the appropriate network interfaces.

To configure the private IP address and MultiPrivNIC manually

1. Log in as the root user on one of the nodes in the cluster.
2. Change the cluster configuration to read-write mode:

   ```
   # haconf -makerw
   ```

3. Create the MultiPrivNIC resource and add the resource to the cvm group:

   ```
   # hares -add multi_priv MultiPrivNIC cvm
   ```

4 Modify the MultiPrivNIC resource:

```
# hares -modify multi_priv Critical 0
# hares -local multi_priv Device
# hares -local multi_priv Address
# hares -modify multi_priv \
Device -add lan1 0 -sys galaxy
# hares -modify multi_priv \
Device -add lan2 1 -sys galaxy
# hares -modify multi_priv \
Address -add 192.168.12.1 0 -sys galaxy
# hares -modify multi_priv \
Address -add 192.168.2.1 1 -sys galaxy
# hares -modify multi_priv \
Device -add lan1 0 -sys nebula
# hares -modify multi_priv \
Device -add lan2 1 -sys nebula
# hares -modify multi_priv \
Address -add 192.168.12.2 0 -sys nebula
# hares -modify multi_priv \
Address -add 192.168.2.2 1 -sys nebula
# hares -modify multi_priv \
NetMask 255.255.255.0
# hares -modify multi_priv Enabled 1
```

5 Change the cluster configuration to read-only mode:

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

Adding private IP addresses to the /etc/hosts file manually

Perform the steps in the following procedure only if you plan to install Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1 and you chose to add the private IP address information manually to the `/etc/hosts` file at the time of configuring them using the SF Oracle RAC installer.

To add private IP addresses to the /etc/hosts file manually

1 Log in to each system as the root user.

2 For a configuration using the PrivNIC agent, add the following entries to the /etc/hosts file:

```
192.168.12.1  galaxy-priv

192.168.12.2  nebula-priv
```

For a configuration using the MultiPrivNIC agent, add the following entries to the /etc/hosts file:

```
192.168.12.1  galaxy-priv

192.168.2.1  galaxy-priv1

192.168.12.2  nebula-priv

192.168.2.2  nebula-priv1
```

Verifying the VCS configuration for PrivNIC and MultiPrivNIC

After you complete the steps for configuring PrivNIC/MultiPrivNIC and the private IP addresses, verify the configuration in the VCS main.cf configuration file.

To verify the VCS configuration for PrivNIC and MultiPrivNIC

1 View the main.cf file located in the directory `/etc/VRTSvcs/conf/config`:

```
# more /etc/VRTSvcs/conf/config/main.cf
```

2 For a configuration using the PrivNIC agent:

- Verify that the PrivNIC resource `ora_priv` displays in the file:

```
PrivNIC ora_priv (
                    Critical = 0
                    Device @galaxy = {lan1= 0, lan2= 1}
                    Device @nebula = {lan1= 0, lan2= 1}
                    Address @galaxy = "192.168.12.1"
                    Address @nebula = "192.168.12.2"
                    NetMask = "255.255.255.0"
                    )
```

- Verify that the `ora_priv` resource is online on all systems in the cluster:

```
# hares -state ora_priv
Resource Attribute System Value
ora_priv State    galaxy   ONLINE
ora_priv State    nebula   ONLINE
```

3 For a configuration using the MultiPrivNIC agent:

- Verify that the MultiPrivNIC resource `multi_priv` displays in the file:

```
MultiPrivNIC multi_priv (
             Critical = 0
             Device @galaxy = {lan1= 0, lan2 = 1}
             Device @nebula = {lan1= 0, lan2 = 1}
             Address @galaxy = {"192.168.12.1" =0, "192.168.2.1" =1}
             Address @nebula = {"192.168.12.2" =0, "192.168.2.2" =1}
             NetMask = "255.255.255.0"
             )
```

- Verify that the `multi_priv` resource is online on all systems in the cluster:

```
# hares -state multi_priv
Resource      Attribute        System      Value
multi_priv       State          galaxy     ONLINE
multi_priv       State          nebula     ONLINE
```

4 On each system, check the output of "ifconfig". Make sure that the specified private IP addresses and devices are displayed.

```
# netstat -in
```

5 From each system, verify that the private IP addresses are operational using the `ping` command.

Creating Oracle Clusterware/Grid Infrastructure and Oracle database home directories manually

You can create the Oracle Clusterware/Grid Infrastructure and Oracle database home directories on the local file system, on a local Veritas file system, or on a Veritas cluster file system. Perform this step if you plan to place the directories on VxFS or CFS. When the installer prompts for the home directories at the time of installing Oracle Clusterware/Grid Infrastructure and Oracle database, it creates the directories locally on each node, if they do not exist.

Note: Symantec recommends that you install the Oracle RAC binaries local to each node in the cluster.

Table 17-3 lists the Oracle RAC directories you need to create:

Table 17-3 List of directories

Directory	Description
Oracle Clusterware Home Directory (CRS_HOME) (For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1)	The path to the home directory that stores the Oracle Clusterware binaries. The Oracle Universal Installer (OUI) installs Oracle Clusterware into this directory, also referred to as CRS_HOME. The directory must be owned by the installation owner of Oracle Clusterware (oracle), with the permission set to 755. Follow Oracle Optimal Flexible Architecture (OFA) guidelines while choosing the path.
Oracle Grid Infrastructure Home Directory (GRID_HOME) (For Oracle RAC 11g Release 2)	The path to the home directory that stores the Oracle Grid Infrastructure binaries. The Oracle Universal Installer (OUI) installs Oracle Grid Infrastructure and Oracle ASM into this directory, also referred to as GRID_HOME. The directory must be owned by the installation owner of Oracle Grid Infrastructure (oracle or grid), with the permission set to 755. The path to the grid home directory must be the same on all nodes. Follow Oracle Optimal Flexible Architecture (OFA) guidelines while choosing the path.
Oracle base directory (ORACLE_BASE)	The base directory that contains all the Oracle installations. For Oracle RAC 11g Release 2, create separate Oracle base directories for the grid user and the Oracle user. It is recommended that installations of multiple databases maintain an Optimal Flexible Architecture (OFA) configuration. The path to the Oracle base directory must be the same on all nodes. The permission on the Oracle base directory must be at least 755.
Oracle home directory (ORACLE_HOME)	The directory in which the Oracle database software is installed. The path to the Oracle home directory must be the same on all nodes. The permission on the Oracle home directory must be at least 755.

Table 17-4 lists the sample directories for Oracle RAC 10g Release 2/Oracle RAC 11g Release 1 used in the procedures.

Table 17-4 Sample directories for Oracle RAC 10g Release 2/Oracle RAC 11g Release 1

Directory	Path
ORACLE_BASE	/u01/app/oracle
CRS_HOME	/u01/app/oracle/product/10.2.0/crshome
ORACLE_HOME	/u01/app/oracle/product/*release*/dbhome_1 where *release* is 10.2.0 or 11.1.0 depending on the Oracle RAC version

Table 17-5 lists the sample directories for Oracle RAC 11g Release 2 used in the procedures.

Table 17-5 Sample directories for Oracle RAC 11g Release 2

Directory	Path
ORACLE_BASE (Grid user)	/u01/app/gridbase
GRID_HOME (Grid user)	/u01/app/grid/product/11.2.0/gridhome
ORACLE_BASE (Oracle user)	/u01/app/oracle
ORACLE_HOME (Oracle user)	/u01/app/oracle/product/11.2.0/dbhome_1

Use one of the following options to create the directories:

Local file system — See "To create the directories on the local file system" on page 311.

Veritas File System — See "To create the file system and directories on the Veritas File system (VxFS) " on page 311.

Cluster File System — See "To create the file system and directories on cluster file system for Oracle Grid Infrastructure and Oracle database" on page 315.

To create the directories on the local file system

1. Log in as the root user on each node.
2. Create the directories and set the ownership and permissions:

   For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

   ```
   # mkdir -p /u01/app/oracle
   # mkdir -p /u01/app/oracle/product/10.2.0/crshome
   # mkdir -p /u01/app/oracle/product/10.2.0/dbhome_1
   # chown -R oracle:oinstall /u01/app
   # chmod -R 775 /u01/app
   ```

   For Oracle RAC 11g Release 2:

   ```
   # mkdir -p /u01/app/gridbase
   # mkdir -p /u01/app/grid/product/11.2.0/gridhome
   # chown -R grid:oinstall /u01/app
   # chmod -R 775 /u01/app

   # mkdir -p /u01/app/oracle
   # mkdir -p /u01/app/oracle/product/11.2.0/dbhome_1
   # chown -R oracle:oinstall /u01/app/oracle
   # chmod -R 775 /u01/app/oracle
   ```

To create the file system and directories on the Veritas File system (VxFS)

The sample commands in the procedure are for node galaxy. Repeat the steps on each node of the cluster.

1. As the root user, create a VxVM local diskgroup `bindg_hostname` on each node.

   Make sure that the size of the disk group is approximately 12 GB; if not, add another disk to the disk group.

   ```
   # vxdg init bindg_galaxy Disk_1
   ```

2. Create separate volumes for Oracle Clusterware/Oracle Grid Infrastructure (`crsbinvol`) binaries and Oracle binaries (`orabinvol`):

   ```
   # vxassist -g bindg_galaxy make crsbinvol 5G
   # vxassist -g bindg_galaxy make orabinvol 7G
   ```

3 Create the directories for Oracle RAC.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# mkdir -p /u01/app/oracle
# mkdir -p /u01/app/oracle/product/10.2.0/crshome
# mkdir -p /u01/app/oracle/product/10.2.0/dbhome_1
```

For Oracle RAC 11g Release 2:

```
# mkdir -p /u01/app/gridbase
# mkdir -p /u01/app/grid/product/11.2.0/gridhome
# mkdir -p /u01/app/oracle
# mkdir -p /u01/app/oracle/product/11.2.0/dbhome_1
```

4 Create file systems with the volumes `crsbinvol` and `orabinvol`:

```
# mkfs -F vxfs /dev/vx/rdsk/bindg_galaxy/crsbinvol
# mkfs -F vxfs /dev/vx/rdsk/bindg_galaxy/orabinvol
```

5 Mount the file systems. Perform this step on each node.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# mount -F vxfs /dev/vx/dsk/bindg_galaxy/crsbinvol \
/u01/app/oracle/product/10.2.0/crshome
# mount -F vxfs /dev/vx/dsk/bindg_galaxy/orabinvol \
/u01/app/oracle/product/10.2.0/dbhome_1
```

For Oracle RAC 11g Release 2:

```
# mount -F vxfs /dev/vx/dsk/bindg_galaxy/crsbinvol \
/u01/app/grid/product/11.2.0/gridhome
# mount -F vxfs /dev/vx/dsk/bindg_galaxy/orabinvol \
/u01/app/oracle/product/11.2.0/dbhome_1
```

6 Set appropriate ownership and permissions for the directories.

Note: For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: The ownership and permissions must be changed on all nodes of the cluster because `/u01/app/oracle` must be owned by oracle:oinstall, otherwise `/u01/app/oracle/oraInventory` does not get created correctly on all the nodes. This can cause the Oracle Universal Installer to fail.

For Oracle RAC 11g Release 2: The ownership and permissions must be changed on all nodes of the cluster because `/u02/app` must be owned by grid:oinstall, otherwise `/u02/app/oraInventory` does not get created correctly on all the nodes. This can cause the Oracle Universal Installer to fail.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# chown -R oracle:oinstall /u01/app
# chmod -R 775 /u01/app
```

For Oracle RAC 11g Release 2:

```
# chown -R grid:oinstall /u01/app
# chmod -R 775 /u01/app
# chown -R oracle:oinstall /u01/app/oracle
# chmod -R 775 /u01/app/oracle
```

7 Add the resources to the VCS configuration.

See "To add the storage resources created on VxFS to the VCS configuration" on page 313.

8 Repeat all the steps on each node of the cluster.

To add the storage resources created on VxFS to the VCS configuration

1 Change the permissions on the VCS configuration file:

```
# haconf -makerw
```

2 Configure the VxVM volumes under VCS:

```
# hares -add bin_dg DiskGroup cvm
# hares -modify bin_dg DiskGroup bindg_galaxy -sys galaxy
# hares -modify bin_dg DiskGroup bindg_nebula -sys nebula
# hares -modify bin_dg Enabled 1
```

3 Set up the file system under VCS:

```
# hares -add crsbin_mnt Mount cvm
```

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# hares -modify crsbin_mnt MountPoint \
"/u01/app/oracle/product/10.2.0/crshome"
```

For Oracle RAC 11g Release 2:

```
# hares -modify crsbin_mnt MountPoint \
"/u01/app/grid/product/11.2.0/gridhome"
```

The following commands are common to all Oracle RAC versions:

```
# hares -modify crsbin_mnt BlockDevice \
"/dev/vx/dsk/bindg_galaxy/crsbinvol" -sys galaxy
# hares -modify crsbin_mnt BlockDevice \
"/dev/vx/dsk/bindg_nebula/crsbinvol" -sys nebula
# hares -modify crsbin_mnt FSType vxfs
# hares -modify crsbin_mnt FsckOpt "-y"
# hares -modify crsbin_mnt Enabled 1
# hares -add orabin_mnt Mount cvm
```

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# hares -modify orabin_mnt MountPoint \
"/u01/app/oracle/product/10.2.0/dbhome_1"
```

For Oracle RAC 11g Release 2:

```
# hares -modify orabin_mnt MountPoint \
"/u01/app/oracle/product/11.2.0/dbhome_1"
```

The following commands are common to all Oracle RAC versions:

```
# hares -modify orabin_mnt BlockDevice \
"/dev/vx/dsk/bindg_galaxy/orabinvol" -sys galaxy
# hares -modify orabin_mnt BlockDevice \
"/dev/vx/dsk/bindg_nebula/orabinvol" -sys nebula
# hares -modify orabin_mnt FSType vxfs
# hares -modify orabin_mnt FsckOpt "-n"
# hares -modify orabin_mnt Enabled 1
```

4 Link the parent and child resources:

```
# hares -link crsbin_mnt bin_dg
# hares -link orabin_mnt bin_dg
```

To create the file system and directories on cluster file system for Oracle Grid Infrastructure and Oracle database

Perform the following steps on the CVM master node in the cluster.

1 As the root user, create a VxVM shared disk group `bindg`:

```
# vxdg -s init bindg Disk_1
```

2 Set the activation mode for the disk group on all the nodes:

```
# vxdg -g bindg set activation=sw
```

3 From the CVM master node, start the disk group:

```
# vxvol -g bindg startall
```

4 Create separate volumes for Oracle Clusterware/Oracle Grid Infrastructure (`crsbinvol`) and Oracle database (`orabinvol`):

```
# vxassist -g bindg make crsbinvol 5G
# vxassist -g bindg make orabinvol 7G
```

5 Create the following directories for Oracle. The file system and directories created on shared storage in this procedure are based on the following layout:

$ORACLE_BASE	*/u01/app/oracle* /u01/app/oracle is on local storage. For Oracle RAC 11g Release 2, create a separate Oracle base directory for the grid user, in addition to the directory for the Oracle user: */u01/app/gridbase* /u01/app/gridbase is on local storage.
$CRS_HOME (For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1)	*/u01/app/oracle/product/10.2.0/crshome* /u01/app/oracle/product/10.2.0 is on local storage. /u01/app/oracle/product/10.2.0/crshome is on shared storage.
$GRID_HOME (For Oracle RAC 11g Release 2)	*/u01/app/grid/product/11.2.0/gridhome* /u01/app/grid/product/11.2.0 is on local storage. /u01/app/grid/product/11.2.0/gridhome is on shared storage.
$ORACLE_HOME	*/u01/app/oracle/product/release/dbhome_1* where *release* is 10.2.0, 11.1.0, or 11.2.0 depending on the Oracle RAC version /u01/app/oracle/product/*release* is on local storage. /u01/app/oracle/product/*release*/dbhome_1 is on shared storage.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# mkdir -p /u01/app/oracle
# mkdir -p /u01/app/oracle/product/10.2.0/crshome
# mkdir -p /u01/app/oracle/product/10.2.0/dbhome_1
```

For Oracle RAC 11g Release 2:

```
# mkdir -p /u01/app/gridbase
# mkdir -p /u01/app/grid/product/11.2.0/gridhome
# mkdir -p /u01/app/oracle
# mkdir -p /u01/app/oracle/product/11.2.0/dbhome_1
```

6 Create file systems with the volumes `crsbinvol` and `orabinvol`:

```
# mkfs -F vxfs /dev/vx/rdsk/bindg/crsbinvol
# mkfs -F vxfs /dev/vx/rdsk/bindg/orabinvol
```

7 Mount the file systems. Perform this step on each node.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# mount -F vxfs -o cluster /dev/vx/dsk/bindg/crsbinvol \
/u01/app/oracle/product/10.2.0/crshome
# mount -F vxfs -o cluster /dev/vx/dsk/bindg/orabinvol \
/u01/app/oracle/product/10.2.0/dbhome_1
```

For Oracle RAC 11g Release 2:

```
# mount -F vxfs -o cluster /dev/vx/dsk/bindg/crsbinvol \
/u01/app/grid/product/11.2.0/gridhome
# mount -F vxfs -o cluster /dev/vx/dsk/bindg/orabinvol \
/u01/app/oracle/product/11.2.0/dbhome_1
```

8 Change the ownership and permissions on all nodes of the cluster.

Note: For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: The ownership and permissions must be changed on all nodes of the cluster because `/u01/app/oracle` must be owned by oracle:oinstall, otherwise `/u01/app/oracle/oraInventory` does not get created correctly on all the nodes. This can cause the Oracle Universal Installer to fail.

For Oracle RAC 11g Release 2: The ownership and permissions must be changed on all nodes of the cluster because `/u01/app` must be owned by grid:oinstall, otherwise `/u01/app/oraInventory` does not get created correctly on all the nodes. This can cause the Oracle Universal Installer to fail.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# chown -R oracle:oinstall /u01/app
# chmod -R 775 /u01/app
```

For Oracle RAC 11g Release 2:

```
# chown -R grid:oinstall /u01/app
# chmod -R 775 /u01/app
# chown -R oracle:oinstall /u01/app/oracle
# chmod -R 775 /u01/app/oracle
```

9 Add the CVMVolDg and CFSMount resources to the VCS configuration.

See "To add the CFSMount and CVMVolDg resources to the VCS configuration using CLI" on page 319.

To add the CFSMount and CVMVolDg resources to the VCS configuration using CLI

1 Change the permissions on the VCS configuration file:

```
# haconf -makerw
```

2 Configure the CVM volumes under VCS:

```
# hares -add crsorabin_voldg CVMVolDg cvm

# hares -modify crsorabin_voldg Critical 0

# hares -modify crsorabin_voldg CVMDiskGroup bindg

# hares -modify crsorabin_voldg CVMVolume -add crsbinvol

# hares -modify crsorabin_voldg CVMVolume -add orabinvol

# hares -modify crsorabin_voldg CVMActivation sw
```

3 Set up the file system under VCS:

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# hares -add crsbin_mnt CFSMount cvm
# hares -modify crsbin_mnt Critical 0
# hares -modify crsbin_mnt MountPoint \
"/u01/app/oracle/product/10.2.0/crshome"
# hares -modify crsbin_mnt BlockDevice  \
"/dev/vx/dsk/bindg/crsbinvol"
# hares -add orabin_mnt CFSMount cvm
# hares -modify orabin_mnt Critical 0
# hares -modify orabin_mnt MountPoint \
"/u01/app/oracle/product/10.2.0/dbhome_1"
# hares -modify orabin_mnt BlockDevice  \
"/dev/vx/dsk/bindg/orabinvol"
```

For Oracle RAC 11g Release 2:

```
# hares -add crsbin_mnt CFSMount cvm
# hares -modify crsbin_mnt Critical 0
# hares -modify crsbin_mnt MountPoint \
"/u01/app/grid/product/11.2.0/gridhome"
# hares -modify crsbin_mnt BlockDevice  \
"/dev/vx/dsk/bindg/crsbinvol"
# hares -add orabin_mnt CFSMount cvm
# hares -modify orabin_mnt Critical 0
# hares -modify orabin_mnt MountPoint \
"/u01/app/oracle/product/11.2.0/dbhome_1"
# hares -modify orabin_mnt BlockDevice  \
"/dev/vx/dsk/bindg/orabinvol"
```

4 Link the parent and child resources:

```
# hares -link crsorabin_voldg cvm_clus

# hares -link crsbin_mnt crsorabin_voldg

# hares -link crsbin_mnt vxfsckd

# hares -link orabin_mnt crsorabin_voldg

# hares -link orabin_mnt vxfsckd
```

5 Enable the resources:

```
# hares -modify crsorabin_voldg Enabled 1

# hares -modify crsbin_mnt Enabled 1

# hares -modify orabin_mnt Enabled 1

# haconf -dump -makero
```

6 Verify the resource configuration in the main.cf file.

The following is a sample resource configuration for Oracle RAC 11g Release 2:

```
CFSMount crsbin_mnt (
               Critical = 0
               MountPoint = "/u01/app/grid/product/11.2.0/gridhome"
               BlockDevice = "/dev/vx/dsk/bindg/crsbinvol"
               )

CFSMount orabin_mnt (
               Critical = 0
               MountPoint = "/u01/app/oracle/product/11.2.0/dbhome_1"
               BlockDevice = "/dev/vx/dsk/bindg/orabinvol"
               )

CVMVolDg crsorabin_voldg (
              Critical = 0
              CVMDiskGroup = bindg
              CVMVolume = { crsbinvol, orabinvol }
              CVMActivation = sw
              )
crsbin_mnt requires crsorabin_voldg
crsbin_mnt requires vxfsckd
orabin_mnt requires crsorabin_voldg
orabin_mnt requires vxfsckd
crsorabin_voldg requires cvm_clus
```

7 Verify that the resources are online on all systems in the cluster.

```
# hares -state crsorabin_voldg

# hares -state crsbin_mnt

# hares -state orabin_mnt
```

Note: At this point, the crsorabin_voldg resource is reported offline, and the underlying volumes are online. Therefore, you need to manually bring the resource online on each node.

To bring the resource online manually:

```
# hares -online crsorabin_voldg -sys galaxy

# hares -online crsorabin_voldg -sys nebula
```

Setting up user equivalence

You must establish grid user (Oracle RAC 11g Release 2) and Oracle user equivalence on all nodes to allow the Oracle Universal Installer to securely copy files and run programs on the nodes in the cluster without requiring password prompts.

Set up passwordless SSH communication between the cluster nodes for the Oracle user and the grid user.

For more information, see the Oracle documentation.

Setting privileges for the DBA user

Set the privileges for the DBA user.

To set privileges for the DBA user

1 Give the MLOCK privilege to the dba group:

```
# setprivgrp dba MLOCK
```

For Oracle RAC 11g: In addition to MLOCK, give the RTSCHED and RTPRIO privileges to the dba group:

```
# setprivgrp dba RTSCHED

# setprivgrp dba RTPRIO
```

2 Create the `/etc/privgroup` file and add the line:

For Oracle RAC 10g:

```
dba MLOCK
```

For Oracle RAC 11g:

```
dba MLOCK RTSCHED RTPRIO
```

3 Verify the availability of the privileges for the dba group:

```
# /usr/bin/getprivgrp dba
```

Verifying the systems for Oracle RAC installation

Run the SF Oracle RAC installer as described in this section to verify that the cluster configuration settings are conducive for a successful Oracle RAC installation.

Table 17-6 lists the checks performed by the installer on each node. For information on resolving issues that you may encounter during the process, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*, Chapter: Troubleshooting SF Oracle RAC, Section: Troubleshooting installation and configuration check failures.

Table 17-6 List of checks

Check	Description
Time synchronization	The time settings are synchronized across nodes. If the time difference exceeds five seconds, the check fails.

Table 17-6 List of checks *(continued)*

Check	Description
System checks	All the nodes in the cluster have the same architecture. All the nodes in the cluster have the same number and type of processors.
Operating system and patch level checks	All the nodes in the cluster have the same operating system version and patch levels.
Kernel parameter	Verifies that the kernel parameter settings and tunables are in accordance with Oracle RAC recommendations.

Table 17-6 List of checks *(continued)*

Check	Description
LLT checks	The LLT checks are performed on only two links, the first and the last link specified in the `/etc/llttab` file. Verifies that the media speed setting for the links are set to full duplex. If the links are not set to full duplex, the check fails. Verifies that the media speed and auto-negotiation settings are the same across all nodes in the cluster. The check fails if the settings vary across the nodes and if auto-negotiation is enabled for the interface on any node in the cluster. Verifies that the payload (MTU) for the jumbo frames is between 1500 and 9000 bytes. Verifies that this setting is the same for all LLT links in the cluster. The check fails if the value is different for different LLT links in the cluster. Verifies that the links are not cross-connected. If the links are cross-connected, the check fails. Make sure that the links do not have a direct path of communication through switch interconnects. Verifies that the cluster has at least two high-priority links that do not belong to the public network. Verifies that the cluster configuration in the `/etc/llthosts` file is the same on all nodes in the cluster. Verifies that the cluster ID in the `/etc/llttab` file is the same on all the nodes. **Note:** The following checks are skipped if LLT is configured over UDP: LLT links' full duplex setting LLT link jumbo frame setting (MTU) LLT links' cross connection LLT links' speed and auto negotiation settings

Table 17-6 List of checks *(continued)*

Check	Description
I/O fencing checks	Verifies that I/O fencing is enabled on each node in the cluster. **Note:** The verification applies only for disk-based fencing. Verifies that all nodes in the cluster have registered keys with the coordinator disks. If registration keys are missing for any node in the cluster, the check fails for that node. The possible causes for check failure are: ■ Fencing is not configured on the cluster. ■ Fencing is configured in disabled mode. ■ Fencing is configured using CPS.
ODM checks	Verifies that port d is up and running on the nodes.The check fails if the port is not up. The possible causes for check failure are: ■ ODM is not running in the cluster. ■ ODM is running in standalone mode.
VCSMM checks	Verifies that port o is up and running on the nodes.The check fails if port o is not up.
GAB checks	Verifies that the ports a, b, d, f, h, o, v, w are up and running on the nodes. The check fails if any of the SF Oracle RAC components are not running.
LMX checks	Verifies that the LMX helper thread is disabled. The check fails if the helper thread is enabled.

To verify the systems for Oracle RAC installation

1 Start the SF Oracle RAC installer:

```
# cd /opt/VRTS/install

# ./installsfrac -configure galaxy nebula
```

2 Enter **2** to select the option **SF Oracle RAC Installation and Configuration Checks**.

```
1)  Configure SF Oracle RAC sub-components
2)  SF Oracle RAC Installation and Configuration Checks
3)  Prepare to Install Oracle
4)  Install Oracle Clusterware/Grid Infrastructure and Database
5)  Post Oracle Installation Tasks
6)  Exit SF Oracle RAC Configuration
Choose option: [1-6,q] (1) 2
```

The installer displays the location of the temporary log file and starts the verification process.

3 Enter **n** to return to the menu.

```
Is Oracle installed on the system(s) [y,n,q] (y) n
```

Chapter 18

Installing Oracle RAC

This chapter includes the following topics:

- About installing Oracle RAC
- Installing the Oracle Clusterware/Grid Infrastructure software
- Configuring LLT links in the GPnP profile
- Installing the Oracle RAC database software
- Verifying the Oracle Clusterware/Grid Infrastructure and database installation

About installing Oracle RAC

You can install Oracle RAC on shared storage or locally on each node.

Use one of the following ways to install Oracle RAC:

SF Oracle RAC installer	The SF Oracle RAC installer starts the installation process and prompts for information that is required by the Oracle Universal Installer. The Oracle Universal Installer launches with these installation values pre-filled and installs Oracle RAC. You need to invoke the SF Oracle RAC installer to start the installation.
Oracle Universal Installer	The Oracle Universal Installer installs Oracle RAC. The installation values must be manually entered at the time of installation. You need to invoke the Oracle Universal Installer to install Oracle RAC.

Response files	The SF Oracle RAC installer supports silent installation of Oracle RAC using its own response files. You need to modify the SF Oracle RAC response files to include the path information of the Oracle RAC software binaries and the Oracle RAC response files. For more information and instructions: See "About response files" on page 371. For instructions, see the chapter "Installing Oracle RAC using a response file" in this document.

Before you start the installation:

- Keep the Oracle worksheets handy as you perform the installation tasks.
  See "Required installation information for Oracle Clusterware/Grid Infrastructure" on page 599.
  See "Required installation information for Oracle database" on page 603.
- Review your Oracle installation manuals and the appropriate Oracle support Web sites for additional information required during the installation.

Installing the Oracle Clusterware/Grid Infrastructure software

This section provides instructions for installing Oracle Clusterware/Grid Infrastructure using the SF Oracle RAC installer. The SF Oracle RAC installer prompts for information required to invoke the Oracle Universal Installer and launches it. The responses provided to the SF Oracle RAC installer are pre-filled in the Oracle Universal Installer wizard. When you step through the installation, review or change these installation values in the Oracle Universal Installer.

Note: Before you begin the installation, verify that the nodes in the cluster are connected with network links using similar network devices. For example, if you use lan0 as a public link on one node in the cluster, all other nodes in the cluster must also use lan0 as the public link. Similarly, if you use lan1 as a private link on one node in the cluster, all other nodes in the cluster must also use lan1 as the private link.

Oracle Clusterware/Grid Infrastructure software is installed on each node in the CRS_HOME or GRID_HOME location, depending on the version of Oracle RAC you install.

Note: If you want to install Oracle Clusterware/Grid Infrastructure on VxFS or CFS, make sure that you created the appropriate storage before proceeding with the installation.

See "Creating Oracle Clusterware/Grid Infrastructure and Oracle database home directories manually" on page 308.

Note: If you want to pass any arguments to the Oracle Universal Installer, then set up the OUI_ARGS environment variable. You must perform this step before you start the SF Oracle RAC installer.

Refer to the Oracle documentation for details on the arguments that you can pass to the Oracle Universal Installer.

For example: `# export OUI_ARGS=-ignoreSysPrereqs`

Install the software using one of the following methods:

SF Oracle RAC installer	See "Installing Oracle Clusterware/Grid Infrastructure using the SF Oracle RAC installer" on page 331.
Oracle Universal Installer	See "Installing Oracle Clusterware/Grid Infrastructure using the Oracle Universal Installer" on page 334.

Installing Oracle Clusterware/Grid Infrastructure using the SF Oracle RAC installer

The SF Oracle RAC installer performs the following tasks:

- Invokes the Oracle Universal Installer to install Oracle Clusterware/Grid Infrastructure
- Verifies the Oracle Oracle Clusterware/Grid Infrastructure installation

To install Oracle Clusterware/Grid Infrastructure using the SF Oracle RAC installer

1 Make sure that you completed the required pre-installation steps.

2 Return to the following SF Oracle RAC installer menu and select the option **Install Oracle Clusterware/Grid Infrastructure and Database**.

```
1)  Configure SF Oracle RAC sub-components
2)  SF Oracle RAC Installation and Configuration Checks
3)  Prepare to Install Oracle
4)  Install Oracle Clusterware/Grid Infrastructure and Database
5)  Post Oracle Installation Tasks
6)  Exit SF Oracle RAC Configuration
Choose option: [1-6,q] (1) 4
```

3 Select the option **Install Oracle Clusterware/Grid Infrastructure**.

```
1)  Install Oracle Clusterware/Grid Infrastructure
2)  Install Oracle Database
3)  Exit SF Oracle RAC Configuration
b)  Back to previous menu
Choose option: [1-3,b,q] (1) 1
```

4 Verify that the nodes in the cluster are connected with network links using similar network devices. Review the related information on screen and press **Enter** to confirm.

```
Do you want to continue? [y,n,q] (y)
```

5 Set the DISPLAY environment variable that is required for the Oracle Universal Installer:

```
Enter DISPLAY environment variable: [b] 10.20.12.150:0.0
```

where 10.20.12.150 is the IP address of X client where you want to export the display for the installer.

6 Enter the Oracle UNIX user name. The Oracle UNIX user name was previously set up during the pre-installation process.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
Enter Oracle UNIX user name:  [b] (oracle)
```

For Oracle RAC 11g Release 2:

```
Enter Oracle UNIX user name:  [b] (grid)
```

7 Enter Oracle UNIX group name. The Oracle UNIX group name was previously set up during the pre-installation process.

```
Enter Oracle UNIX group name:  [b] (oinstall)
```

8 Enter the full path of the Oracle base directory.

Note: The ORACLE_BASE directory must be a local directory.

9 Enter the full path of the Oracle Clusterware/Grid Infrastructure home directory.

If the Oracle Clusterware/Grid Infrastructure home directory you specified does not exist, the installer creates the directory locally on each node and sets appropriate permissions for the Oracle user.

10 Enter the full path of the Oracle Clusterware/Grid Infrastructure installation image. Press **Return** to proceed.

The installer detects the version of the Oracle Clusterware/Grid Infrastructure software.

11 Enter **y** to continue with the installation.

12 Review and confirm the configuration information. The installer invokes the Oracle Universal Installer:

13 Enter the required information when prompted by the Oracle Universal Installer.

See "Required installation information for Oracle Clusterware/Grid Infrastructure" on page 599.

14 Review the configuration summary presented by the Oracle Universal Installer. The Oracle Universal Installer begins the Oracle Clusterware/Grid Infrastructure installation.

15 For Oracle RAC versions 10.2.0.3 and earlier, patch the init.cssd script.

- Open another window on the system where you are running the installer.
- Log in as oracle user.
- Change to the directory where the patch is to be copied:

```
$ cd $CRS_HOME/css/admin

$ cp /opt/VRTSvcs/rac/patch/init.cssd-10gR2.patch .
```

- As oracle user, run the following command to install the patch:

```
$ /usr/bin/patch < init.cssd-10gR2.patch init.cssd
```

16 At the end of the Oracle Clusterware/Grid Infrastructure installation, run the following configuration scripts as the root user from each node of the cluster, in the listed order.

- `orainstRoot.sh` (located in the `oraInventory` directory)
  Make sure the script exists on each node before proceeding.
- `root.sh` (located in the CRS_HOME or GRID_HOME directory, depending on your Oracle RAC version)

Do not run the scripts simultaneously on the cluster nodes.

Note: For Oracle RAC 10g Release 2: If vipca fails to run silently, run the script manually on one of the nodes as the root user.

```
# export DISPLAY=10.20.12.150:0.0
# cd $CRS_HOME/bin
# ./vipca
```

Note: For Oracle RAC 11g Release 2: The Oracle Cluster Verification Utility fails during the installation of the Oracle Grid Infrastructure software. You may ignore this error. This is a known issue with Oracle.

---

17 Return to the Oracle Universal Installer window and click "OK" to continue.

The Oracle Universal Installer informs you that the Oracle Clusterware/Grid Infrastructure installation was successful.

18 Return to the SF Oracle RAC installer and press Return to proceed. The installer verifies whether Oracle Clusterware/Grid Infrastructure is installed properly.

This completes the Oracle Clusterware/Grid Infrastructure installation.

Installing Oracle Clusterware/Grid Infrastructure using the Oracle Universal Installer

This section provides instructions for installing the Oracle Clusterware/Grid Infrastructure software using the Oracle Universal Installer. The software is installed on each node in the Oracle Clusterware/Grid Infrastructure home directory.

To install Oracle Clusterware/Grid Infrastructure using the Oracle Universal Installer

1 Log in as the Oracle grid user (Oracle RAC 11g Release 2) or the Oracle user. On the first node, set the DISPLAY variable.

- For Bourne Shell (bash), type:

```
$ DISPLAY=10.20.12.150:0.0;export DISPLAY
```

  where 10.20.12.150 is the IP address of X client where you want to export the display for the installer.

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

```
$ setenv DISPLAY 10.20.12.150:0.0
```

  where 10.20.12.150 is the IP address of X client where you want to export the display for the installer.

2 Start the Oracle Universal Installer on the first node.

```
$ cd /dvd_mount

$ ./runInstaller
```

3 Enter the required information when prompted by the Oracle Universal Installer.

See "Required installation information for Oracle Clusterware/Grid Infrastructure" on page 599.

4 Review the configuration summary presented by the Oracle Universal Installer. The Oracle Universal Installer begins the Oracle Clusterware/Grid Infrastructure installation.

Note: For Oracle RAC 11g Release 2: If you want to save the Oracle Grid Infrastructure installation configuration into a response file for future installations, click the **Save Response File** option on the Summary page of the Oracle Universal Installer.

---

5 For Oracle RAC versions 10.2.0.3 and earlier, patch the init.cssd script.

- Open another window on the system where you are running the installer.
- Log in as oracle user.
- Change to the directory where the patch is to be copied:

```
$ cd $CRS_HOME/css/admin
```

```
$ cp /opt/VRTSvcs/rac/patch/init.cssd-10gR2.patch .
```

- As oracle user, run the following command to install the patch:

```
$ /usr/bin/patch < init.cssd-10gR2.patch init.cssd
```

6 Run the orainstRoot.sh script as prompted by the Oracle Universal Installer.

7 Run the root.sh script on each node as prompted by the Oracle Universal Installer:

The Oracle Clusterware daemons are started on the node.

Note: The Oracle Cluster Verification Utility fails during the installation of the Oracle Clusterware/Grid Infrastructure software. You may ignore this error. This is a known issue with Oracle.

Configuring LLT links in the GPnP profile

Perform this step only for Oracle RAC 11g Release 2 installations.

Update the GPnP profile to include the remaining LLT links that were not added to the profile during the Oracle Grid Infrastructure installation.

To configure the LLT links in the GPnP profile

1 View the currently configured interfaces:

```
# $GRID_HOME/bin/oifcfg getif
lan0 10.2.156.0         global      public
lan1 192.168.12.0       global      cluster_interconnect
```

The interfaces that are currently stored in the GPnP profile, their subnets, and their role (public or cluster_interconnect) are displayed.

2 Add the remaining LLT links to the GPnP profile:

```
# $GRID_HOME/bin/oifcfg setif -global \
lan2/192.168.12.0:cluster_interconnect
```

If you are using multiple IP addresses on different subnet for cluster interconnect (for load balancing), add the remaining interface subnets to the GPnP profile.

```
# $GRID_HOME/bin/oifcfg setif -global \
lan2/192.168.2.0:cluster_interconnect
# $GRID_HOME/bin/oifcfg setif -global \
lan1/192.168.2.0:cluster_interconnect
```

3 Verify that the correct interface subnet is in use:

```
# $GRID_HOME/bin/oifcfg getif
lan0 10.2.156.0         global      public
lan1 192.168.12.0       global      cluster_interconnect
lan2 192.168.12.0       global      cluster_interconnect
lan1 192.168.2.0        global      cluster_interconnect
lan2 192.168.2.0        global      cluster_interconnect
```

Make sure all the LLT links are configured and listed in the GPnP profile.

Installing the Oracle RAC database software

Before you start the installation of Oracle database, make sure that Oracle Clusterware/Grid Infrastructure is up and running. Symantec recommends you to install the Oracle database locally on each node.

Note: Make sure any required HP-UX patches listed in the Oracle documentation are installed before you install the Oracle software.

Note: If you want to install Oracle database on VxFS or CFS, make sure that you created the appropriate storage before proceeding with the installation.

See "Creating Oracle Clusterware/Grid Infrastructure and Oracle database home directories manually" on page 308.

Install the software using one of the following methods:

SF Oracle RAC installer	See "Installing the Oracle RAC database using the SF Oracle RAC installer" on page 338.
Oracle Universal Installer	See "Installing the Oracle RAC database using the Oracle Universal Installer" on page 340.

Installing the Oracle RAC database using the SF Oracle RAC installer

The SF Oracle RAC installer performs the following tasks:

- Verifies the status of Oracle Clusterware/Grid Infrastructure on all nodes
- Invokes the Oracle Universal Installer to install the Oracle database
- Verifies the Oracle RAC database installation

To install the Oracle RAC database

1 Return to the SF Oracle RAC installer and type **4** to select the option **Install Oracle Clusterware/Grid Infrastructure and Database**.

```
1)  Configure SF Oracle RAC sub-components
2)  SF Oracle RAC Installation and Configuration Checks
3)  Prepare to Install Oracle
4)  Install Oracle Clusterware/Grid Infrastructure and Database
5)  Post Oracle Installation Tasks
6)  Exit SF Oracle RAC Configuration
Choose option: [1-6,q] (1) 4
```

2 Select the option **Install Oracle Database**.

```
1)  Install Oracle Clusterware/Grid Infrastructure
2)  Install Oracle Database
3)  Exit SF Oracle RAC Configuration
b)  Back to previous menu
Choose option: [1-3,b,q] (1) 2
```

3 Set the DISPLAY environment variable that is required for the Oracle Universal Installer.

```
Enter the DISPLAY environment variable: [b] 10.20.12.150:0.0
```

4 Enter Oracle UNIX user name. The Oracle UNIX user name was previously set up during the pre-installation process.

```
Enter Oracle UNIX user name:  [b] (oracle)
```

5 Enter Oracle UNIX group name. The Oracle UNIX group name was previously set up during the pre-installation process.

```
Enter Oracle UNIX group name:  [b] (oinstall)
```

6 Enter the full path of the Oracle base directory.

```
Enter absolute path of Oracle Base directory: [b]
```

7 Enter the full path of the Oracle Clusterware/Grid Infrastructure home directory.

```
Enter absolute path of Oracle Clusterware/Grid Infrastructure
Home directory: [b]
```

8 Enter the full path of the Oracle database home directory.

```
Enter absolute path of Oracle Database Home directory: [b]
```

If the Oracle RAC database home directory you specified does not exist, the installer creates the directory locally on each node and sets appropriate permissions for the Oracle user.

9 Enter the full path of the database installation image.

```
Enter absolute path of Oracle Database install image: [b]
```

The installer determines the version of the Oracle software from the binaries.

10 Enter **y** to proceed with the installation.

11 Review and confirm the configuration information.

The installer verifies that Oracle Clusterware/Grid Infrastructure is running and invokes the Oracle Universal Installer:

12 Enter the required information when prompted by the Oracle Universal Installer.

See "Required installation information for Oracle database" on page 603.

13 Review the configuration summary presented by the Oracle Universal Installer. The Oracle Universal Installer begins the Oracle database installation.

14 Run the root.sh script as the root user on the cluster nodes:

Return to the Oracle Universal Installer window and click "OK" to continue.

15 Return to the SF Oracle RAC installer and press **Return** to continue. The installer verifies the Oracle database installation.

Note: Symantec recommends you to relink the SF Oracle RAC libraries only after completing all the required patch additions.

Installing the Oracle RAC database using the Oracle Universal Installer

The following procedure describes how to install the Oracle RAC database using the Oracle Universal Installer. Symantec recommends that you install the Oracle RAC database locally on each node.

To install Oracle RAC database using the Oracle Universal Installer

1 Log in as the Oracle user. On the first node, set the DISPLAY variable.

- For Bourne Shell (bash), type:

```
$ DISPLAY=10.20.12.150:0.0;export DISPLAY
```

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

```
$ setenv DISPLAY 10.20.12.150:0.0
```

2 Start the Oracle Universal Installer.

```
$ cd /dvd_mount

$ ./runInstaller
```

3 Enter the required information when prompted by the Oracle Universal Installer.

See "Required installation information for Oracle database" on page 603.

4 Review the configuration summary presented by the Oracle Universal Installer.

Note: For Oracle RAC 11g Release 2: If you want to save the Oracle RAC database installation configuration into a response file for future installations, click the **Save Response File** option on the Summary page of the Oracle Universal Installer.

The Oracle Universal Installer begins the Oracle database installation.

5 Run the root.sh script as prompted by the Oracle Universal Installer.

```
# cd $ORACLE_HOME

# ./root.sh
```

Verifying the Oracle Clusterware/Grid Infrastructure and database installation

The following procedure verifies the Oracle Clusterware/Grid Infrastructure and Oracle RAC database installation by verifying that the Oracle processes are running on all nodes.

To verify the installation, run the following command from any node in the cluster. Verify in the command output that the Oracle Clusterware/Grid Infrastructure processes are online on the nodes.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# $CRS_HOME/bin/crs_stat -t

Name            Type         Target      State       Host
ora.galaxy.vip  application  ONLINE      ONLINE      galaxy
ora.galaxy.gsd  application  ONLINE      ONLINE      galaxy
ora.galaxy.ons  application  ONLINE      ONLINE      galaxy
ora.nebula.vip  application  ONLINE      ONLINE      nebula
ora.nebula.gsd  application  ONLINE      ONLINE      nebula
ora.nebula.ons  application  ONLINE      ONLINE      nebula
```

For Oracle RAC 11g Release 2:

```
# $GRID_HOME/bin/crsctl stat res -t
```

```
--------------------------------------------------------------
NAME           TARGET  STATE     SERVER    STATE_DETAILS
--------------------------------------------------------------
Local Resources
--------------------------------------------------------------
ora.LISTENER.lsnr
               ONLINE  ONLINE    galaxy
               ONLINE  ONLINE    nebula
ora.asm
               OFFLINE OFFLINE   galaxy
               OFFLINE OFFLINE   nebula

.
.
.
--------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------
ora.LISTENER_SCAN1.lsnr
      1        ONLINE  ONLINE       nebula
ora.LISTENER_SCAN2.lsnr
      1        ONLINE  ONLINE       galaxy
ora.LISTENER_SCAN3.lsnr
      1        ONLINE  ONLINE       galaxy
.
.
.
```

To verify the Oracle RAC database installation, check the oraInventory logs located in the ORACLE_BASE directory.

Node numbering discrepancies in Oracle RAC 11g Release 2

For Oracle RAC 11g Release 2, you will observe that the output of the `lsnodes` command (used to obtain membership information from SF Oracle RAC) and the `olsnodes` command (used to obtain membership information from Oracle Grid Infrastructure) differ. Oracle RAC starts the count at 1 while SF Oracle RAC starts the count at 0.

For example, in a two-node cluster:

The `lsnodes` command produces the following output:

```
# lsnodes -n
Node1         0
Node2         1
```

The `olsnodes` command produces the following output:

```
# olsnodes -n
Node1         1
Node2         2
```

In previous Oracle RAC releases (starting with Oracle RAC 10g Release 1), the commands produced the same output unless there were configuration issues in the cluster. Whenever node numbering discrepancies were observed, further issues were seen in the cluster.

However, the discrepancy in node numbering in Oracle RAC 11g Release 2 is conformant with the design change in Oracle Grid Infrastructure. It does not indicate any configuration issues in the cluster.

Chapter 19

Performing Oracle RAC post-installation tasks

This chapter includes the following topics:

- Adding Oracle RAC patches or patchsets
- Configuring the CSSD resource
- Preventing automatic startup of Oracle Clusterware/Grid Infrastructure
- Relinking the SF Oracle RAC libraries with Oracle RAC
- Creating the Oracle RAC database
- Adding Oracle UDP IPC private IP addresses to the Oracle initialization parameter file
- Preventing automatic database startup
- Configuring VCS service groups for Oracle RAC
- Removing permissions for communication
- Configuring the SFDB repository database after installation

Adding Oracle RAC patches or patchsets

To install the required patches or patchsets, review the notes that accompany the patch or patchset.

Before installing any Oracle RAC patch or patchset software:

- Review the latest information on supported Oracle RAC patches and patchsets: http://www.symantec.com/docs/TECH44807

- You must have installed the base version of the Oracle RAC software.

Configuring the CSSD resource

You must configure the CSSD resource to ensure that the CSSD dependencies on the resources that manage OCR and voting disk and the private IP address are satisfied before Oracle Clusterware/Grid Infrastructure starts.

Note: It is mandatory to use CSSD agent in SF Oracle RAC installations. Using the CSSD agent ensures adequate handling of inter-dependencies, thus preventing the premature startup of Oracle Clusterware/Grid Infrastructure, which causes cluster failures.

Use one of the following ways to configure the CSSD resource:

SF Oracle RAC installer	See "Configuring the CSSD resource using the SF Oracle RAC installer" on page 346.
Manual	See "Configuring the CSSD resource manually" on page 348.

Configuring the CSSD resource using the SF Oracle RAC installer

Configure the CSSD resource using the SF Oracle RAC installer if the OCR and voting disk storage is configured on CVM raw volumes or CFS.

Note: If the OCR and voting disk storage is configured on ASM disk groups, configure the CSSD resource manually.

Before you configure the CSSD resource, make sure that the following requirements are satisfied:

1. Oracle Clusterware/Grid Infrastructure is up and running.
2. OCR and voting disk is configured on CVM raw volumes or CFS and managed by VCS.
3. The private IP address for Oracle Clusterware/Grid Infrastructure is configured under the PrivNIC or MultiPrivNIC resource in the same VCS group as that of OCR and voting disk.

Note: The SF Oracle RAC installer configures the OCR, voting disk, and PrivNIC/MultiPrivNIC resources in the cvm group. If you configured one of these resources manually, make sure that these resources are placed in the cvm group. If the resources are not in the same group, configure the the CSSD resource manually.

See "Configuring the CSSD resource manually" on page 348.

The installer performs the following configuration tasks:

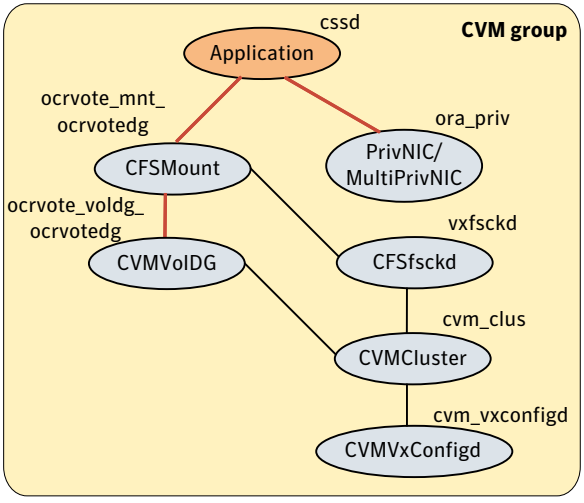
- Adds the CSSD resource to the VCS configuration in the cvm group.

Note: If the CSSD resource already exists, the installer enables reconfiguration of the resource by deleting the existing resource.

- Sets the dependency of the CSSD resource on the PrivNIC or MultiPrivNIC resource that manages the private IP address for Oracle Clusterware/Grid Infrastructure.
- Sets the dependency of the CSSD resource on the CFSMount or CVMVolDg resources that manage OCR and voting disk.
- Enables the CSSD resource and saves the new configuration.

Figure 19-1 illustrates the configuration performed by the SF Oracle RAC installer. In the figure, the CSSD resource is configured under the CVM group.

Figure 19-1 CSSD configuration by SF Oracle RAC installer



To configure the CSSD resource

1. Start the SF Oracle RAC installer, if it is not already running. Select the option **Post Oracle Installation Tasks**.

```
1)  Configure SF Oracle RAC sub-components
2)  SF Oracle RAC Installation and Configuration Checks
3)  Prepare to Install Oracle
4)  Install Oracle Clusterware/Grid Infrastructure and Database
5)  Post Oracle Installation Tasks
6)  Exit SF Oracle RAC Configuration
Choose option: [1-6,q] (1) 5
```

2. Select the option **Configure CSSD agent**.

   The installer verifies that Oracle Clusterware/Grid Infrastructure is running on all the nodes.

3. Press **Return** to continue with the configuration. The installer reads the resource and group mappings for the CSSD agent from the VCS configuration file and displays the information.

4. Enter **y** to continue with the configuration. Review the messages as the installer configures the CSSD agent and sets the appropriate dependencies.

5. Press **Return** to return to the installer menu.

6. If the Oracle Clusterware/Grid Infrastructure and the Oracle database binaries are on CFS, set the dependencies between the cssd resource and the CFSMount resources for the binaries manually:

```
# hares -link cssd crsbin_mnt
# hares -link cssd orabin_mnt
```

Configuring the CSSD resource manually

Add the `cssd` resource to the VCS configuration and set CSSD dependencies on the resources that manage OCR and voting disk and the private IP addresses for Oracle Clusterware/Grid Infrastructure.

Note: It is recommended that the OCR, voting disk, and PrivNIC/MultiPrivNIC resources be configured in the same VCS group as that of the cssd resource. If the resources are not in the same group, set the appropriate dependencies between the service groups.

To configure the CSSD resource

1 Change the permission on the VCS configuration file to read-write mode:

```
# haconf -makerw
```

2 Add the CSSD resource to the cvm group:

```
# hares -add cssd Application cvm
```

3 Modify the CSSD resource attributes:

```
# hares -modify cssd StartProgram /opt/VRTSvcs/rac/bin/cssd-online
# hares -modify cssd StopProgram  /opt/VRTSvcs/rac/bin/cssd-offline
# hares -modify cssd MonitorProgram /opt/VRTSvcs/rac/bin/cssd-monitor
# hares -modify cssd CleanProgram /opt/VRTSvcs/rac/bin/cssd-clean
# hares -modify cssd Critical 0
# hares -override cssd OnlineWaitLimit
# hares -modify cssd OnlineWaitLimit 5
```

4 Enable the CSSD resource:

```
# hares -modify cssd Enabled 1
```

5 Set the dependency of the CSSD resource on the CFSMount or CVMVolDg resources that manage OCR and voting disk.

If you configured OCR and voting disk on CVM raw volumes:

```
# hares -link cssd ocr_voldg_ocrvotedg

# hares -link cssd vote_voldg_ocrvotedg
```

If you configured OCR and voting disk on CFS:

```
# hares -link cssd ocrvote_mnt_ocrvotedg
```

6 Set the dependency of the CSSD resource on the PrivNIC or MultiPrivNIC resources that manage the private IP address for Oracle Clusterware/Grid Infrastructure.

If you configured the PrivNIC or MultiPrivNIC resource:

```
# hares -link cssd resource_name
```

where *resource_name* is the name of the PrivNIC or MultiPrivNIC resource.

7 If the Oracle Clusterware/Grid Infrastructure and the Oracle database binaries are on CFS, set the dependencies between the CSSD resource and the CFSMount resources for the binaries manually:

```
# hares -link cssd crsbin_mnt
# hares -link cssd orabin_mnt
```

8 Change the permission on the VCS configuration file to read-only mode:

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

Preventing automatic startup of Oracle Clusterware/Grid Infrastructure

The use of the CSSD agent is mandatory to ensure adequate handling of service group inter-dependencies and thereby prevent the premature startup of Oracle Clusterware/Grid Infrastructure. Therefore, disable automatic startup of Oracle Clusterware/Grid Infrastructure when the system starts.

To prevent automatic startup of Oracle Clusterware/Grid Infrastructure

1 Log in as the root user on each node in the cluster.

2 Disable automatic startup of Oracle Clusterware/Grid Infrastructure.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# $CRS_HOME/bin/crsctl disable crs
```

For Oracle RAC 11g Release 2:

```
# $GRID_HOME/bin/crsctl disable crs
```

Relinking the SF Oracle RAC libraries with Oracle RAC

If you added or upgraded the Oracle patches, you must relink the SF Oracle RAC libraries to Oracle. If you are using Oracle RAC 10g, you need to link Oracle RAC with VCSIPC, VCSMM, and ODM libraries. If you are using Oracle RAC 11g, you need to link Oracle RAC with VCSMM and ODM libraries. Relinking the libraries enables coordinated exchange of cluster membership information and protection of data.

Note: Symantec recommends that you relink the SF Oracle RAC libraries only after completing all the required patch additions.

Use one of the following ways to relink the libraries:

SF Oracle RAC installer	See "Relinking the SF Oracle RAC libraries with Oracle RAC using the SF Oracle RAC installer" on page 351.
Manual	See "Relinking the SF Oracle RAC libraries with Oracle RAC manually" on page 352.

Relinking the SF Oracle RAC libraries with Oracle RAC using the SF Oracle RAC installer

Perform the steps in the following procedure to relink the libraries using the SF Oracle RAC installer.

To relink the SF Oracle RAC libraries with Oracle RAC

1 Return to the SF Oracle RAC installer menu, and select the option **Post Oracle Installation**.

```
1)  Configure SF Oracle RAC sub-components
2)  SF Oracle RAC Installation and Configuration Checks
3)  Prepare to Install Oracle
4)  Install Oracle Clusterware/Grid Infrastructure and Database
5)  Post Oracle Installation Tasks
6)  Exit SF Oracle RAC Configuration
Choose option: [1-6,q] (1) 5
```

2 Select the option **Relink Oracle Database Binary**.

3 Provide the Oracle environment information—user name, group name, CRS_HOME (or GRID_HOME), ORACLE_HOME. Based on this information, the installer detects the version of Oracle installed.

Note: You need to provide the Oracle environment information only if you quit the installer after installing Oracle Clusterware/Grid Infrastructure and the Oracle database.

```
Enter Oracle UNIX user name: [b] oracle
Enter Oracle UNIX group name: [b] (oinstall)
Enter absolute path of Oracle Clusterware/Grid Infrastructure
Home directory: [b]
Enter absolute path of Oracle Database Home directory: [b]
.
.
Do you want to continue? [y,n,q] (y)
```

4 Review and confirm the Oracle database information.

The installer starts relinking the libraries.

Relinking the SF Oracle RAC libraries with Oracle RAC manually

If you added or upgraded the Oracle patches, you must relink the SF Oracle RAC libraries to Oracle. You must enable Oracle to use the Veritas ODM and cluster membership (VCSMM) libraries.

Note: Symantec recommends that you relink the SF Oracle RAC libraries only after completing all the required patch additions.

To relink the SF Oracle RAC libraries with Oracle RAC, run the following command as the oracle user:

```
$ /opt/VRTSvcs/rac/bin/linkrac oracle_version
```

Where oracle_version is 10gR2, 11gR1, or 11gR2 depending on the version of Oracle RAC you installed.

For example, to relink the SF Oracle RAC libraries with Oracle RAC 11g Release 2, run the following command as the oracle user:

```
$ /opt/VRTSvcs/rac/bin/linkrac 11gR2
```

Verifying whether Oracle uses Veritas libraries

After relinking the libraries, you must verify whether Oracle uses Veritas libraries.

To verify whether Oracle uses Veritas libraries

1 On each node, start the Oracle service group:

```
# hagrp -online oracle_grp -sys node_name
```

2 After starting Oracle instances, confirm that Oracle uses the Veritas libraries.

On each node in the cluster, examine the Oracle alert file, alert_$ORACLE_SID.log, for the following lines:

```
Oracle instance running with ODM: Veritas 5.1 ODM Library,
Version 2.0
```

Additionally, for Oracle RAC 10g, verify that the cluster interconnect IPC version is `VERITAS IPC '5.0.31.0'`.

Creating the Oracle RAC database

Create the Oracle RAC database on shared raw VxVM volumes or shared VxFS file systems. Use your own tools or scripts or review the guidelines on using the Oracle DBCA (Database Creation Assistant) tool to create the database.

For instructions on creating an Oracle RAC database:

See "About creating a test database" on page 653.

For more information, see the Oracle RAC documentation.

Note: If you plan to configure global clusters, then set up the Oracle RAC database only on the primary site. On the secondary site, the database will be replicated.

Note: For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: Make sure that you configure the database for availability if the database cache fusion traffic is configured to use Oracle UDP IPC private IP addresses and if these addresses are configured as a PrivNIC or MultiPrivNIC resource.

See "Adding Oracle UDP IPC private IP addresses to the Oracle initialization parameter file" on page 354.

Adding Oracle UDP IPC private IP addresses to the Oracle initialization parameter file

Perform this step only for Oracle RAC 10 Release 2/Oracle RAC 11 Release 1 installations.

Add the Oracle UDP IPC private IP addresses to the Oracle initialization parameter file (for example, `pfile` or `spfile`) if the database cache fusion traffic is configured to use Oracle UDP IPC private IP addresses and if these addresses are configured as a PrivNIC or MultiPrivNIC resource for high availability. You need to configure the `cluster_interconnects` parameter in the Oracle initialization parameter file to use the appropriate private IP addresses.

To add Oracle UDP IPC private IP addresses to the initialization parameter file

1. Log in as the Oracle user on one of the nodes in the cluster.
2. Set the `cluster_interconnects` parameter in the Oracle initialization parameter file to use the Oracle UDP IPC private IP addresses that are used for database cache fusion and are managed by PrivNIC or MultiPrivNIC.

   Note: Configure multiple IP addresses for each database instance in the `cluster_interconnects` parameter to distribute the database cache fusion traffic across multiple links.

   ```
   $ sqlplus '/ as sysdba'

   SQL> alter system set cluster_interconnects='192.168.2.1:192.168.3.1' \
   scope=spfile sid='vrts1';
   SQL> alter system set cluster_interconnects='192.168.2.2:192.168.3.2' \
   scope=spfile sid='vrts2';
   SQL> exit;
   ```

3. Stop the Oracle database on all nodes:

   If the database is configured under VCS:

   ```
   # hares -offline oracle_resource -sys system_name
   ```

   If the database is not configured under VCS:

   ```
   $ srvctl stop database -d db-name
   ```

4 For Oracle RAC 10g: Unlink the Veritas VCS IPC library.

Perform this step on each node if the Oracle libraries are on local storage. If the Oracle libraries are installed on shared storage, perform the step on one node only.

```
$ cd $ORACLE_HOME/rdbms/lib

$ make -f ins_rdbms.mk ioracle
```

5 As the Oracle user on one of the nodes in the cluster, restart the Oracle database:

```
$ srvctl start database -d db-name
```

6 As the root user on each node in the cluster, verify that the private IP addresses are running.

```
# ifconfig lan1
```

Preventing automatic database startup

Configure the Oracle RAC database for manual startup if you want the Oracle RAC database to be managed by VCS using the Oracle agent. Before you configure the VCS service groups for Oracle, you need to prevent the Oracle database from starting automatically. The Oracle Clusterware/Grid Infrastructure and Oracle agent may attempt to start the database instance at the same time if the database mount is available. To prevent the Oracle database from starting automatically, you must change the management policy for the database from automatic to manual using the Oracle SRVCTL command. The command changes the AUTO_START attribute of the Oracle database and instance resources.

To prevent automatic database startup

1 Register the database, if not already registered:

```
$ srvctl add database -d db-name -o oracle_home \
-p location-of-parameterfile -y manual
```

2 Once the database is registered, change the management policy for the database to manual:

```
$ srvctl stop database -d db-name
$ srvctl modify database -d db-name -y manual
```

3 Start the database:

```
$ srvctl start database -d db-name
```

Configuring VCS service groups for Oracle RAC

You can set up the Oracle database to be managed by VCS or by Oracle Clusterware/Grid Infrastructure. Symantec recommends that the Oracle database be configured under VCS.

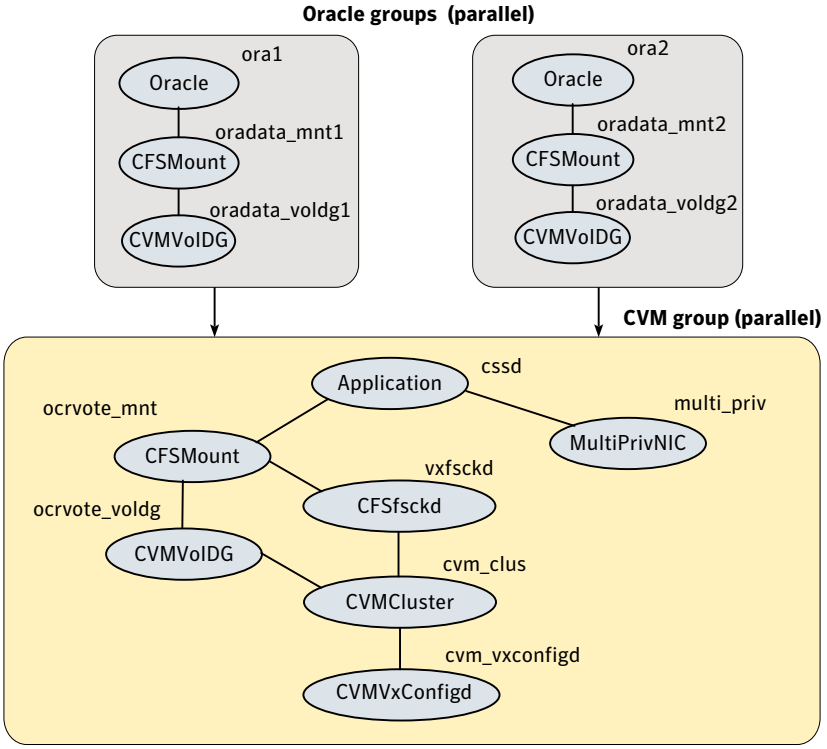
Note: The VCS Oracle agent is supported only for administrator-managed databases. For policy-managed databases, use the service group configuration without the VCS Oracle agent.

When the database is configured under VCS:

- You can choose to configure the service group in a way that insulates all the databases from failure in any of the databases in the group.
- VCS manages the start and stop sequence of the applications and the database.

Figure 19-2 illustrates a service group configuration with the VCS Oracle agent.

Figure 19-2 Service group configuration with the VCS Oracle agent



If your configuration does not use the VCS Oracle agent, you need to modify the existing configuration as illustrated.

Figure 19-3 illustrates a sample configuration in the absence of the VCS Oracle agent for single database configurations.

Figure 19-3 Service group configuration without VCS Oracle agent (single database)

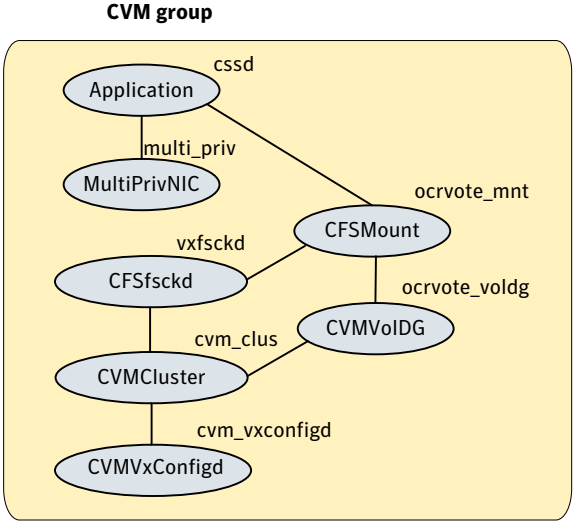
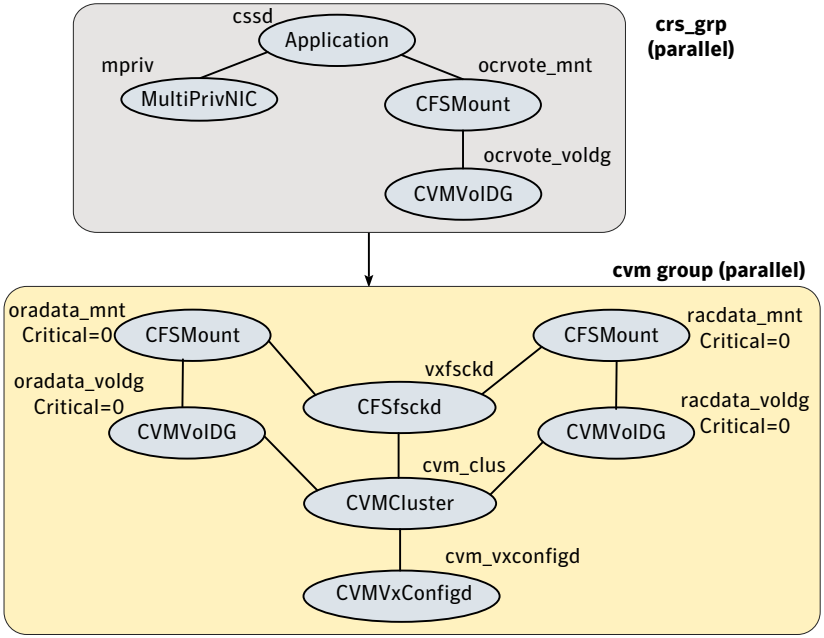


Figure 19-4 illustrates a sample service group configuration in the absence of the VCS Oracle agent for multiple database configurations.

Figure 19-4 Service group configuration without the VCS Oracle agent (multiple databases)



In a service group configuration without the VCS Oracle agent, Oracle Clusterware/Grid Infrastructure controls the database. An online local firm dependency exists between the Oracle Clusterware/Grid Infrastructure group and the CVM group. When the system starts, the CVM group brings up the volume and mount points for the databases. The Oracle Clusterware/Grid Infrastructure group brings up the OCR and voting disk, configures the private IP address for Oracle Clusterware/Grid Infrastructure, and starts Oracle Clusterware/Grid Infrastructure. Oracle Clusterware/Grid Infrastructure starts the database and the application is brought online.

Note: In a service group configuration without the VCS Oracle agent, when the system starts, all volumes and mount points MUST be online for the dependent service groups to be online.

To configure the Oracle database under VCS, create Oracle service groups after installing Oracle RAC and creating a database.

See "Using the CLI to configure VCS service groups for Oracle RAC" on page 360.

Using the CLI to configure VCS service groups for Oracle RAC

This section describes how to configure the Oracle service group using the CLI.

The following procedure assumes that you have created the database.

To configure the Oracle service group using the CLI

1. Change the cluster configuration to read-write mode:

```
# haconf -makerw
```

2. Add the service group to the VCS configuration:

```
# hagrp -add oradb1_grp
```

3. Modify the attributes of the service group:

```
# hagrp -modify oradb1_grp Parallel 1

# hagrp -modify oradb1_grp SystemList galaxy 0  nebula 1

# hagrp -modify oradb1_grp AutoStartList galaxy nebula
```

4. Add the CVMVolDg resource for the service group:

```
# hares -add oradata_voldg CVMVolDg oradb1_grp
```

5. Modify the attributes of the CVMVolDg resource for the service group:

```
# hares -modify oradata_voldg CVMDiskGroup oradatadg
# hares -modify oradata_voldg CVMActivation sw
# hares -modify oradata_voldg CVMVolume oradatavol
```

6. Add the CFSMount resource for the service group:

```
# hares -add oradata_mnt CFSMount oradb1_grp
```

7. Modify the attributes of the CFSMount resource for the service group:

```
# hares -modify oradata_mnt MountPoint "/oradata"
# hares -modify oradata_mnt BlockDevice \
"/dev/vx/dsk/oradatadg/oradatavol"
```

8. Add the Oracle RAC database instance to the service group:

```
# hares -add ora1 Oracle oradb1_grp
```

9 Modify the attributes of the Oracle resource for the service group:

```
# hares -modify ora1 Owner oracle
# hares -modify ora1 Home "/app/oracle/orahome"
# hares -modify ora1 StartUpOpt SRVCTLSTART
# hares -modify ora1 ShutDownOpt SRVCTLSTOP
```

10 Localize the Sid attribute for the Oracle resource:

```
# hares -local ora1 Sid
```

11 Set the Sid attributes for the Oracle resource on each system:

```
# hares -modify ora1 Sid vrts1 -sys galaxy
# hares -modify ora1 Sid vrts2 -sys nebula
```

12 Set the dependencies between the CFSMount resource and the CVMVolDg resource for the Oracle service group:

```
# hares -link oradata_mnt oradata_voldg
```

13 Set the dependencies between the Oracle resource and the CFSMount resource for the Oracle service group:

```
# hares -link ora1 oradata_mnt
```

14 Create an online local firm dependency between the oradb1_grp service group and the cvm service group:

```
# hagrp -link oradb1_grp cvm online local firm
```

15 Enable the Oracle service group:

```
# hagrp -enableresources oradb1_grp
```

16 Change the cluster configuration to the read-only mode:

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

17 Bring the Oracle service group online on all the nodes:

```
# hagrp -online oradb1_grp -any
```

For more information and instructions on configuring the service groups using the CLI:

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

Location of VCS log files

You may want to review the log files at `/var/VRTSvcs/log/engine_A.log` for errors or status messages. When large amounts of data are written, multiple log files may be written, such as engine_B.log, engine_C.log, and so on. The engine_A.log contains the most recent data.

Removing permissions for communication

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

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

Configuring the SFDB repository database after installation

If you want to use the Storage Foundation Database (SFDB) tools, you must set up the SFDB repository after installing and configuring SF Oracle RAC and Oracle. For SFDB repository set up procedures:

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

Chapter 20

Upgrading Oracle RAC

This chapter includes the following topics:

- Supported upgrade paths
- Preparing to upgrade Oracle RAC
- Upgrading Oracle RAC binaries
- Migrating the Oracle RAC database

Supported upgrade paths

Table 20-1 lists the upgrade paths for Oracle RAC.

Table 20-1 Supported upgrade paths for Oracle RAC

From current version	Upgrade to
Oracle RAC 9i Release 2	Oracle RAC 10g Release 2 Oracle RAC 11g Release 1
Oracle RAC 10g Release 1	Oracle RAC 10g Release 2 Oracle RAC 11g Release 1 Oracle RAC 11g Release 2
Oracle RAC 10g Release 2	Oracle RAC 11g Release 1 Oracle RAC 11g Release 2
Oracle RAC 11g Release 1	Oracle RAC 11g Release 2

Note: When you upgrade to a different version of Oracle RAC, make sure that the full path of the Oracle Clusterware/Grid Infrastructure home directory and the Oracle database home directory is different from the path where the existing version of Oracle RAC resides.

The upgrade procedure assumes that the beginning configuration includes the following components, and that these components are running on the cluster nodes:

- SF Oracle RAC 5.1 SP1
- A supported version of the operating system

Preparing to upgrade Oracle RAC

Complete the following preparatory tasks before you upgrade Oracle RAC:

1. Depending on the version you are upgrading from, perform the steps in one of the following sections:

   See "Preparing to upgrade from Oracle RAC 10g or Oracle RAC 11g " on page 364.

   See "Preparing to upgrade from Oracle RAC 9i" on page 365.

2. Verify that the cluster configuration is compatible for upgrading Oracle RAC.

   See "Verifying the systems for Oracle RAC installation" on page 324.

Preparing to upgrade from Oracle RAC 10g or Oracle RAC 11g

Perform the following tasks before upgrading Oracle RAC.

To prepare for upgrade from Oracle RAC 10g or Oracle RAC 11g

1 Take a hot or cold backup of the existing database.

2 Back up the existing Oracle home and central inventory.

3 If the Oracle RAC database is under VCS control, freeze the Oracle service groups to prevent VCS from reporting the resource as faulted when Oracle RAC stops and starts the database during the upgrade:

```
# haconf -makerw

# hagrp -freeze oracle_group -persistent

# haconf -dump -makero
```

Preparing to upgrade from Oracle RAC 9i

Perform the following pre-upgrade tasks before upgrading from Oracle RAC 9i.

To prepare for upgrade from Oracle RAC 9i

1. Take a hot or cold backup of the existing Oracle RAC 9i Release 2 database.
2. Back up the existing Oracle Home and Central Inventory.
3. If the Oracle RAC database is under VCS control, freeze the Oracle service groups to prevent VCS from reporting the resource as faulted when Oracle RAC stops and starts the database during the upgrade:

   ```
   # haconf -makerw

   # hagrp -freeze oracle_group -persistent

   # haconf -dump -makero
   ```

4. As the "Oracle" user, stop the Global Services Daemon, GSD:

   ```
   $ $ORACLE_HOME/bin/gsdctl stop
   ```

5. Perform the following pre-installation steps:
   - Identify the public virtual addresses for use by Oracle
   - Set the kernel tunables and other parameters
   - Configure private IP addresses for Oracle RAC
   - Create voting disk volumes and mount points
   - Set up Oracle user equivalence

   For instructions on performing the tasks, see the chapter *Before installing Oracle RAC* in this guide.

Upgrading Oracle RAC binaries

Review your Oracle installation manuals and the appropriate Oracle support Web sites before upgrading Oracle RAC.

Note: If you upgrade to Oracle RAC 11g Release 2, make sure that you upgrade with the same user credentials as that of the existing installation.

To upgrade Oracle RAC binaries

1 Upgrade Oracle Clusterware.

Note: If you upgrade to Oracle RAC 11g Release 2, upgrade Oracle Clusterware to a new directory called the Oracle grid infrastructure home directory (GRID_HOME).

Starting with Oracle RAC 11g Release 2, ASM must reside in the Oracle Grid Infrastructure home directory. If you plan to upgrade ASM to Release 11g R2, make sure that you upgrade it to run in the Oracle Grid Infrastructure home directory.

For instructions, see the Oracle RAC documentation.

2 Make sure that Oracle Clusterware is running.

3 Install the Oracle RAC database binaries.

For instructions, see the Oracle RAC documentation.

4 Complete the following post-installation tasks:

- Add Oracle RAC patches or patchsets.
  See "Adding Oracle RAC patches or patchsets" on page 345.
- Relink the SF Oracle RAC libraries with Oracle RAC.
  See "Relinking the SF Oracle RAC libraries with Oracle RAC" on page 350.
- For upgrades from Oracle RAC 9i: Add the CSSD resource to the VCS configuration.
  See "Configuring the CSSD resource" on page 346.

Migrating the Oracle RAC database

For instructions on migrating the existing Oracle RAC database, see the Oracle metalink documentation.

After migrating the database, complete the post-upgrade tasks:

See "Performing post-upgrade tasks" on page 366.

Performing post-upgrade tasks

Perform the steps in the following procedure to complete the upgrade.

To perform post-upgrade tasks

1 Change the cluster configuration to read-write mode:

```
# haconf -makerw
```

2 For upgrades from Oracle RAC 9i: Modify the resources in the Oracle service groups:

```
# hares -modify oracle_resource StartUpOpt SRVCTLSTART
# hares -modify oracle_resource ShutDowmOpt SRVCTLSTOP
# hares -modify oracle_resource pfile "" -sys galaxy
# hares -modify oracle_resource pfile "" -sys nebula
```

3 Add the Oracle UDP IPC private IP addresses to the Oracle `init.ora` file if the database cache fusion traffic is configured to use Oracle UDP IPC private IP addresses and if these addresses are configured as a PrivNIC or MultiPrivNIC resource for high availability.

See "Adding Oracle UDP IPC private IP addresses to the Oracle initialization parameter file" on page 354.

4 Modify the Oracle RAC configuration to prevent automatic startup of Oracle Clusterware.

See "Preventing automatic startup of Oracle Clusterware/Grid Infrastructure" on page 350.

5 Modify the Oracle RAC database configuration to prevent automatic database startup if you want the Oracle RAC database to be managed by VCS using the Oracle agent.

See "Preventing automatic database startup" on page 355.

6 Unfreeze the VCS service groups that were frozen earlier.

As root user, enter:

```
# hagrp -unfreeze oracle_group -persistent

# hagrp -unfreeze cvm_group -persistent

# haconf -dump -makero
```

7 Migrate OCR and voting disk to CFS or ASM.

For migrating OCR and voting disk to CFS:

- Create the required storage on CFS.
  For instructions:

See "Creating the OCR and voting disk storage on CFS" on page 286.

- Migrate OCR and voting disk to CFS.
  For instructions, see the Oracle documentation.

For instructions on migrating OCR and voting disk to ASM, see the Oracle documentation.

Section 5

Installation of SF Oracle RAC and Oracle RAC using a response file

- Chapter 21. About response files
- Chapter 22. Installing and configuring SF Oracle RAC using a response file
- Chapter 23. Configuring I/O fencing using a response file
- Chapter 24. Installing Oracle RAC using a response file
- Chapter 25. Response file variable definitions

Chapter 21

About response files

This chapter includes the following topics:

- About response files
- Response file syntax
- Guidelines for creating the SF Oracle RAC response file
- Installation scenarios for response files

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 Oracle RAC
- Preparing the nodes for installation of Oracle RAC
- Installing Oracle RAC
- Relinking the SF Oracle RAC libraries with Oracle RAC
- Configuring the CSSD agent
- Upgrading SF Oracle RAC
- Uninstalling SF Oracle RAC

You can perform end-to-end installations or modular deployments.

For more information on modular deployments:

See "Modular deployments using response files" on page 373.

Table 21-1 lists the various options available for creating or obtaining a response file.

Table 21-1 Options for obtaining a response file

Option	Description
Create a response file	Create a response file based on the response file template provided with SF Oracle RAC. The file is located at `/opt/VRTSvcs/rac/install`.

Reuse or customize the response files generated by an installation	The Veritas installation programs generate a response file during the installation, configuration, upgrade, or uninstallation of SF Oracle RAC and for installer-based pre-installation tasks for Oracle RAC.
	
	The response file generated by the installer is located in the following directory:
	
	`/opt/VRTS/install/logs/installsfrac-`*`installernumber`*`\`
	`/installsfrac-`*`installernumber`*`.response file`
	
	You can reuse or customize the response files to perform a complete end-to-end installation or to perform a specialized activity, such as setting up the PrivNIC or MultiPrivNIC configuration on your clusters. All you need to do is update the response file variable definitions to enable or disable the options, depending on the task you want to perform.
	
	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 Oracle RAC configuration** option.

Use the installation simulator	Create a response file by specifying the `-makeresponsefile` option with the SF Oracle RAC installer. Mount the product disc and navigate to the folder that contains the installation program. Start the installation program. `# ./installsfrac -makeresponsefile` The option creates a response file by simulating an installation. The response file is created in the directory `/opt/VRTS/install/logs/`. **Note:** You can use the `-makeresponsefile` option to create response files only for installing, configuring, and uninstalling SF Oracle RAC. For more information: See "About the installation simulator" on page 374.

At the end of the SF Oracle RAC 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 Oracle RAC response files also contain VCS variables used for the installation and configuration of VCS.

For the VCS variable definitions, see the *Veritas Cluster Server Installation Guide*.

Modular deployments using response files

Modular deployments offer flexibility in planning your installation and configuration activities. You can choose to perform any installation or configuration task independent of other related activities. For example, you can disable Oracle user and group creation across all nodes in a cluster while installing Oracle RAC.

Modular deployments are supported for the following installation and configuration activities:

- Installing SF Oracle RAC
- Configuring SF Oracle RAC
- Creating Oracle user and group
- Creating storage for OCR and voting disk
- Configuring private IP addresses for Oracle RAC
- Installing Oracle Clusterware
- Installing Oracle database
- Oracle post-installation tasks:
  Configuring CSSD agent
  Relinking Oracle RAC libraries

The variables required for each of the above tasks are described in the chapter "Response file variable definitions".

All modular deployment activities require the following variable definitions:

```
$CFG{prod}
$CFG{systems}
```

About the installation simulator

The SF Oracle RAC installer includes the option (`-makeresponsefile`) to simulate the installation, configuration, or uninstallation of the product. The simulation option steps through the installation script, including all of the preinstallation checks on the systems. However, the simulation does not actually install the depots, uninstall previously installed depots, or start or stop any processes.

Use the installation simulator in the following situations:

- To understand the information that is required when you install, configure, or uninstall SF Oracle RAC
  As the simulator steps through the same code that is used by the installer, you can use the simulation process to preview the installation or configuration steps without disrupting your existing installation. You can skip the preinstallation checks, if not required.
- To create a response file
  The simulation process enables you to create a response file that can be used as a template for installing, configuring, or uninstalling SF Oracle RAC. You can customize the response file, as required.

To simulate an installation or configuration, specify the `-makeresponsefile` option with the installer or product installation script at the command line.

To simulate an uninstallation, specify the `-makeresponsefile` option with the installer or the product uninstall script at the command line.

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 Oracle RAC response file

This section provides guidelines for creating the SF Oracle RAC response file.

1. Create a response file using one of the available options.

   For various options on creating or obtaining an SF Oracle RAC response file:

   See "About response files" on page 371.

2. Set the following master values to 1 to enable SF Oracle RAC 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 Oracle RAC.

Installing SF Oracle RAC	`$CFG{opt}{install}=1;`
Configuring SF Oracle RAC	`$CFG{opt}{configure}=1;` `$CFG{config_sfrac_subcomponents} = 1;`

3. Now, set the appropriate value in the dependent variable definitions for installing and configuring SF Oracle RAC.

   The set of minimum definitions for a successful installation and configuration is as follows:

```
$CFG{accepteula}=1;
$CFG{opt}{install}=1;
$CFG{opt}{configure}=1;
$CFG{config_sfrac_subcomponents} = 1;
$CFG{opt}{installallpkgs}=1;
$CFG{opt}{vxkeyless}=1;
$CFG{prod}="SFRAC51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=101;
```

```
$CFG{vcs_clustername}="rac_cluster101";
$CFG{vcs_lltlink1}{galaxy}="lan1";
$CFG{vcs_lltlink1}{nebula}="lan1";
$CFG{vcs_lltlink2}{galaxy}="lan2";
$CFG{vcs_lltlink2}{nebula}="lan2";
$CFG{vcs_userenpw}=[ qw(gpqIpkPmqLqqOyqKpn) ];
$CFG{vcs_username}=[ qw(admin) ];
$CFG{vcs_userpriv}=[ qw(Administrators) ];
```

You can add more variable definitions, as required.

4. Set the following master values to 1 to enable the Oracle pre-installation tasks.

Note: This step assumes that you have already set the master value `$CFG{opt}{configure}` to 1 in the previous step.

The following is the list of additional master values that must be set for completing Oracle pre-installation tasks:

Private IP address configuration	If you plan to use the PrivNIC agent, use the following master settings:
	`$CFG{config_privnic}=1;`
	`$CFG{config_multiprivnic}=0;`
	If you plan to use the MultiPrivNIC agent, use the following master settings:
	`$CFG{config_multiprivnic}=1;`
	`$CFG{config_privnic}=0;`

OCR and voting disk storage	`$CFG{create_ocr_vote_storage}=1;`
Oracle Clusterware/Grid Infrastructure installation	`$CFG{install_oracle_clusterware}=1;`
Oracle database installation	`$CFG{install_oracle_database}=1;`
Post Oracle tasks	`$CFG{config_cssd_agent}=1;` `$CFG{relink_oracle_database}=1;`

Set the master value for the `$CFG{create_oracle_user_group}` variable to 0 as follows:

```
$CFG{create_oracle_user_group}=0;
```

Note: If you are performing an end-to-end installation, the creation of Oracle user and group must be completed before starting the installation. This is because user equivalence must be manually established on all nodes to allow the Oracle Universal Installer to securely copy files and run programs on the nodes in the cluster without requiring password prompts.

5. Set the appropriate value for the dependent variable definitions for the Oracle pre-installation tasks.

Private IP address configuration

If you plan to use the PrivNIC agent, provide the following definitions:

```
$CFG{privnic_resname} = "ora_priv";
$CFG{privnic_interface_priority}="lan2 lan3";
$CFG{galaxy}{privnicip} = "192.168.12.1";
$CFG{galaxy}->{hostname_for_ip} = "galaxy-priv";
$CFG{nebula}{privnicip} = "192.168.12.2";
$CFG{nebula}->{hostname_for_ip} = "nebula-priv";
$CFG{nic_netmask} = "255.255.255.0";
$CFG{nic_add_ip_to_files} = 1;
```

If you plan to use the MultiPrivNIC agent, use the following master settings:

```
$CFG{multiprivnic_resname} = "ora_priv";
$CFG{nic_add_ip_to_files} = 1;
$CFG{galaxy}->{lan1}->{multiprivnicip}
= "192.168.12.1";
$CFG{galaxy}->{lan1}->{hostname_for_ip}
= "galaxy-priv";
$CFG{galaxy}->{lan2}->{multiprivnicip}
= "192.168.2.1";
$CFG{galaxy}->{lan2}->{hostname_for_ip}
= "galaxy-priv1";
$CFG{nebula}->{lan1}->{multiprivnicip}
= "192.168.12.2";
$CFG{nebula}->{lan1}->{hostname_for_ip}
= "nebula-priv";
$CFG{nebula}->{lan2}->{multiprivnicip}
= "192.168.2.2";
$CFG{nebula}->{lan2}->{hostname_for_ip}
= "nebula-priv1";
$CFG{nic_netmask} = "255.255.255.0";
```

OCR and voting disk storage

If you choose to create the OCR and voting disk storage:

```
$CFG{ocrvotedgoption} = 0;
$CFG{ocrvotescheme} = 1;
$CFG{ocrvotedisks} = [ qw(Disk_1 Disk_2) ];
$CFG{ocrvotedgname} = "ocrvotedg";
$CFG{ocrvotevolname} = "ocrvotevol";
$CFG{ocrvotevolsize} = 640;
$CFG{ocrvotemount} = "/ocrvote";
$CFG{oracle_user} = "oracle";
$CFG{oracle_group} = "oinstall";
```

If you choose to use an existing storage for the OCR and voting disk storage:

```
$CFG{ocrvotedgoption} = 1;
$CFG{ocrvotescheme} = 0;
$CFG{ocrvotedgname} = "ocrvotedg";
$CFG{ocrvotevolname} = "ocrvotevol";
$CFG{ocrvotevolsize} = 640;
$CFG{ocrvotemount} = "/ocrvote";
$CFG{oracle_user} = "oracle";
$CFG{oracle_group} = "oinstall";
```

Oracle Clusterware/Grid Infrastructure installation

```
$CFG{oracle_user} = "oracle";
$CFG{oracle_group} = "oinstall";
$CFG{oracle_base} = "/app/oracle";
$CFG{crs_home} = "/app/oracle/crshome";
$CFG{crs_installpath} = "/cdrom/oracle/clusterware";
$CFG{oracle_version} = "11.1.0.6";
$CFG{crs_responsefile} = "/oracle/crs.rsp";
```

Oracle database installation

```
$CFG{oracle_user} = "oracle";
$CFG{oracle_group} = "oinstall";
$CFG{oracle_base} = "/app/oracle";
$CFG{crs_home} = "/app/oracle/crshome";
$CFG{db_home} = "/app/oracle/dbhome";
$CFG{db_installpath} = "/cdrom/oracle/database";
$CFG{oracle_version} = "11.1.0.6";
$CFG{db_responsefile} = "/oracle/db.rsp";
```

Post Oracle tasks

The master value (set in the previous step) suffices for CSSD resource configuration.

For relinking libraries, the dependent variable settings are as follows:

```
$CFG{oracle_user} = "oracle";
$CFG{oracle_group} = "oinstall";
$CFG{crs_home} = "/app/oracle/crshome";
$CFG{db_home} = "/app/oracle/dbhome";
$CFG{oracle_version} = "11.1.0.6";
```

Installation scenarios for response files

The chapters in this section cover the following installation scenarios using response files:

- Installing and configuring SF Oracle RAC
  See "Installing and configuring SF Oracle RAC" on page 381.
- Installing Oracle RAC
  See "About installing Oracle RAC using response files" on page 389.

Chapter 22

Installing and configuring SF Oracle RAC using a response file

This chapter includes the following topics:

- Installing and configuring SF Oracle RAC
- Sample response file for installing SF Oracle RAC
- Sample response file for configuring SF Oracle RAC

Installing and configuring SF Oracle RAC

You can create a single response file or separate response files for installing and configuring SF Oracle RAC.

The installer performs the following tasks:

- Installs SF Oracle RAC.
- Configures SF Oracle RAC.

Note: Fencing is configured in disabled mode. You must configure I/O fencing after the installation.

The following sample procedure uses a single response file for installing and configuring SF Oracle RAC.

To install and configure SF Oracle RAC using response files

1 Make sure that the systems meet the installation requirements.

2 Complete the preparatory steps before starting the installation.

For instructions, see the chapter "Preparing to install SF Oracle RAC" in this document.

3 Create a response file using one of the available options.

For information on various options available for creating a response file:

See “About response files” on page 371.

Note: You must replace the host names in the response file with that of the new systems in the cluster.

For guidelines on creating a response file:

See “Guidelines for creating the SF Oracle RAC response file” on page 375.

For a sample response file:

See “Sample response file for installing SF Oracle RAC” on page 383.

See “Sample response file for configuring SF Oracle RAC” on page 383.

4 Mount the product disc and navigate to the product directory that contains the installation program.

5 Start the installation:

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

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

6 Restart the nodes after installation. Some of the depots require a restart operation before you can proceed to configure SF Oracle RAC.

Note: Do not use the reboot command to restart the nodes.

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

7 Start the configuration:

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

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

Note: Fencing is configured in disabled mode. You need to configure fencing after the configuration.

---

8 Configure I/O fencing.

Note: Before you configure I/O fencing, make sure that you complete the required pre-configuration tasks. For instructions, see the chapter *Preparing to configure SF Oracle RAC* in this document.

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.

9 Complete the SF Oracle RAC post-installation tasks.

For instructions, see the chapter *Performing post-installation and configuration tasks* in this document.

Sample response file for installing SF Oracle RAC

The following sample response file installs SF Oracle RAC on two nodes, galaxy and nebula.

```
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{vxkeyless}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{prod}="SFRAC51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{uploadlogs}=0;

1;
```

Sample response file for configuring SF Oracle RAC

The following sample response file configures SF Oracle RAC on two nodes, galaxy and nebula.

```
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{install}=1;
$CFG{prod}="SFRAC51SP1";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{opt}{configure}=1;
```

```
$CFG{config_sfrac_subcomponents} = 1;
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=101;
$CFG{vcs_clustername}="rac_cluster101";
$CFG{vcs_lltlink1}{galaxy}="lan1";
$CFG{vcs_lltlink1}{nebula}="lan1";
$CFG{vcs_lltlink2}{galaxy}="lan2";
$CFG{vcs_lltlink2}{nebula}="lan2";
$CFG{vcs_username}=[ qw(admin) ];
$CFG{vcs_userpriv}=[ qw(Administrators) ];
$CFG{vcs_userenpw}=[ qw(gpqIpkPmqLqqOyqKpn) ];
$CFG{uploadlogs}=0;

1;
```

Chapter 23

Configuring I/O fencing using a response file

This chapter includes the following topics:

- Configuring I/O fencing using response files
- Sample response file for configuring disk-based I/O fencing
- Sample response file for configuring server-based I/O fencing

Configuring I/O fencing using response files

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

To configure I/O fencing using response files

1. Make sure that SF Oracle RAC is configured.
2. Based on whether you want to configure disk-based or server-based I/O fencing, make sure you have completed the preparatory tasks.

   See "About planning to configure I/O fencing" on page 62.
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 386.

   See "Sample response file for configuring server-based I/O fencing" on page 386.

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

See "Response file variables to configure disk-based I/O fencing" on page 407.

See "Response file variables to configure server-based I/O fencing" on page 409.

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

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

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

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 407.

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

$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;

$CFG{prod}="SFRAC51";

$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=13221;
$CFG{vcs_clustername}="rac_cluster101";
$CFG{vxfen_config_fencing_dg}="fendg";
$CFG{vxfen_config_fencing_mechanism}="dmp";
$CFG{vxfen_config_fencing_newdg_disks}=
 [ qw(c1t1d0 c2t1d0 c3t1d0) ];
$CFG{vxfen_config_fencing_option}=2;
```

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

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

```
$CFG{fencing_cpc_config_cpagent}=0;
$CFG{fencing_cpc_cps}=[ qw(10.200.117.145) ];
$CFG{fencing_cpc_dgname}="vxfencoorddg";
$CFG{fencing_cpc_diffab}=0;
$CFG{fencing_cpc_disks}=[ qw(emc_clariion0_37 emc_clariion0_13) ];
$CFG{fencing_cpc_mechanism}="raw";
$CFG{fencing_cpc_ncps}=3;
$CFG{fencing_cpc_ndisks}=2;
$CFG{fencing_cpc_ports}{"10.200.117.145"}=14250;
$CFG{fencing_cpc_reusedg}=1;
$CFG{fencing_cpc_security}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="SFRAC51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="rac_cluster101";
$CFG{vxfen_config_fencing_option}=1;
```

Chapter 24

Installing Oracle RAC using a response file

This chapter includes the following topics:

- About installing Oracle RAC using response files
- Before you install
- Installing Oracle RAC
- Sample response file for installing Oracle RAC

About installing Oracle RAC using response files

You can perform an unattended pre-configuration of your systems by running the SF Oracle RAC installer with the `-responsefile` option. This capability in tandem with the Oracle response files for Oracle Clusterware and Oracle database installation enables you to standardize and automate Oracle RAC deployments in your cluster.

Before you install

Make sure that you complete the tasks in the following procedure before starting the silent installation of Oracle RAC.

To prepare the systems for installing Oracle RAC using response files

1 Complete the following preparatory tasks on the nodes manually or by using the SF Oracle RAC installer:

- Identify the public virtual IP addresses for use by Oracle
- Plan for the storage and the private network configuration for Oracle RAC

- Set the kernel parameters
- Verify the user "nobody" exists
- Create Oracle user and groups
- Set up Oracle user equivalence
- Edit the Oracle user profile

For instructions:

See "About preparing to install Oracle RAC" on page 275.

2 Create response files for Oracle Clusterware/Grid Infrastructure and Oracle database installation using the response file template provided by Oracle RAC.

For instructions on using the response file template, see the Oracle RAC documentation.

Note: Keep at hand the full path of the directory where these response files will be saved. The full path of the Oracle Clusterware/Grid Infrastructure response file must be set in the SF Oracle RAC response file variable `$CFG{crs_responsefile};`. The full path of the Oracle database response file must be set in the SF Oracle RAC response file variable `$CFG{db_responsefile};`.

---

3 Create an SF Oracle RAC response file.

For information on various options available for creating a response file:

See "About response files" on page 371.

Make sure that you provide the full path information of the Oracle Clusterware/Grid Infrastructure and Oracle database response files.

For guidelines on creating a response file:

See "Guidelines for creating the SF Oracle RAC response file" on page 375.

For information on the list of required and optional variables:

See "Response file variable definitions for Oracle RAC" on page 411.

For a sample response file:

See "Sample response file for installing Oracle RAC" on page 392.

4 Make sure that the Oracle user has appropriate read and write permissions on the response files.

5 Make sure that passwordless communication between Oracle users is set up on the nodes of the cluster.

Installing Oracle RAC

To perform a silent installation of Oracle RAC, run the SF Oracle RAC installer.

The installer supports completion of the following tasks using the response file:

- Creates storage for OCR and voting disk
- Configures the private network for Oracle RAC
- Installs Oracle Clusterware/Grid Infrastructure by leveraging the corresponding Oracle response file
- Installs Oracle database by leveraging the Oracle database response file
- Relinks the Oracle RAC libraries with SF Oracle RAC libraries
- Configures the CSSD agent

The sample procedure assumes that Oracle user equivalence is established on all the nodes in the cluster.

To perform Oracle pre-installation and installation on the nodes

1 Navigate to the directory containing the SF Oracle RAC installer:

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

2 Start the installation:

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

Where `/tmp/response_file` is the full path name of the SF Oracle RAC response file.

3 Run the root.sh script as the root user on the cluster nodes.

Note: Do not run the script simultaneously on your cluster nodes.

4 Complete the following Oracle post-installation tasks:

- Add any patches or patchsets required by Oracle RAC .
- Create the Oracle RAC database.

- Add the Oracle UDP IPC private IP addresses to the Oracle `init.ora` file if the database cache fusion traffic is configured to use Oracle UDP IPC private IP addresses and if these addresses are configured as a PrivNIC or MultiPrivNIC resource for high availability.
- Configure the Oracle RAC database for manual startup if you want the Oracle RAC database to be managed by VCS using the Oracle agent.
- Configure the VCS service groups for Oracle RAC.
- Verify the cluster.
- Remove the temporary communication permissions.

For instructions:

See the chapter *Performing Oracle RAC post-installation tasks*.

Sample response file for installing Oracle RAC

The following sample response file installs Oracle RAC 11g Release 2 and performs the following Oracle RAC pre-installation and installation tasks on two nodes, galaxy and nebula, in the cluster:

- Creates a disk group for OCR and voting disk storage
- Creates OCR and voting disk storage on raw volumes
- Configures the PrivNIC agent for high availability on both nodes
- Installs Oracle Clusterware
- Installs Oracle database
- Relinks the Oracle RAC libraries with SF Oracle RAC libraries
- Configures the CSSD agent

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

$CFG{prod}="SFRAC51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{opt}{configure}=1;

$CFG{config_privnic}=1;
$CFG{privnic_resname}="ora_priv";
$CFG{privnic_interface_priority}="lan2 lan3";
```

```
$CFG{galaxy}{privnicip}=" 192.168.12.1";
$CFG{galaxy}->{hostname_for_ip}="galaxy-priv";
$CFG{nebula}{privnicip}=" 192.168.12.2";
$CFG{nebula}->{hostname_for_ip}="nebula-priv";
$CFG{nic_netmask}="255.255.255.0";
$CFG{nic_add_ip_to_files}=1;
$CFG{nic_reuseip}=1;
$CFG{nic_reusealias}=1;

$CFG{create_ocr_vote_storage}=1;
$CFG{ocrvotedgoption}=0;
$CFG{oracle_group}="dba";
$CFG{grid_user}="grid";
$CFG{oracle_user}="oracle";
$CFG{ocrvolname}="ocrvotevol";
$CFG{ocrvolsize}=640;
$CFG{ocrvotedgname}="ocrvotedg";
$CFG{ocrvotedisks}=[qw(Disk_1 Disk_2)];
$CFG{ocrvotescheme}=0;
$CFG{votevolname}="votevol";
$CFG{votevolsize}=500;

$CFG{install_oracle_clusterware}=1;
$CFG{install_oracle_database}=1;
$CFG{oracle_base} = "/app/oracle";
$CFG{crs_home}="/app/oracle ";
$CFG{db_home}="/app/oracle/orahome";
$CFG{crs_installpath}="/cdrom/oracle/clusterware";
$CFG{db_installpath}="/cdrom/oracle/database";
$CFG{crs_responsefile}="/oracle/crs.rsp";
$CFG{db_responsefile} = "/oracle/db.rsp";

$CFG{config_cssd_agent}=1;
$CFG{relink_oracle_database}=1;
$CFG{uploadlogs}=0;

1;
```

Chapter 25

Response file variable definitions

This chapter includes the following topics:

- Response file variables for installing SF Oracle RAC
- Response file variables to configure SF Oracle RAC
- Response file variables to configure disk-based I/O fencing
- Response file variables to configure server-based I/O fencing
- Response file variable definitions for Oracle RAC

Response file variables for installing SF Oracle RAC

Table 25-1 lists the response file variables that you can define to install SF Oracle RAC.

Table 25-1 Response file variables for installing SF Oracle RAC

Variable	List or Scalar	Description
CFG{opt}{install}	Scalar	Required Installs SF Oracle RAC depots.
CFG{opt}{systems}	List	Required List of systems on which the product is to be installed.
CFG{opt}{upi}	Scalar	Required for the installer Defines the product to be installed.

Table 25-1 Response file variables for installing SF Oracle RAC *(continued)*

Variable	List or Scalar	Description
CFG{opt}{installallpkgs} or CFG{opt}{installrecpkgs} or CFG{opt}{installminpkgs}	Scalar	Required Instructs the installer to install SF Oracle RAC depots based on the variable that has the value set to 1: ■ installallpkgs: Installs all depots ■ installrecpkgs: Installs recommended depots ■ installminpkgs: Installs minimum depots **Note:** Set only one of these variable values to 1. In addition to setting the value of one of these variables, you must set the variable *$CFG{opt}{install}* to 1.
CFG{opt}{rsh}	Scalar	Optional Defines that remote shell must be used instead of ssh as the communication method between systems.
CFG{opt}{gco}	Scalar	Optional Defines that the installer must enable the global cluster option. You must set this variable value to 1 if you want to configure global clusters.
CFG{opt}{keyfile}	Scalar	Optional Defines the location of an ssh keyfile that is used to communicate with all remote systems.
CFG{opt}{patchpath}	Scalar	Optional Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems.

Table 25-1 Response file variables for installing SF Oracle RAC *(continued)*

Variable	List or Scalar	Description
CFG{opt}{pkgpath}	Scalar	Optional Defines a location, typically an NFS mount, from which all remote systems can install product depots. The location must be accessible from all target systems.
CFG{opt}{tmppath}	Scalar	Optional Defines the location where a working directory is created to store temporary files and the depots that are needed during the install. The default location is /var/tmp.
CFG{opt}{logpath}	Scalar	Optional Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location.
CFG{opt}{donotinstall} {depot}	List	Optional Instructs the installation to not install the optional depots in the list.
$CFG{opt}{vxkeyless}	Scalar	Optional Defines a Boolean value 0 or 1. The value 1 indicates keyless installation. The value 0 indicates that a license key is required for the product. You must set the variable *$CFG{keys}{hostname}* with appropriate values.

Table 25-1 Response file variables for installing SF Oracle RAC *(continued)*

Variable	List or Scalar	Description
CFG{keys} {hostname}	Scalar	Optional List of keys to be registered on the system if the variable *$CFG{opt}{vxkeyless}* is set to 0.
$CFG{uploadlogs}	Scalar	Optional Defines a Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site.

Response file variables to configure SF Oracle RAC

Table 25-2 lists the response file variables that you can define to configure SF Oracle RAC.

Table 25-2 Response file variables specific to configuring SF Oracle RAC

Variable	List or Scalar	Description
CFG{opt}{configure}	Scalar	Performs the configuration if the depots are already installed. (Required)
$CFG{config_sfrac_subcomponents}	Scalar	Set the variable to 1 to configure the SF Oracle RAC components. (Required) **Note:** You must set the *$CFG{opt}{configure}* variable to 1.
CFG{accepteula}	Scalar	Specifies whether you agree with `EULA.pdf` on the media. (Required)

Table 25-2 Response file variables specific to configuring SF Oracle RAC *(continued)*

Variable	List or Scalar	Description
CFG{systems}	List	List of systems on which the product is to be configured. (Required)
CFG{prod}	Scalar	Defines the product to be configured. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *remsh* 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 *logpath* location. (Optional)
$CFG{uploadlogs}	Scalar	Defines Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site. (Optional)

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (the csgnic, csgvip, and csgnetmask variables) must be defined if any are defined. The same is true for the SMTP notification (the smtpserver, smtprecp, and smtprsev variables), the SNMP trap notification (the snmpport, snmpcons, and snmpcsev variables), and the Global Cluster Option (the gconic, gcovip, and gconetmask variables).

Table 25-3 lists the response file variables that specify the required information to configure a basic SF Oracle RAC cluster.

Table 25-3 Response file variables specific to configuring a basic SF Oracle RAC 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)

Table 25-4 lists the response file variables that specify the required information to configure LLT over Ethernet.

Table 25-4 Response file variables specific to configuring private LLT over Ethernet

Variable	List or Scalar	Description
CFG{vcs_lltlink#} {"system"}	Scalar	Defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (lltlink1 and lltlink2). You can configure up to four LLT links. You must enclose the system name within double quotes. (Required)
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 25-5 lists the response file variables that specify the required information to configure LLT over UDP.

Table 25-5 Response file variables specific to configuring LLT over UDP

Variable	List or Scalar	Description
CFG{lltoverudp}=1	Scalar	Indicates whether to configure heartbeat link using LLT over UDP. (Required)

Table 25-5 Response file variables specific to configuring LLT over UDP *(continued)*

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

Table 25-5 Response file variables specific to configuring LLT over UDP *(continued)*

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

Table 25-6 lists the response file variables that specify the required information to configure virtual IP for SF Oracle RAC cluster.

Table 25-6 Response file variables specific to configuring virtual IP for SF Oracle RAC 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 25-7 lists the response file variables that specify the required information to configure the SF Oracle RAC cluster in secure mode.

Table 25-7 Response file variables specific to configuring SF Oracle RAC cluster in secure mode

Variable	List or Scalar	Description
CFG{at_rootdomain}	Scalar	Defines the name of the system where the root broker is installed. (Optional)
CFG{at_rootbroker}	Scalar	Defines the root broker's name.
CFG{vcs_securitymenuopt}	Scalar	Specifies the menu option to choose to configure the cluster in secure mode. ■ 1—Automatic ■ 2—Semi-automatic ■ 3—Manual (Optional)
CFG{vcs_vssdefport}	Scalar	Specifies the default port address of the root broker. (Optional)
CFG{vcs_roothashpath}	Scalar	Specifies the path of the root hash file. (Optional)
CFG{vcs_ab_prplname} {system}	Scalar	Specifies the authentication broker's principal name on system. (Optional)
CFG{vcs_ab_password} {system}	Scalar	Specifies the authentication broker's password on system. (Optional)
CFG{vcs_blobpath} {system}	Scalar	Specifies the path of the encrypted BLOB file for system. (Optional)

Table 25-8 lists the response file variables that specify the required information to configure VCS users.

Table 25-8 Response file variables specific to configuring VCS users

Variable	List or Scalar	Description
CFG{vcs_userenpw}	List	List of encoded passwords for VCS users. The value in the list can be "Administrators Operators Guests." **Note:** The order of the values for the vcs_userenpw list must match the order of the values in the vcs_username list. (Optional)
CFG{vcs_username}	List	List of names of VCS users. (Optional)
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 25-9 lists the response file variables that specify the required information to configure VCS notifications using SMTP.

Table 25-9 Response file variables specific to configuring VCS notifications using SMTP

Variable	List or Scalar	Description
CFG{vcs_smtpserver}	Scalar	Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for Web notification. (Optional)
CFG{vcs_smtprecp}	List	List of full email addresses (example: user@symantecexample.com) of SMTP recipients. (Optional)

Table 25-9 Response file variables specific to configuring VCS notifications using SMTP *(continued)*

Variable	List or Scalar	Description
CFG{vcs_smtprsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, and SevereError) that listed SMTP recipients are to receive. Note that the ordering of severity levels must match that of the addresses of SMTP recipients. (Optional)

Table 25-10 lists the response file variables that specify the required information to configure VCS notifications using SNMP.

Table 25-10 Response file variables specific to configuring VCS notifications using SNMP

Variable	List or Scalar	Description
CFG{vcs_snmpport}	Scalar	Defines the SNMP trap daemon port (default=162). (Optional)
CFG{vcs_snmpcons}	List	List of SNMP console system names. (Optional)
CFG{vcs_snmpcsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, and SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names. (Optional)

Table 25-11 lists the response file variables that specify the required information to configure SF Oracle RAC global clusters.

Table 25-11 Response file variables specific to configuring SF Oracle RAC 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)

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

Table 25-12 lists the response file variables that specify the required information to configure disk-based I/O fencing for SF Oracle RAC.

Table 25-12 Response file variables specific to configuring disk-based I/O fencing

Variable	List or Scalar	Description
CFG{opt}{fencing}	Scalar	Performs the I/O fencing configuration. (Required)
CFG{vxfen_config_fencing_option}	Scalar	Specifies the I/O fencing configuration mode. ■ 1—Coordination Point Server-based I/O fencing ■ 2—Coordinator disk-based I/O fencing ■ 3—Disabled mode (Required)

Table 25-12 Response file variables specific to configuring disk-based I/O fencing *(continued)*

Variable	List or Scalar	Description
CFG {vxfen_config _fencing_mechanism}	Scalar	Specifies the I/O fencing mechanism. This variable is not required if you had configured fencing in disabled mode. For disk-based fencing, you must configure the vxfen_config _fencing_mechanism variable and either the vxfen_config_fencing_dg variable or the vxfen_config _fencing_newdg_disks variable. (Optional)
CFG{vxfen_config_fencing_dg}	Scalar	Specifies the disk group for I/O fencing. (Optional) **Note:** You must define the vxfen_config_fencing_dg variable to use an existing disk group. If you want to create a new disk group, you must use both the vxfen_config_fencing_dg variable and the vxfen_config_fencing_newdg_disks variable.
CFG{vxfen_config _fencing_newdg_disks}	List	Specifies the disks to use to create a new disk group for I/O fencing. (Optional) **Note:** You must define the vxfen_config_fencing_dg variable to use an existing disk group. If you want to create a new disk group, you must use both the vxfen_config_fencing_dg variable and the vxfen_config_fencing_newdg_disks variable.

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

You can use a CP server response file to configure server-based customized I/O fencing. The installer uses the CP server response file for the following types of I/O fencing configurations:

- Client cluster fencing (server-based I/O fencing configuration itself)
  The installer configures server-based customized I/O fencing on the SF Oracle RAC cluster without prompting for user input.
- Disk-based fencing with the disk group already created
  The installer configures fencing in disk-based mode on the SF Oracle RAC cluster without prompting for user input.
  Disk-based fencing configuration is one in which SCSI-3 disks are used as the only coordination points.
  Disk-based fencing with the disk group already created means that the disk group consisting of the coordinating disks already exists on the SF Oracle RAC cluster nodes.
- Disk-based fencing with the disk group to be created
  The installer creates the disk group and configures fencing properly on all the nodes in the SF Oracle RAC cluster without user intervention.
  Disk-based fencing with the disk group to be created means that the disk group does not exist yet, but will be created with the disks mentioned as coordination point.

Table 25-13 lists the fields in the response file that are relevant for server-based customized I/O fencing.

Table 25-13 CP server response file definitions

Response file field	Definition
fencing_cpc_config_cpagent	Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter "0" if you do not want to configure the Coordination Point agent using the installer. Enter "1" if you want to use the installer to configure the Coordination Point agent.

Table 25-13 CP server response file definitions *(continued)*

Response file field	Definition
fencing_cpc_cpagentgrp	Name of the service group which will have the Coordination Point agent resource as part of it. **Note:** This field is obsolete if the `fencing_cpc_config_cpagent` field is given a value of '0'.
fencing_cpc_cps	Virtual IP address or Virtual hostname of the CP servers.
fencing_cpc_reusedg	This response file field indicates whether to reuse an existing DG name for the fencing configuration in customized fencing (CP server and coordinator disks). Enter either a "1" or "0". Entering a "1" indicates reuse, and entering a "0" indicates do not reuse. When reusing an existing DG name for the mixed mode fencing configuration. you need to manually add a line of text , such as "$CFG{fencing_cpc_reusedg}=0" or "$CFG{fencing_cpc_reusedg}=1" before proceeding with a silent installation.
fencing_cpc_dgname	The name of the disk group to be used in the customized fencing, where at least one disk is being used.
fencing_cpc_diffab	This response field indicates whether the CP servers and SF Oracle RAC clusters use different root brokers. Entering a "1" indicates that they are using different root brokers. Entering a "0" indicates that they are not using different root brokers.
fencing_cpc_disks	The disks being used as coordination points if any.
fencing_cpc_ncps	Total number of coordination points being used, including both CP servers and disks.
fencing_cpc_ndisks	The number of disks being used.
fencing_cpc_ports	The port of the CP server that is denoted by *cps* .

Table 25-13 CP server response file definitions *(continued)*

Response file field	Definition
fencing_cpc_ccab	The name of the authentication broker (AB) for any one of the SF Oracle RAC cluster nodes.
fencing_cpc_cpsabport	The port at which the authentication broker (AB) mentioned above listens for authentication..
fencing_cpc_ccabport	The port at which the authentication broker (AB) mentioned above listens for authentication.
fencing_cpc_mechanism	The disk mechanism that is used by customized fencing. The value for this field is either "raw" or "dmp"
fencing_cpc_cpsab	The name of the authentication broker (AB) for any one of the CP servers.
fencing_cpc_security	This field indicates whether security is enabled or not Entering a "1" indicates that security is enabled. Entering a "0" indicates that security has not been enabled.

Response file variable definitions for Oracle RAC

The variable definitions for Oracle RAC are grouped in tabular format for the following Oracle tasks:

Creating Oracle user and group — See Table 25-14 on page 412.

Creating storage for OCR and voting disk — See Table 25-15 on page 413.

Configuring the private IP address and PrivNIC resource under VCS — See Table 25-16 on page 416.

Configuring the private IP address and MultiPrivNIC resource under VCS — See Table 25-17 on page 420.

Installing Oracle Clusterware — See Table 25-18 on page 423.

Installing Oracle database — See Table 25-19 on page 424.

Configuring CSSD resource — See Table 25-20 on page 425.

Relinking Oracle RAC libraries — See Table 25-21 on page 426.

Note: Some of the variable definitions may occur in multiple sections, for example `$CFG{oracle_user}`. These variables need not be repeated if all the tasks are performed as a single installation activity. However, if you perform these tasks independently, make sure that all the required variables, as indicated in the table for each task, are supplied in the response file.

Table 25-14 lists the variables that are used to create the Oracle user and group.

Table 25-14 Variables for creating Oracle user and group

Variable	List or Scalar	Description
$CFG{create_oracle_user_group}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that Oracle user and group will be created. The value 0 indicates that Oracle user and group will not be created.
$CFG{grid_user}	Scalar	Required Defines the name of the grid user.
$CFG{oracle_user}	Scalar	Required Defines the name of the Oracle user.
$CFG{oracle_uid}	Scalar	Required Defines the user ID of the Oracle user.
$CFG{oracle_group}	Scalar	Required Defines the primary group of the Oracle user.
$CFG{oracle_gid}	Scalar	Required Defines the group ID of the Oracle user.
$CFG{oracle_user_home}	Scalar	Required Defines the full path of the Oracle user's home directory.

Table 25-14 Variables for creating Oracle user and group *(continued)*

Variable	List or Scalar	Description
$CFG{oracle_secondary_group}	List	Optional Defines the list of secondary groups for the Oracle user.
$CFG{oracle_secondary_gid}	List	Optional Defines the list of secondary group IDs for the Oracle user. The elements of this variable must be in the same order as that of the elements in the variable `$CFG{oracle_secondary_group}`.

Table 25-15 lists the variables that are used to create the storage for OCR and voting disk.

Table 25-15 Variables for creating storage for OCR and voting disk

Variable	List or Scalar	Description
$CFG{create_ocr_vote_storage}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the storage for OCR and voting disk will be created. The value 0 indicates that the storage for OCR and voting disk will not be created.

Table 25-15 Variables for creating storage for OCR and voting disk *(continued)*

Variable	List or Scalar	Description
$CFG{ocrvotedgoption}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that an existing disk group will be used to create the storage for OCR and voting disk. **Note:** If you choose to use an existing disk group, use the `$CFG{ocrvotedgname}` variable to specify the name of an existing disk group that has a minimum of two disks (for mirroring). The value 0 indicates that a new disk group will be created for OCR and voting disk storage. **Note:** If you choose to create a disk group, you must set the following variables: `$CFG{ocrvotedisks}`, `$CFG{ocrvotedgname}`
$CFG{ocrvotescheme}	Scalar	Required Defines the storage scheme to be used for OCR and voting disk. The value 1 indicates Clustered File System. The value 0 indicates CVM raw volumes.
$CFG{ocrvotedisks}	List	Required Defines the list of shared disks to be used for OCR and voting disk.
$CFG{ocrvotedgname}	Scalar	Required Defines the name of the disk group to be used for OCR and voting disk.

Table 25-15 Variables for creating storage for OCR and voting disk *(continued)*

Variable	List or Scalar	Description
$CFG{ocrvotevolname}	Scalar	Required Defines the volume name for OCR and voting disk. This variable must be used only if you have set the storage scheme to 1 (Clustered File System).
$CFG{ocrvotevolsize}	Scalar	Required Defines the size of the OCR and voting disk volume. This variable must be used only if you have set the storage scheme to 1 (Clustered File System).
$CFG{ocrvotemount}	Scalar	Required Defines the full path to the CFS mount point. This variable must be used only if you have set the storage scheme to 1 (Clustered File System).
$CFG{ocrvolname}	Scalar	Required Defines the volume name for OCR. This variable must be used only if you have set the storage scheme to 0 (CVM Raw Volumes).
$CFG{ocrvolsize}	Scalar	Required Defines the size of the OCR volume. This variable must be used only if you have set the storage scheme to 0 (CVM Raw Volumes).
$CFG{votevolname}	Scalar	Required Defines the volume name for voting disk. This variable must be used only if you have set the storage scheme to 0 (CVM Raw Volumes).

Table 25-15 Variables for creating storage for OCR and voting disk *(continued)*

Variable	List or Scalar	Description
$CFG{votevolsize}	Scalar	Required Defines the size of the voting disk volume. This variable must be used only if you have set the storage scheme to 0 (CVM Raw Volumes).
$CFG{oracle_user}	Scalar	Required Defines the name of the Oracle user.
$CFG{oracle_group}	Scalar	Required Defines the primary group of the Oracle user.

Table 25-16 lists the variables that are used to configure the private IP address and PrivNIC resource under VCS.

Table 25-16 Variables for configuring the private IP address and PrivNIC resource under VCS

Variable	List or Scalar	Description
$CFG{config_privnic}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the PrivNIC and private IP address information will be configured for Oracle Clusterware. The value 0 indicates that the PrivNIC and private IP address information will not be configured for Oracle Clusterware.
$CFG{privnic_resname}	Scalar	Required Defines the PrivNIC resource name in the `main.cf` file.

Table 25-16 Variables for configuring the private IP address and PrivNIC resource under VCS *(continued)*

Variable	List or Scalar	Description
$CFG{privnic_interface_priority}	String	Required Defines the priority that determines which NIC will be used in the event of a failover. Set the priority in decreasing order. For example, the following priority setting indicates that lan2 will be given priority in the event of a failover: **$CFG{privnic_interface_priority}="lan2 lan3";**

$CFG{*host1*}{privnicip}	Scalar	Required
		Defines the IP address to be configured for the PrivNIC resource on the node.
		Repeat this variable for each node in the cluster. For example, if you have two nodes in the cluster, you must provide this variable for each node.
		For example:
		`$CFG{galaxy}{privnicip} ="192.168.12.1"`
		`$CFG{nebula}{privnicip} ="192.168.12.2"`

$CFG{nic_reuseip}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the existing IP addresses in the `/etc/hosts` or `/etc/inet/ipnodes` files will be used. The value 0 indicates that the IP addresses will not be reused.

Table 25-16 Variables for configuring the private IP address and PrivNIC resource under VCS *(continued)*

Variable	List or Scalar	Description

$CFG{*host*}{hostname_for_ip}	Scalar	Required
		Defines the private node name of the IP address (*hostname_for_ip*) for the PrivNIC resource and the node (*system*) for which the resource is configured.
		Repeat this variable for each node in the cluster. For example, if you have two nodes in the cluster, you must provide this variable for each node.
		For example:
		`$CFG{galaxy}{hostname_for_ip} ="galaxy-priv"`
		`$CFG{nebula}{hostname_for_ip} ="galaxy-priv"`

$CFG{nic_netmask}	Scalar	Required Defines the netmask for the private network.
$CFG{nic_add_ip_to_files}	Scalar	Required Defines a Boolean value 0 or 1. **Note:** Make sure that the IP addresses for the NIC resource are not already present in the files or set the *$CFG{nic_reuseip}* and *$CFG{nic_reusealias}* variables, otherwise the network configuration step fails. The value 0 indicates that the IP addresses may already be present in the file.

Table 25-16 Variables for configuring the private IP address and PrivNIC resource under VCS *(continued)*

Variable	List or Scalar	Description
$CFG{nic_reconfigure_existing_resource}	Scalar	Optional Defines a Boolean value 0 or 1. The value 1 indicates that the existing PrivNIC resource in the `main.cf` file will be deleted and reconfigured. The value 0 indicates that the existing PrivNIC resource in the `main.cf` file will be reused.
$CFG{nic_reusealias}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the installer will not check the `/etc/hosts` file to determine whether the host name alias for the private IP addresses exist or not. The installer assumes that the host names alias information is present in the file. Make sure that the alias information is present in the file. The value 0 indicates that the installer checks whether the host name alias information is present in the `/etc/hosts` file. Make sure that the alias information is present in the file otherwise the installation fails.

Table 25-17 lists the variables that are used to configure the private IP addresses and the MultiPrivNIC resource under VCS.

Table 25-17 Variables for configuring the private IP addresses and the MultiPrivNIC resource under VCS

Variable	List or Scalar	Description
$CFG{config_multiprivnic}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the MultiPrivNIC and private IP address information will be configured for Oracle Clusterware. The value 0 indicates that the MultiPrivNIC and private IP address information will not be configured for Oracle Clusterware.
$CFG{multiprivnic_resname}	Scalar	Required Defines the MultiPrivNIC resource name in the `main.cf` file.
$CFG{nic_add_ip_to_files}	Scalar	Required Defines a Boolean value 0 or 1. **Note:** Make sure that the IP addresses for the NIC resource are not already present in the files or set the *$CFG{nic_reuseip}* and *$CFG{nic_reusealias}* variables, otherwise the network configuration step fails. The value 0 indicates that the IP addresses may already be present in the file.

Table 25-17 Variables for configuring the private IP addresses and the MultiPrivNIC resource under VCS *(continued)*

Variable	List or Scalar	Description

$CFG{*host1*}->{*NIC1*}->{multiprivnicip}	List	Required
		Defines the list of IP addresses for the MultiPrivNIC resource.
		Note: The private IP addresses must be configured for each node and each interface in the cluster.
		For example, if you have two nodes galaxy and nebula in the cluster:
		`$CFG{galaxy}{lan1}`
		`{multiprivnicip}="192.168.12.1";`
		`$CFG{galaxy}{lan2}`
		`{multiprivnicip}=="192.168.2.1";`
		`$CFG{nebula}{lan1}`
		`{multiprivnicip}="192.168.12.2";`
		`$CFG{nebula}{lan2}`
		`{multiprivnicip}="192.168.2.2";`

$CFG{*host1*}->{*NIC1*}->{hostname_for_ip}	List	Required
		Defines the list of private node names (*hostname_for_ip*) for the IP addresses configured in the MultiPrivNIC resource for the interface (*inf*) on the node (*system*) .
		Note: The private IP address must be configured for each node and each interface in the cluster.
		For example, if you have two nodes galaxy and nebula in the cluster:
		`$CFG{galaxy}{lan1}`
		`{hostname_for_ip}="galaxy-priv";`
		`$CFG{galaxy}{lan2}`
		`{hostname_for_ip}="galaxy-priv1";`
		`$CFG{nebula}{lan1}`
		`{hostname_for_ip}="nebula-priv";`
		`$CFG{nebula}{lan2}`
		`{hostname_for_ip}="nebula-priv1";`

Table 25-17 Variables for configuring the private IP addresses and the MultiPrivNIC resource under VCS *(continued)*

Variable	List or Scalar	Description
$CFG{nic_netmask}	Scalar	Required Defines the netmask for the private network.
$CFG{nic_reconfigure_existing_resource}	Scalar	Optional Defines a Boolean value 0 or 1. The value 1 indicates that the existing MultiPrivNIC resource in the `main.cf` file will be deleted and reconfigured. The value 0 indicates that the existing MultiPrivNIC resource in the `main.cf` file will be reused.
$CFG{nic_reuseip}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the existing IP addresses in the `/etc/hosts` or `/etc/inet/ipnodes` files will be used. The value 0 indicates that the IP addresses will not be reused.
$CFG{nic_reusealias}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the installer will not check the `/etc/hosts` file to determine whether the host name alias for the private IP addresses exist or not. The installer assumes that the host names alias information is present in the file. Make sure that the alias information is present in the file. The value 0 indicates that the installer checks whether the host name alias information is present in the `/etc/hosts` file. Make sure that the alias information is present in the file otherwise the installation fails.

Table 25-18 lists the variables that are used to install Oracle Clusterware.

Table 25-18 Variables for installing Oracle Clusterware

Variable	List or Scalar	Description
$CFG{install_oracle_clusterware}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that Oracle Clusterware will be configured. The value 0 indicates that Oracle Clusterware will not be configured.
$CFG{oracle_user}	Scalar	Required Defines the name of the Oracle user.
$CFG{oracle_group}	Scalar	Required Defines the primary group of the Oracle user.
$CFG{oracle_base}	Scalar	Required Defines the base directory for the Oracle RAC installation.
$CFG{crs_home}	Scalar	Required Defines the Oracle Clusterware home directory. The value in this variable must be the same as that of the 'ORACLE_HOME' variable in the Oracle Clusterware response file.
$CFG{crs_installpath}	Scalar	Required Defines the full path of the Oracle Clusterware installation binaries.
$CFG{oracle_version}	Scalar	Required Defines the version of the Oracle RAC binaries (for example, 11.2.0.1.0). This definition is overridden if a different Oracle RAC version is detected during the installation.

Table 25-18 Variables for installing Oracle Clusterware *(continued)*

Variable	List or Scalar	Description
$CFG{crs_responsefile}	Scalar	Required Defines the full path of the Oracle Clusterware response file.

Table 25-19 lists the variables that are used to install Oracle database.

Table 25-19 Variables for installing Oracle database

Variable	List or Scalar	Description
$CFG{install_oracle_database}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the Oracle RAC database will be configured. The value 0 indicates that the Oracle RAC database will not be configured.
$CFG{oracle_user}	Scalar	Required Defines the name of the Oracle user.
$CFG{oracle_group}	Scalar	Required Defines the primary group of the Oracle user.
$CFG{oracle_base}	Scalar	Required Defines the base directory for the Oracle RAC installation.
$CFG{crs_home}	Scalar	Required Defines the Oracle Clusterware home directory. The value in this variable must be the same as that of the 'ORACLE_HOME' variable in the Oracle Clusterware response file.

Table 25-19 Variables for installing Oracle database *(continued)*

Variable	List or Scalar	Description
$CFG{db_home}	Scalar	Required Defines the Oracle RAC database home directory. The value in this variable must be the same as that of the 'ORACLE_HOME' variable in the Oracle RAC database response file.
$CFG{db_installpath}	Scalar	Required Defines the full path of the Oracle RAC database installation binaries.
$CFG{oracle_version}	Scalar	Required Defines the version of the Oracle RAC binaries (for example, 11.2.0.1.0). This definition is overridden if a different Oracle RAC version is detected during the installation.
$CFG{db_responsefile}	Scalar	Required Defines the full path of the Oracle database response file.

Table 25-20 lists the variables that are used to configure CSSD resource.

Table 25-20 Variables for configuring CSSD resource

Variable	List or Scalar	Description
$CFG{config_cssd_agent}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the CSSD agent will be configured after Oracle RAC installation. The value 0 indicates that the CSSD agent will not be configured after Oracle RAC installation.

Table 25-20 Variables for configuring CSSD resource *(continued)*

Variable	List or Scalar	Description
$CFG{reconfigure_cssd_resource}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the SF Oracle RAC installer deletes the existing CSSD resource from the `main.cf` file and reconfigures it. The value 0 indicates that the SF Oracle RAC installer does not delete and reconfigure the resource. The installer exits the task with the message that the resource exists.

Table 25-21 lists the variables that are used to relink Oracle RAC libraries.

Table 25-21 Variables for relinking Oracle RAC libraries

Variable	List or Scalar	Description
$CFG{relink_oracle_database}	Scalar	Required Defines a Boolean value 0 or 1. The value 1 indicates that the SF Oracle RAC libraries will be relinked with the Oracle RAC database after Oracle RAC installation. The value 0 indicates that the SF Oracle RAC libraries will not be relinked with the Oracle RAC database after Oracle RAC installation.
$CFG{oracle_user}	Scalar	Required Defines the name of the Oracle user.
$CFG{oracle_group}	Scalar	Required Defines the primary group of the Oracle user.

Table 25-21 Variables for relinking Oracle RAC libraries *(continued)*

Variable	List or Scalar	Description
$CFG{crs_home}	Scalar	Required Defines the Oracle Clusterware home directory. The value in this variable must be the same as that of the 'ORACLE_HOME' variable in the Oracle Clusterware response file.
$CFG{db_home}	Scalar	Required Defines the Oracle RAC database home directory. The value in this variable must be the same as that of the 'ORACLE_HOME' variable in the Oracle RAC database response file.
$CFG{oracle_version}	Scalar	Required Defines the version of the Oracle RAC binaries (for example, 11.2.0.1.0). This definition is overridden if a different Oracle RAC version is detected during the installation.

Section 6

Adding or removing nodes from an SF Oracle RAC cluster

- Chapter 26. Adding a node to SF Oracle RAC clusters
- Chapter 27. Removing a node from SF Oracle RAC clusters

Chapter 26

Adding a node to SF Oracle RAC clusters

This chapter includes the following topics:

- About adding a node to a cluster
- Before adding a node to a cluster
- Preparing to add a node to a cluster
- Adding a node to a cluster
- Preparing the new node for installing Oracle RAC
- Adding the new node to Oracle RAC
- Updating the Storage Foundation for Databases (SFDB) repository after adding a node

About adding a node to a cluster

After you install SF Oracle RAC and create a cluster, you can add and remove nodes from the cluster.You can create clusters of up to 16 nodes.

You can add a node:

- Using the product installer
- Using the Web installer
- Manually

The example procedures describe how to add a node to an existing cluster with two nodes.

Before adding a node to a cluster

Before preparing to add the node to an existing SF Oracle RAC cluster, verify the following:

- Hardware and software requirements are met.
  See "Meeting hardware and software requirements" on page 432.
- Hardware is set up for the new node.
  See "Setting up the hardware" on page 432.
- The existing cluster is an SF Oracle RAC cluster and that SF Oracle RAC is running on the cluster.
- The new system has the same identical operating system versions and patch levels as that of the existing cluster.

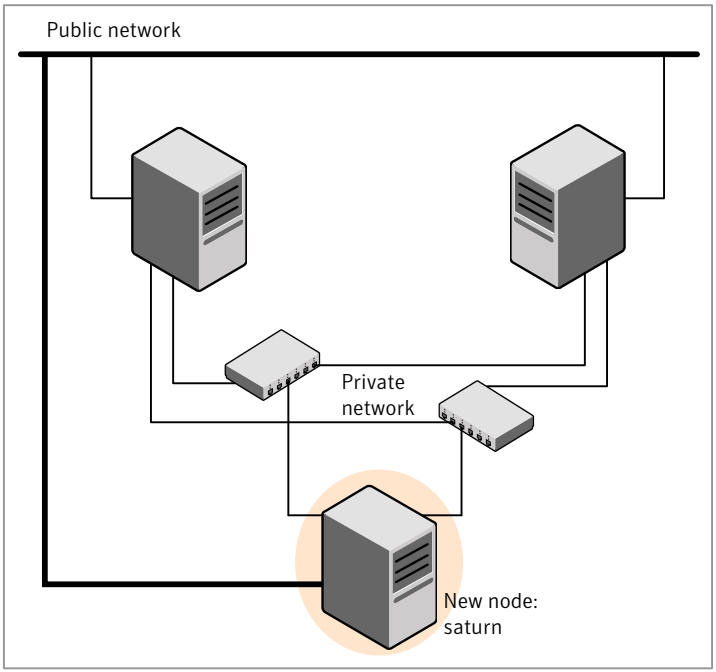
Meeting hardware and software requirements

The system you add to the cluster must meet the hardware and software requirements.

Setting up the hardware

Figure 26-1 shows that before you configure a new system on an existing cluster, you must physically add the system to the cluster.

Figure 26-1 Adding a node to a two-node cluster using two switches



To set up the hardware

1 Connect the SF Oracle RAC private Ethernet controllers.

Perform the following tasks as necessary:

- When you add nodes to a cluster, use independent switches or hubs for the private network connections. You can only use crossover cables for a cluster, so you might have to swap out the cable for a switch or hub.
- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

Figure 26-1 illustrates a new node being added to an existing two-node cluster using two independent hubs.

2 Make sure that you meet the following requirements:

- The node must be connected to the same shared storage devices as the existing nodes.
- The node must have private network connections to two independent switches for the cluster.
  For more information, see the *Veritas Cluster Server Installation Guide*.

- The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster.

Preparing to add a node to a cluster

Complete the following preparatory steps on the new node before you add the node to an existing SF Oracle RAC cluster.

To prepare the new node

1 Verify that the new node meets installation requirements.

```
# ./installsfrac -precheck saturn
```

2 Install SF Oracle RAC on the new system.

Note: Use the `-install` option to install SF Oracle RAC. Do not configure SF Oracle RAC after the installation.

```
Would you like to configure SF Oracle RAC on saturn [y, n, q] (n)
```

You can configure the new node later using the configuration from the existing cluster nodes.

See "About installing SF Oracle RAC " on page 87.

Adding a node to a cluster

You can use one of the following methods to add a node to an existing SF Oracle RAC cluster:

SF Oracle RAC installer	See "Adding a node to a cluster using the SF Oracle RAC installer" on page 434.
Manual	See "Adding the node to a cluster manually" on page 438.

Note: Before you add the node, make sure that SF Oracle RAC is not configured on the node.

Adding a node to a cluster using the SF Oracle RAC installer

You can add a node using the `-addnode` option with the SF Oracle RAC installer.

The SF Oracle RAC installer performs the following tasks:

- Verifies that the node and the existing cluster meet communication requirements.
- Verifies the products and packages installed on the new node.
- Discovers the network interfaces on the new node and checks the interface settings.
- Creates the following files on the new node:

  `/etc/llttab`

  `/etc/VRTSvcs/conf/sysname`
- Updates the following configuration files and copies them on the new node:

  `/etc/llthosts`

  `/etc/gabtab`

  `/etc/VRTSvcs/conf/config/main.cf`
- Copies the following files from the existing cluster to the new node:

  `/etc/vxfenmode`

  `/etc/vxfendg`

  `/etc/vcsmmtab`

  `/etc/vx/.uuids/clusuuid`
- Configures security on the new node if the existing cluster is a secure cluster.

  Warning: If the root broker system has failed, then you must recover or reconfigure the root broker system before you add a new node to the cluster.
- Configures disk-based or server-based fencing depending on the fencing mode in use on the existing cluster.
- Adds the new node to the CVM, ClusterService, and VxSS service groups in the VCS configuration.

  Note: For other service groups configured under VCS, update the configuration for the new node manually.
- Starts SF Oracle RAC processes and configures CVM and CFS on the new node.

At the end of the process, the new node joins the SF Oracle RAC cluster.

Note: If you have configured server-based fencing on the existing cluster, make sure that the CP server does not contain entries for the new node. If the CP server already contains entries for the new node, remove these entries before adding the node to the cluster, otherwise the process may fail with an error.

Caution: If you plan to use the SF Oracle RAC installer for completing the Oracle pre-installation tasks on the new node, do not quit the installer after adding the node to the cluster. If you quit the installer, you must perform the Oracle pre-installation tasks manually.

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 Oracle RAC installer with the -addnode option.

   ```
   # cd /opt/VRTS/install

   # ./installsfrac -addnode
   ```

   The installer displays the copyright message and the location where it stores the temporary installation logs.
3. Enter the name of a node in the existing SF Oracle RAC cluster. The installer uses the node information to identify the existing cluster.

   ```
   Enter one node of the SF Oracle RAC cluster to which
   you would like to add one or more nodes: galaxy
   ```
4. Review and confirm the cluster information.
5. Enter the name of the systems that you want to add as new nodes to the cluster.

   ```
   Enter the system names separated by spaces
   to add to the cluster: saturn
   ```

   The installer checks the installed products and packages on the nodes and discovers the network interfaces.

6 Enter the name of the network interface that you want to configure as the first private heartbeat link.

Note: The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster. The LLT configuration for the new node must be the same as that of the existing cluster.

```
Enter the NIC for the first private heartbeat
link on saturn: [b,q,?] lan1
```

7 Enter **y** to configure a second private heartbeat link.

Note: At least two private heartbeat links must be configured for high availability of the cluster.

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

8 Enter the name of the network interface that you want to configure as the second private heartbeat link.

```
Enter the NIC for the second private heartbeat link
on saturn: [b,q,?] lan2
```

9 Depending on the number of LLT links configured in the existing cluster, configure additional private heartbeat links for the new node.

The installer verifies the network interface settings and displays the information.

10 Review and confirm the information.

11 If you have configured SMTP, SNMP, or the global cluster option in the existing cluster, you are prompted for the NIC information for the new node.

```
Enter the NIC for VCS to use on saturn: lan3
```

12 If the existing cluster uses server-based fencing in secure mode, provide responses to the following installer prompts.

If you are using different root brokers for the CP server and the client SF Oracle RAC cluster, enter **y** to confirm the use of different root brokers. The installer attempts to establish trust between the new node being added to the cluster and the authentication broker of the CP server.

```
Are you using different Root Brokers for the CP Server(s) and the
client cluster? (If so then installer will try to establish trust
between the new node(s) being added and CP Server's
Authentication Broker) [y,n,q] (n) y
```

Enter the host name of the authentication broker used for any one of the CP servers.

```
Enter hostname of the Authentication Broker being used for any one
of the CP Server(s): [b] mycps1.symantecexample.com
```

Enter the port number where the authentication broker for the CP server listens to establish trust with the new node:

```
Enter the port where the Authentication Broker
mycps1.symantecexample.com for the CP Server(s) is listening
for establishing trust: [b] (2821)
```

The installer then starts all the required Veritas processes and joins the new node to cluster.

Note: Do not quit the installer if you want to perform the Oracle pre-installation tasks using the SF Oracle RAC installer.

---

13 Confirm using `lltstat -n` and `gabconfig -a`.

Adding the node to a cluster manually

Perform this procedure after you install SF Oracle RAC only if you plan to add the node to the cluster manually.

To add the node manually to the cluster

1 Start the Volume Manager.

See "Starting Volume Manager on the new node" on page 439.

2 Configure LLT, GAB, and VCSMM.

See "Configuring LLT, GAB, and VCSMM on the new node" on page 440.

3 If the existing cluster is a secure cluster, set up the new node to run in secure mode.

See "Setting up the node to run in secure mode" on page 442.

4 If the existing cluster is configured to use server-based I/O fencing, configure server-based I/O fencing on the new node.

See "Starting fencing on the new node" on page 447.

5 Start VCS.

See "To start VCS on the new node" on page 448.

6 Configure CVM and CFS.

See "Configuring CVM and CFS on the new node" on page 448.

7 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 450.

Starting Volume Manager on the new node

Volume Manager uses license keys to control access. As you run the `vxinstall` utility, answer **n** to prompts about licensing. You installed the appropriate license when you ran the `installsfrac` program.

To start Volume Manager on the new node

1 To start Veritas Volume Manager on the new node, use the vxinstall utility:

```
# vxinstall
```

2 VxVM uses license keys to control access. As you run the utility, answer "n" when prompted about licensing; you installed the appropriate license when you ran the installsfrac utility.

3 Enter **n** when prompted to set up a system wide disk group for the system.

The installation completes.

4 Verify that the daemons are up and running. Enter the command:

```
# vxdisk list
```

Make sure the output displays the shared disks without errors.

Configuring LLT, GAB, and VCSMM on the new node

Perform the steps in the following procedure to configure LLT, GAB, and VCSMM on the new node.

To configure LLT, GAB, and VCSMM on the new node

1 Edit the `/etc/llthosts` file on the existing nodes. Using vi or another text editor, add the line for the new node to the file. The file resembles:

```
0 galaxy
1 nebula
2 saturn
```

2 Copy the `/etc/llthosts` file from one of the existing systems over to the new system. The `/etc/llthosts` file must be identical on all nodes in the cluster.

3 Create an `/etc/lltab` file on the new system. For example:

```
set-node saturn
set-cluster 101

link lan1 /dev/lan:1 - ether --
link lan2 /dev/lan:2 - ether --
```

Except for the first line that refers to the node, the file resembles the `/etc/lltab` files on the existing nodes. The second line, the cluster ID, must be the same as in the existing nodes.

4 Use vi or another text editor to create the file `/etc/gabtab` on the new node. This file must contain a line that resembles the following example:

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

Where N represents the number of systems in the cluster. For a three-system cluster, N would equal 3.

5 Edit the `/etc/gabtab` file on each of the existing systems, changing the content to match the file on the new system.

6 Copy the following files from one of the nodes in the existing cluster to the new node:

```
/etc/rc.config.d/lltconf
/etc/rc.config.d/gabconf
/etc/rc.config.d/vcsconf
/etc/rc.config.d/vcsmmconf
/etc/rc.config.d/vxfenconf
/etc/vcsmmtab
```

7 Use vi or another text editor to create the file `/etc/VRTSvcs/conf/sysname` on the new node. This file must contain the name of the new node added to the cluster.

For example:

```
saturn
```

8 Create the Unique Universal Identifier file `/etc/vx/.uuids/clusuuid` on the new node:

```
# uuidconfig.pl -remsh -clus -copy \
-from_sys galaxy -to_sys saturn
```

9 Start the LLT, GAB, VCSMM, LMX, and ODM drivers on the new node:

```
# /sbin/init.d/llt start

# sbin/init.d/gab start

# /sbin/init.d/vxfen start

# sbin/init.d/vcsmm start

# sbin/init.d/lmx start

# kcmodule vxgms=loaded

# kcmodule odm=loaded

# /sbin/init.d/odm stop

# /sbin/init.d/odm start
```

10 On the new node, verify that the GAB port memberships are a, d, and o:

```
# gabconfig -a


GAB Port Memberships
===============================================================
Port a gen    df204 membership 012
Port d gen    df20a membership 012
Port o gen    df207 membership 012
```

Port h may also be present.In that case, run:

```
# hastop -local
```

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 26-1 uses the following information for the following command examples.

Table 26-1 The command examples definitions

Name	Fully-qualified host name (FQHN)	Function
saturn	saturn.nodes.example.com	The new node that you are adding to the cluster.
RB1	RB1.brokers.example.com	The root broker for the cluster
RB2	RB2.brokers.example.com	Another root broker, not the cluster's RB

To verify the existing security setup on the node

1. If node saturn is configured as an authentication broker (AB) belonging to a root broker, perform the following steps. Else, proceed to configuring the authentication broker on node saturn.

2. Find out the root broker to which the node saturn belongs using the following command.

```
# vssregctl -l -q -b \
"Security\Authentication\Authentication Broker" \
 -k "BrokerName"
```

3. If the node saturn already belongs to root broker RB1, it is configured as part of the cluster. Proceed to setting up VCS related security configuration.

4. If the node saturn belongs to a different root broker (for example RB2), perform the following steps to remove the security credentials from node saturn.

   - Kill `/opt/VRTSat/bin/vxatd` process.
   - Remove the credential that RB2 has given to AB on node saturn.

     ```
     # vssat deletecred --domain type:domainname \
     --prplname prplname
     ```

     For example:

     ```
     # vssat deletecred --domain vx:root@RB2.brokers.example.com \
     --prplname saturn.nodes.example.com
     ```

Configuring the authentication broker on node saturn

Configure a new authentication broker (AB) on node saturn. This AB belongs to root broker RB1.

To configure the authentication broker on node saturn

1 Create a principal for node saturn on root broker RB1. Execute the following command on root broker RB1.

```
# vssat addprpl --pdrtype root --domain domainname \
 --prplname prplname --password password \
 --prpltype service
```

For example:

```
# vssat addprpl --pdrtype root \
--domain root@RB1.brokers.example.com \
--prplname saturn.nodes.example.com \
--password flurbdicate --prpltype service
```

2 Ensure that there is no clock skew between the times on node saturn and RB1.

3 Copy the `/opt/VRTSat/bin/root_hash` file from RB1 to node saturn.

4 Configure AB on node saturn to talk to RB1.

```
# vxatd -o -a -n prplname -p password -x vx -y domainname -q \
rootbroker -z 2821 -h roothash_file_path
```

For example:

```
# vxatd -o -a -n saturn.nodes.example.com -p flurbdicate \
-x vx -y root@RB1.brokers.example.com -q RB1 \
-z 2821 -h roothash_file_path
```

5 Verify that AB is configured properly.

```
#  vssat showbrokermode
```

The command should return 1, indicating the mode to be AB.

Setting up SF Oracle RAC related security configuration

Perform the following steps to configure SF Oracle RAC related security settings.

Setting up SF Oracle RAC related security configuration

1 Start `/opt/VRTSat/bin/vxatd` process.

2 Create HA_SERVICES domain for SF Oracle RAC.

```
# vssat createpd --pdrtype ab --domain HA_SERVICES
```

3 Add SF Oracle RAC and webserver principal to AB on node saturn.

```
# vssat addprpl --pdrtype ab --domain HA_SERVICES --prplname
webserver_VCS_prplname --password new_password --prpltype
service --can_proxy
```

4 Create `/etc/VRTSvcs/conf/config/.secure` file.

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

Configuring server-based fencing on the new node

Perform this step if your existing cluster uses server-based I/O fencing.

To configure server-based fencing on the new node

1 Log in to each CP server as the root user.

2 Update each CP server configuration with the new node information:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt \
-a add_node -c clus1 -u {f0735332-1dd1-11b2} -h saturn -n2
Node 2 (saturn) successfully added
```

3 Verify that the new node is added to the CP server configuration:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt -a list_nodes
```

The new node must be listed in the output.

4 Add the VCS user `cpsclient@saturn` to each CP server:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt \
-a add_user -e cpsclient@saturn \
-f cps_operator -g vx
User cpsclient@saturn successfully added
```

To configure server-based fencing with security on the new node

1 As the root user, create the VCS user and the domain on the new node:

- Create a dummy configuration file `/etc/VRTSvcs/conf/config/main.cf` that resembles the following example:

```
# cat main.cf
include "types.cf"
cluster clus1 {
    SecureClus = 1
   }
system saturn {
 }
```

- Start VCS in one node mode on the new node:

```
# /opt/VRTSvcs/bin/hastart -onenode
```

2 Verify that the VCS user and the domain are created on the new node:

```
# /opt/VRTScps/bin/cpsat showcred | grep _HA_VCS_
# /opt/VRTScps/bin/cpsat listpd -t local | grep HA_SERVICES
```

3 Stop VCS if the VCS user and domain are created successfully on the new node:

```
# /opt/VRTSvcs/bin/hastop
```

4 If the root broker for the CP server and the new node are different, run the following command to establish trust between the authentication broker of the CP Server and the new node:

```
# /usr/bin/echo y | /opt/VRTScps/bin/cpsat setuptrust \
-b thunderbolt -s high
```

5 Log in to each CP server as the root user.

6 Update each CP server configuration with the new node information:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt \
-a add_node -c clus1 -u {f0735332-1dd1-11b2} -h saturn -n2
Node 2 (saturn) successfully added
```

7 Verify that the new node is added to the CP server configuration:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt -a list_nodes
```

The new node must be listed in the output.

8 Add the VCS user `_HA_VCS_saturn@HA_SERVICES@saturn.veritas.com` to each CP server:

```
# /opt/VRTScps/bin/cpsadm -s thunderbolt \
-a add_user -e _HA_VCS_saturn@HA_SERVICES@saturn.veritas.com \
-f cps_operator -g vx
User _HA_VCS_saturn@HA_SERVICES@saturn.veritas.com successfully added
```

Starting fencing on the new node

Perform the following steps to start fencing on the new node.

To start fencing on the new node

1 If you are using disk-based fencing on at least one node, copy the following files from one of the nodes in the existing cluster to the new node:

```
/etc/default/vxfen
/etc/vxfendg
/etc/vxfenmode
```

If you are using pure CP server-based fencing on the existing cluster, then only the `/etc/vxfenmode` file needs to be copied on the new node.

2 Start fencing on the new node:

3 On the new node, verify that the GAB port memberships are a, b, d, h and o:

```
# gabconfig -a

GAB Port Memberships
===============================================================
Port a gen    df204 membership 012
Port b gen    df20d membership 012
Port d gen    df20a membership 012
Port o gen    df207 membership 012
```

After adding the new node

If you added the new node to the cluster manually, before you starting VCS you must create the file `cssd-pretend-offline` on the new node and make the `cssd`

resource non-critical. Failing this, the `cssd` resource lapses into an UNKNOWN state until Oracle Clusterware is installed on the new node, thus preventing the `cvm` group from coming online.

If you used the product installer to add the new node to the cluster, you will not need to perform this step.

Note: The `cssd` resource will remain in FAULTED/OFFLINE state till Oracle Clusterware is installed on the new node.

Start VCS on the new node.

To start VCS on the new node

1. If you installed the new node manually:
   - On one of the nodes in the existing cluster, configure the `cssd` resource as a non-critical resource:

     ```
     # haconf -makerw
     # hares -modify cssd Critical 0
     # haconf -dump -makero
     ```

   - Create the file `cssd-pretend-offline` on the new node:

     ```
     # touch /var/VRTSvcs/lock/cssd-pretend-offline
     ```

2. Start VCS on the new node:

   ```
   # hastart
   ```

   VCS brings the CVM and CFS groups online.

3. Verify that the CVM and CFS groups are online:

   ```
   # hagrp -state
   ```

Configuring CVM and CFS on the new node

Modify the existing cluster configuration to configure CVM and 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 saturn
```

4 To enable the existing cluster to recognize the new node, run the following commands on one of the existing nodes:

```
# hagrp -modify cvm SystemList -add saturn 2

# hagrp -modify cvm AutoStartList -add saturn

# hares -modify cvm_clus CVMNodeId -add saturn 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 \
saturn:/etc/VRTSvcs/conf/config/main.cf
# rcp /etc/VRTSvcs/conf/config/CFSTypes.cf \
saturn:/etc/VRTSvcs/conf/config/CFSTypes.cf
# rcp /etc/VRTSvcs/conf/config/CVMTypes.cf \
saturn:/etc/VRTSvcs/conf/config/CVMTypes.cf
```

Configuring the ClusterService group for the new node

If the ClusterService group is configured on the existing cluster, add the node to the group by performing the steps in the following procedure on one of the nodes in the existing cluster.

To configure the ClusterService group for the new node

1 On an existing node, for example galaxy, write-enable the configuration:

```
# haconf -makerw
```

2 Add the node saturn to the existing ClusterService group.

```
# hagrp -modify ClusterService SystemList -add saturn 2

# hagrp -modify ClusterService AutoStartList -add saturn
```

3 Modify the IP address and NIC resource in the existing group for the new node.

```
# hares -modify gcoip Device lan0 -sys saturn

# hares -modify gconic Device lan0 -sys saturn
```

4 Save the configuration by running the following command from any node.

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

Preparing the new node for installing Oracle RAC

You must complete certain pre-installation tasks before you add the node to Oracle RAC.

Use one of the following ways to complete the preparatory tasks:

Using the SF Oracle RAC installer	See "Preparing the new nodes for installing Oracle RAC using the SF Oracle RAC installer" on page 451.
Manual	See "Preparing the new node manually for installing Oracle RAC" on page 458.

Note: Some of the pre-installation tasks can be completed using the SF Oracle RAC installer while some of the tasks must be completed manually as indicated in the procedures.

Preparing the new nodes for installing Oracle RAC using the SF Oracle RAC installer

The SF Oracle RAC installer performs the following tasks:

- Creates the Oracle user and groups on the new node
- Configures the private IP addresses and the PrivNIC or MultiPrivNIC resources (if they are configured in the existing cluster).
- If the CFSMount and CVMVolDg resources for OCR and voting disk are configured under the `cvm` service group, the installer brings them online after adding the node to the cluster.
  If the resources are configured in any other service group, make sure that you modify the service group to include the new node and bring the service group online.

  Note: If OCR and voting disk are not configured under VCS, manually mount the OCR and voting disk after you finish the steps in the following procedure.

- Starts the CVM group on the new node.

To prepare to install Oracle RAC on the new node using the SF Oracle RAC installer

1 After you configure SF Oracle RAC on the new node, the installer displays the following options for configuring Oracle RAC:

```
1)  Create Oracle User and Group
2)  Configure private IP addresses (PrivNIC configuration)
3)  Configure private IP addresses (MultiPrivNIC configuration)
4)  Finish
```

Note: The options 2 and 3 are displayed only if you have configured private IP addresses as PrivNIC or MultiPrivNIC resources in the existing cluster.

Enter **1** to select the option **Create Oracle User and Group** from the SF Oracle RAC installer menu.

See "Creating Oracle user and groups on the new node" on page 454.

2 Configure the private IP addresses and the PrivNIC resource for Oracle Clusterware (only if the IP addresses on the existing cluster are configured as PrivNIC resources).

You must manually update the PrivNIC resource configuration in the following cases:

- If the PrivNIC resource on the existing cluster is configured under a group other than `cvm`.
- If the `Device` attribute in the PrivNIC resource configuration on the existing cluster is not configured for each node as follows:

```
Device@galaxy = {lan1=0, lan2=1}
Device@nebula = {lan1=0, lan2=1}
```

Enter **2** to select the option **Configure private IP addresses (PrivNIC configuration)**.

See "Configuring the private IP addresses and PrivNIC resource for Oracle Clusterware" on page 454.

3 Configure private IP addresses and the MultiPrivNIC resource for Oracle Clusterware and Oracle UDP IPC (only if the IP addresses on the existing cluster are configured as MultiPrivNIC resources).

You must manually update the MultiPrivNIC resource configuration in the following cases:

- If the MultiPrivNIC resource on the existing cluster is configured under a group other than `cvm`.
- If the `Device` attribute in the MultiPrivNIC resource configuration on the existing cluster is not configured for each node as follows:

```
Device@galaxy = {lan1=0, lan2=1, lan3=2}
Device@nebula = {lan1=0, lan2=1, lan3=2}
```

Enter **3** to select the option **Configure private IP addresses (MultiPrivNIC configuration)**.

See "Configuring the private IP addresses and MultiPrivNIC resource for Oracle Clusterware and Oracle UDP IPC" on page 456.

4 Select **Finish** to start the `cvm` group on the new node.

Note: The `cssd` resource appears FAULTED until the new node is added to Oracle Clusterware.

---

5 If the `cssd` resource is configured as a critical resource, the cvm group will be brought offline on the new node. Modify the configuration to make the `cssd` resource non-critical and bring the `cvm` group online.

- On one of the nodes in the existing cluster, configure the `cssd` resource as a non-critical resource:

```
# haconf -makerw
# hares -modify cssd Critical 0
# haconf -dump -makero
```

- Bring the cvm group online:

```
# hares -online cvm -sys saturn
```

6 Verify that all the GAB ports are up:

```
# gabconfig -a

GAB Port Memberships
===============================================================
Port a gen ada401 membership 012
Port b gen ada40d membership 012
Port d gen ada409 membership 012
Port f gen ada41c membership 012
Port h gen ada40f membership 012
Port o gen ada406 membership 012
Port u gen ada416 membership 012
Port v gen ada416 membership 012
Port w gen ada418 membership 012
```

7 Complete the following additional preparatory tasks using the instructions in the chapter "Preparing to install Oracle RAC":

- Identify public virtual IP addresses for use by Oracle RAC.
- Set the kernel parameters.
- Verify that the user "nobody" exists.
- Set up Oracle user equivalence for remote shell and remote copy environments.
- Edit the Oracle user profile.
- If the OCR and voting disk resources are not configured under VCS, mount the OCR and voting disk manually.

8 Create Oracle Clusterware and Oracle RAC database home directories manually.

Creating Oracle user and groups on the new node

Perform the steps in the following procedure to create Oracle user and groups on the new node.

Note: Set the password of the Oracle user manually before you configure secure shell or remote shell connection on the node.

To create Oracle user and groups on the new node

1 Enter the Oracle user name that is used for Oracle RAC operations on the existing cluster.

Note: If the Oracle user and groups already exist on the new node, make sure that the UID and GID of the Oracle user and groups are the same as that on the current cluster.

```
Enter Oracle UNIX user name:  [b] Oracle
```

The installer obtains the existing group and identifier information based on the Oracle user name.

2 Review and confirm the information.

The installer adds the user and groups to the new node.

3 Press **Return** to continue with the other configuration tasks.

Configuring the private IP addresses and PrivNIC resource for Oracle Clusterware

Perform this step only if the private IP addresses are configured as PrivNIC resources in the existing cluster.

Note: Make sure that the network interface names of the private interconnects on the new node are the same as those of the existing cluster. For maximum failover options, all available LLT links are used for PrivNIC configuration.

Review the pre-configuration information displayed by the installer and ensure that you meet the requirements.

To configure the private IP addresses and PrivNIC resource for Oracle Clusterware

1 Enter the name for the PrivNIC resource. The installer displays the names of the existing PrivNIC resources. Specify the name of an existing resource.

```
Enter the PrivNIC resource name: [b] (ora_priv)
```

2 Enter **y** if you want the installer to add the IP address to the `/etc/hosts` file.

You can also add the IP address to the file manually after the configuration.

The installer displays the existing PrivNIC resource configuration on the cluster.

```
Resource name: ora_priv
System: galaxy
        Private Interfaces: lan1 lan2
        Private IP address: 192.168.12.1
        Alias for above IP: galaxy-priv
System: nebula
        Private Interfaces: lan1 lan2
        Private IP address: 192.168.12.2
        Alias for above IP: nebula-priv
Is this information correct? [y,n,q] (y)
```

3 Review and confirm the information.

4 Enter the private IP address and its private node name for the new node.

```
Enter the private IP for saturn: [b] 192.168.12.5
Enter Hostname alias for the above IP address: [b] saturn-priv
```

The installer displays the resource configuration for the new node.

```
Resource name: ora_priv
System: saturn
        Private Interfaces: lan1 lan2
        Private IP address: 192.168.12.5
        Alias for above IP: saturn-priv
Is this information correct? [y,n,q] (y)
```

5 Review and confirm the information.

The installer updates the existing PrivNIC resource with the resource configuration for the new node and updates the `/etc/hosts` file on the new node as well as on the existing nodes (if you chose to update the file through the installer).

6 Press **Return** to continue with the other configuration tasks.

Configuring the private IP addresses and MultiPrivNIC resource for Oracle Clusterware and Oracle UDP IPC

Perform this step only if the private IP addresses are configured as MultiPrivNIC resources in the existing cluster.

Note: Make sure that you configure the same interfaces (as those on the existinnebulag cluster) for private interconnects on the new node. For maximum failover options, all available LLT links are used for MultiPrivNIC configuration.

Review the pre-configuration information displayed by the installer and ensure that you meet the requirements.

To configure the private IP addresses and MultiPrivNIC resource for Oracle Clusterware and Oracle UDP IPC

1 Enter the name for the MultiPrivNIC resource. The installer displays the names of the existing MultiPrivNIC resources. Specify the name of an existing resource.

```
Enter the MultiPrivNIC resource name: [b] (multi_priv)
```

2 Enter **y** if you want the installer to add the IP address to the `/etc/hosts` file.

You can also add the IP address to the file manually after the configuration.

The installer displays the existing MultiPrivNIC resource configuration on the cluster.

```
Resource name: multi_priv
System: galaxy
        Private Interfaces: lan1 lan2
        Private IPs on lan1: 192.168.12.1
        Aliases for above IPs: galaxy-priv
        Private IPs on lan2: 192.168.2.1
        Aliases for above IPs: galaxy-priv1
System: nebula
        Private Interfaces: lan1 lan2
        Private IPs on lan1: 192.168.12.2
        Aliases for above IPs: nebula-priv
        Private IPs on lan2: 192.168.2.2
        Aliases for above IPs: nebula-priv1
Is this information correct? [y,n,q] (y)
```

3 Review and confirm the information.

4 Enter the private IP address and the corresponding private node name for the lan1 interface on the new node.

```
Enter IP addresses for saturn for lan1
separated by space: [b,q,?]  192.168.12.5
Enter Hostname aliases for the above IP addresses
separated by space: [b,q,?] saturn-priv
```

5 Enter the private IP address and the corresponding private node name for the lan2 interface on the new node.

```
Enter IP addresses for saturn for lan2
separated by space: [b,q,?]  192.168.2.6
Enter Hostname aliases for the above IP addresses
separated by space: [b,q,?] saturn-priv1
```

The installer displays the resource configuration for the new node.

```
Resource name: multi_priv
System: saturn
        Private Interfaces: lan1 lan2
        Private IPs on lan1: 192.168.12.5
        Aliases for above IPs: saturn-priv
        Private IPs on lan2: 192.168.2.6
        Aliases for above IPs: saturn-priv1
Is this information correct? [y,n,q] (y)
```

6 Review and confirm the information.

The installer updates the existing MultiPrivNIC resource with the resource configuration for the new node and updates the `/etc/hosts` file on the new node as well as on the existing nodes (if you chose to update the file through the installer).

7 Press **Return** to continue with the other configuration tasks.

Preparing the new node manually for installing Oracle RAC

Complete the following preparatory tasks manually before you install Oracle RAC on the new node.

To prepare to install Oracle RAC on the new node

1 Create Oracle user and groups.

See "Creating the Oracle user and groups manually" on page 281.

2 Configure private IP addresses and the PrivNIC resource for Oracle Clusterware.

See "Configuring private IP address and PrivNIC resource for Oracle Clusterware" on page 459.

3 Configure private IP addresses and the MultiPrivNIC resource for Oracle Clusterware and Oracle UDP IPC.

See "Configuring private IP addresses and MultiPrivNIC resource for Oracle Clusterware and UDP IPC" on page 460.

4 Start VCS on the new node.

See "Starting VCS on the new node" on page 461.

5 Create the Oracle Clusterware/Grid Infrastructure and Oracle RAC database home directories for installation.

See "Creating Oracle Clusterware/Grid Infrastructure and Oracle database home directories on the new node " on page 462.

6 Complete the following additional preparatory tasks using the instructions in the chapter "Preparing to install Oracle RAC":

- Identify public virtual IP addresses for use by Oracle RAC.
- Set the kernel parameters.
- Verify that the user "nobody" exists.
- Set up Oracle user equivalence for remote shell and remote copy environments.
- Edit the Oracle user profile.

Configuring private IP address and PrivNIC resource for Oracle Clusterware

This section provides instructions for configuring private IP address and PrivNIC resource for Oracle Clusterware.

Identify a private IP address that you want to use for the new node. Make sure that the IP address is in the same subnet as the existing cluster.

The procedure uses the following IP address for the new node:

On saturn:	192.168.12.5

To configure private IP addresses for Oracle Clusterware

1 Make a backup copy of the main.cf file. For example:

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

# cp main.cf main.cf.2node
```

2 Add the private IP address to the the `ora_priv` resource on the active node:

```
# haconf -makerw

# hares -modify ora_priv Device -add lan1 0 -sys saturn

# hares -modify ora_priv Device -add lan2 1 -sys saturn

# hares -modify ora_priv Address "192.168.12.5" -sys saturn

# haconf -dump -makero
```

Configuring private IP addresses and MultiPrivNIC resource for Oracle Clusterware and UDP IPC

This section provides instructions for configuring private IP addresses and MultiPrivNIC resource for Oracle Clusterware and UDP IPC.

Identify the private IP addresses that you want to use for the new node. Make sure that the IP addresses are in the same subnet as the existing cluster.

The procedure uses the following IP addresses for the new node:

On saturn:	192.168.12.5
	192.168.2.6

To configure private IP addresses for Oracle Clusterware

- Use the following commands to add private IP into multi_priv resource on the active node:

```
# haconf -makerw
# hares -modify multi_priv Device  -add  lan1 0   -sys saturn
# hares -modify multi_priv Device  -add  lan2 1 -sys saturn
# hares -modify multi_priv Address -add 192.168.12.5 0 -sys saturn
# hares -modify multi_priv Address  -add 192.168.2.6 1  -sys saturn
# haconf -dump -makero
```

Starting VCS on the new node

Before you start VCS, create the file `cssd-pretend-offline` on the new node and make the `cssd` resource non-critical. Failing this, the `cssd` resource lapses into an UNKNOWN state until Oracle Clusterware is installed on the new node, thus preventing the `cvm` group from coming online.

Note: The `cssd` resource will remain in FAULTED/OFFLINE state till Oracle Clusterware is installed on the new node.

To start VCS on the new node

1. On one of the nodes in the existing cluster, configure the `cssd` resource as a non-critical resource:

```
# haconf -makerw
# hares -modify cssd Critical 0
# haconf -dump -makero
```

2. Create the file `cssd-pretend-offline` on the new node:

```
# touch /var/VRTSvcs/lock/cssd-pretend-offline
```

3. Start VCS on the new node:

```
# hastart
```

Creating Oracle Clusterware/Grid Infrastructure and Oracle database home directories on the new node

The Oracle Clusterware/Grid Infrastructure and Oracle database home directories must be located on the same storage as that on the existing nodes.

Depending on the storage in the existing cluster, use one of the following options to create the directories:

Local file system	See "To create the directories on the local file system" on page 462.
Veritas File System	See "To create the file system and directories on the Veritas File system (VxFS) " on page 462.
Cluster File System	See "To create the file system and directories on cluster file system" on page 467.

To create the directories on the local file system

1. Log in as the root user on each node.
2. Create the directories and set the ownership and permissions:

   For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

   ```
   # mkdir -p /u01/app/oracle
   # mkdir -p /u01/app/oracle/product/10.2.0/crshome
   # mkdir -p /u01/app/oracle/product/10.2.0/dbhome_1
   # chown -R oracle:oinstall /u01/app
   # chmod -R 775 /u01/app
   ```

   For Oracle RAC 11g Release 2:

   ```
   # mkdir -p /u01/app/gridbase
   # mkdir -p /u01/app/grid/product/11.2.0/gridhome
   # chown -R grid:oinstall /u01/app
   # chmod -R 775 /u01/app

   # mkdir -p /u01/app/oracle
   # mkdir -p /u01/app/oracle/product/11.2.0/dbhome_1
   # chown -R oracle:oinstall /u01/app/oracle
   # chmod -R 775 /u01/app/oracle
   ```

To create the file system and directories on the Veritas File system (VxFS)

The sample commands in the procedure are for node saturn. Repeat the steps on each node of the cluster.

1 As the root user, create a VxVM local diskgroup `bindg_hostname` on each node.

Make sure that the size of the disk group is approximately 12 GB; if not, add another disk to the disk group.

```
# vxdg init bindg_saturn Disk_1
```

2 Create separate volumes for Oracle Clusterware/Oracle Grid Infrastructure (`crsbinvol`) binaries and Oracle binaries (`orabinvol`):

```
# vxassist -g bindg_saturn make crsbinvol 5G
# vxassist -g bindg_saturn make orabinvol 7G
```

3 Create the directories for Oracle RAC.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# mkdir -p /u01/app/oracle
# mkdir -p /u01/app/oracle/product/10.2.0/crshome
# mkdir -p /u01/app/oracle/product/10.2.0/dbhome_1
```

For Oracle RAC 11g Release 2:

```
# mkdir -p /u01/app/gridbase
# mkdir -p /u01/app/grid/product/11.2.0/gridhome
# mkdir -p /u01/app/oracle
# mkdir -p /u01/app/oracle/product/11.2.0/dbhome_1
```

4 Create file systems with the volumes `crsbinvol` and `orabinvol`:

```
# mkfs -F vxfs /dev/vx/rdsk/bindg_saturn/crsbinvol
# mkfs -F vxfs /dev/vx/rdsk/bindg_saturn/orabinvol
```

5 Mount the file systems on the new node.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# mount -F vxfs /dev/vx/dsk/bindg_saturn/crsbinvol \
/u01/app/oracle/product/10.2.0/crshome
# mount -F vxfs /dev/vx/dsk/bindg_saturn/orabinvol \
/u01/app/oracle/product/10.2.0/dbhome_1
```

For Oracle RAC 11g Release 2:

```
# mount -F vxfs /dev/vx/dsk/bindg_saturn/crsbinvol \
/u01/app/grid/product/11.2.0/gridhome
# mount -F vxfs /dev/vx/dsk/bindg_saturn/orabinvol \
/u01/app/oracle/product/11.2.0/dbhome_1
```

6 Set appropriate ownership and permissions for the directories.

Note: For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: The ownership and permissions must be changed on all nodes of the cluster because `/u01/app/oracle` must be owned by oracle:oinstall, otherwise `/u01/app/oracle/oraInventory` does not get created correctly on all the nodes. This can cause the Oracle Universal Installer to fail.

For Oracle RAC 11g Release 2: The ownership and permissions must be changed on all nodes of the cluster because `/u02/app` must be owned by grid:oinstall, otherwise `/u02/app/oraInventory` does not get created correctly on all the nodes. This can cause the Oracle Universal Installer to fail.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# chown -R oracle:oinstall /u01/app
# chmod -R 775 /u01/app
```

For Oracle RAC 11g Release 2:

```
# chown -R grid:oinstall /u01/app
# chmod -R 775 /u01/app
# chown -R oracle:oinstall /u01/app/oracle
# chmod -R 775 /u01/app/oracle
```

7 Add the resources to the VCS configuration.

See "To add the storage resources created on VxFS to the VCS configuration" on page 465.

To add the storage resources created on VxFS to the VCS configuration

1 Change the permissions on the VCS configuration file:

```
# haconf -makerw
```

2 Configure the VxVM volumes under VCS:

```
# hares -add bin_dg DiskGroup cvm
# hares -modify bin_dg DiskGroup bindg_saturn -sys saturn
# hares -modify bin_dg Enabled 1
```

3 Set up the file system under VCS:

```
# hares -add crsbin_mnt Mount cvm
```

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# hares -modify crsbin_mnt MountPoint \
"/u01/app/oracle/product/10.2.0/crshome"
```

For Oracle RAC 11g Release 2:

```
# hares -modify crsbin_mnt MountPoint \
"/u01/app/grid/product/11.2.0/gridhome"
```

The following commands are common to all Oracle RAC versions:

```
# hares -modify crsbin_mnt BlockDevice \
"/dev/vx/dsk/bindg_saturn/crsbinvol" -sys saturn
# hares -modify crsbin_mnt FSType vxfs
# hares -modify crsbin_mnt FsckOpt "-y"
# hares -modify crsbin_mnt Enabled 1
# hares -add orabin_mnt Mount cvm
```

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# hares -modify orabin_mnt MountPoint \
"/u01/app/oracle/product/10.2.0/dbhome_1"
```

For Oracle RAC 11g Release 2:

```
# hares -modify orabin_mnt MountPoint \
"/u01/app/oracle/product/11.2.0/dbhome_1"
```

The following commands are common to all Oracle RAC versions:

```
# hares -modify orabin_mnt BlockDevice \
"/dev/vx/dsk/bindg_saturn/orabinvol" -sys saturn
# hares -modify orabin_mnt FSType vxfs
# hares -modify orabin_mnt FsckOpt "-n"
# hares -modify orabin_mnt Enabled 1
```

4 Link the parent and child resources:

```
# hares -link crsbin_mnt bin_dg
# hares -link orabin_mnt bin_dg
```

To create the file system and directories on cluster file system

1 As the root user, create a VxVM shared disk group `bindg`:

```
# vxdg -s init bindg Disk_1
```

2 Set the activation mode for the disk group on all the nodes:

```
# vxdg -g bindg set activation=sw
```

3 From the CVM master node, start the disk group:

```
# vxvol -g bindg startall
```

4 Create separate volumes for Oracle Clusterware/Oracle Grid Infrastructure (`crsbinvol`) and Oracle database (`orabinvol`):

```
# vxassist -g bindg make crsbinvol 5G
# vxassist -g bindg make orabinvol 7G
```

5 Create the following directories for Oracle. The file system and directories created on shared storage in this procedure are based on the following layout:

$ORACLE_BASE	*/u01/app/oracle* /u01/app/oracle is on local storage. For Oracle RAC 11g Release 2, create a separate Oracle base directory for the grid user, in addition to the directory for the Oracle user: */u01/app/gridbase* /u01/app/gridbase is on local storage.
$CRS_HOME (For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1)	*/u01/app/oracle/product/10.2.0/crshome* /u01/app/oracle/product/10.2.0 is on local storage. /u01/app/oracle/product/10.2.0/crshome is on shared storage.
$GRID_HOME (For Oracle RAC 11g Release 2)	*/u01/app/grid/product/11.2.0/gridhome* /u01/app/grid/product/11.2.0 is on local storage. /u01/app/grid/product/11.2.0/gridhome is on shared storage.
$ORACLE_HOME	*/u01/app/oracle/product/release/dbhome_1* where *release* is 10.2.0, 11.1.0, or 11.2.0 depending on the Oracle RAC version /u01/app/oracle/product/*release* is on local storage. /u01/app/oracle/product/*release*/dbhome_1 is on shared storage.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# mkdir -p /u01/app/oracle
# mkdir -p /u01/app/oracle/product/10.2.0/crshome
# mkdir -p /u01/app/oracle/product/10.2.0/dbhome_1
```

For Oracle RAC 11g Release 2:

```
# mkdir -p /u01/app/gridbase
# mkdir -p /u01/app/grid/product/11.2.0/gridhome
# mkdir -p /u01/app/oracle
# mkdir -p /u01/app/oracle/product/11.2.0/dbhome_1
```

6 Create file systems with the volumes `crsbinvol` and `orabinvol`:

```
# mkfs -F vxfs /dev/vx/rdsk/bindg/crsbinvol
# mkfs -F vxfs /dev/vx/rdsk/bindg/orabinvol
```

7 Mount the file systems on the new node.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# mount -F vxfs -o cluster /dev/vx/dsk/bindg/crsbinvol \
/u01/app/oracle/product/10.2.0/crshome
# mount -F vxfs -o cluster /dev/vx/dsk/bindg/orabinvol \
/u01/app/oracle/product/10.2.0/dbhome_1
```

For Oracle RAC 11g Release 2:

```
# mount -F vxfs -o cluster /dev/vx/dsk/bindg/crsbinvol \
/u01/app/grid/product/11.2.0/gridhome
# mount -F vxfs -o cluster /dev/vx/dsk/bindg/orabinvol \
/u01/app/oracle/product/11.2.0/dbhome_1
```

8 Change the ownership and permissions on the new node.

Note: For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: The ownership and permissions must be changed on all nodes of the cluster because `/u01/app/oracle` must be owned by oracle:oinstall, otherwise `/u01/app/oracle/oraInventory` does not get created correctly on all the nodes. This can cause the Oracle Universal Installer to fail.

For Oracle RAC 11g Release 2: The ownership and permissions must be changed on all nodes of the cluster because `/u01/app` must be owned by grid:oinstall, otherwise `/u01/app/oraInventory` does not get created correctly on all the nodes. This can cause the Oracle Universal Installer to fail.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# chown -R oracle:oinstall /u01/app
# chmod -R 775 /u01/app
```

For Oracle RAC 11g Release 2:

```
# chown -R grid:oinstall /u01/app
# chmod -R 775 /u01/app
# chown -R oracle:oinstall /u01/app/oracle
# chmod -R 775 /u01/app/oracle
```

9 Add the CVMVolDg and CFSMount resources to the VCS configuration.

See "To add the CFSMount and CVMVolDg resources to the VCS configuration using CLI" on page 319.

Adding the new node to Oracle RAC

Install Oracle Clusterware and Oracle RAC database on the node using the Oracle RAC add node procedure.

For instructions, see the Oracle RAC documentation.

After installing Oracle Clusterware and Oracle RAC database, perform the following post-installation tasks:

1. Delete the file `/var/VRTSvcs/lock/cssd-pretend-offline` to bring the CSSD resource online.
2. If CSSD is not configured under the cvm group, add the new node information to the service group containing the CSSD resource.

3. Add new Oracle RAC database instances for the new node.

   For instructions, see the Oracle RAC documentation.

4. Add Oracle UDP IPC private IP addresses to the Oracle `init.ora` file.

5. Update the Oracle RAC database service groups to include the new database instances in the VCS configuration file.

6. For other service groups that are configured under VCS, manually update the service group configuration for the new node.

Updating the Storage Foundation for Databases (SFDB) repository after adding a node

If you are using Database Checkpoints, Database Flashsnap, or Adding a Node in your configuration, update the SFDB repository to enable access for the new node after it is added to the cluster.

To update the SFDB repository after adding a node

1 Run the following to change permission, owner, group of various SFDB directories on the newly added node:

```
# sfua_db_config
```

2 Run the `dbed_update` command on any one node in the cluster. For example:

```
$ dbed_update -S $ORACLE_SID -H $ORACLE_HOME
```

This completes the addition of the node to the SFDB repository.

For information on using SFDB tools features:

See the Storage Foundation guide:*Storage Foundation: Storage and Availability Management for Oracle Databases*.

Chapter 27

Removing a node from SF Oracle RAC clusters

This chapter includes the following topics:

- About removing a node from a cluster
- Removing a node from a cluster
- Modifying the VCS configuration files on existing nodes
- Removing the node configuration from the CP server
- Removing security credentials from the leaving node
- Updating the Storage Foundation for Databases (SFDB) repository after removing a node
- Sample configuration file for removing a node from the cluster

About removing a node from a cluster

You can remove one or more nodes from an SF Oracle RAC cluster if the node no longer needs to be part of the cluster.

Removing a node from a cluster requires:

- Taking Oracle service groups offline.
- Stopping applications that use File System or Cluster File System mount points not configured under VCS.
- Removing database instances and software from the node.
- Stopping VCS on the node to be removed.
- Remove Oracle Clusterware from the node.

- Unmounting the File System and Cluster File System file systems not configured under VCS.
- Uninstalling SF Oracle RAC from the node.
  Modifying the VCS configuration files on the existing nodes.
- Removing the node configuration from the CP server if it is configured.
- Removing the security credentials from the node if it is part of a secure cluster.
- Updating the SFDB repository if you use SFDB tools.

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 remove a node from a cluster

1. Take the Oracle service groups offline (if under VCS control) on the node you want to remove.

   ```
   # hagrp -offline oracle_group -sys saturn
   ```

2. Stop the applications that use VxFS/CFS mount points and are not configured under VCS. Use native application commands to stop the applications.
3. Remove the Oracle RAC database instance from the node.

   For instructions, see the Oracle RAC documentation.
4. Remove the Oracle RAC database software from the node.

   For instructions, see the Oracle RAC documentation.
5. Stop VCS on the node:

   ```
   # hastop -local
   ```

6. Remove Oracle Clusterware from the node.

   For instructions, see the Oracle RAC document.
7. Unmount the VxFS/CFS file systems that are not configured under VCS.

   ```
   # umount mount_point
   ```

8 Uninstall SF Oracle RAC from the node using the SF Oracle RAC installer.

```
# cd /opt/VRTS/install

# ./uninstallsfrac saturn
```

The installer stops all SF Oracle RAC processes and uninstalls the SF Oracle RAC packages.

9 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 475.

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.

The process involves:

- Editing the /etc/llthosts file
- Editing the /etc/gabtab file
- Modifying the VCS configuration to remove the node

For an example main.cf:

Editing 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 saturn is the node removed from the cluster, remove the line "2 saturn" from the file:

```
0 galaxy
1 nebula
2 saturn
```

Change to:

```
0 galaxy
1 nebula
```

Editing 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
```

Modifying the VCS configuration to remove the node

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 VCS configuration using the CLI

1. Back up the `/etc/VRTSvcs/conf/config/main.cf` file.

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

   # cp main.cf main.cf.3node.bak
   ```

2. Change the cluster configuration to read-write mode:

   ```
   # haconf -makerw
   ```

3. Remove the node from the AutoStartList attribute of the service group by specifying the remaining nodes in the desired order:

   ```
   # hagrp -modify cvm AutoStartList galaxy nebula
   ```

4 Remove the node from the SystemList attribute of the service group:

```
# hagrp -modify cvm SystemList -delete saturn
```

5 Remove the node from the CVMNodeId attribute of the service group:

```
# hares -modify cvm_clus CVMNodeId -delete saturn
```

6 If you have the other service groups (such as the database service group or the ClusterService group) that have the removed node in their configuration, perform step 4 and step 5 for each of them.

7 Remove the deleted node from the NodeList attribute of all CFS mount resources:

```
# hares -modify CFSMount NodeList -delete saturn
```

8 Remove the deleted node from the system list of any other service groups that exist on the cluster. For example, to delete the node saturn:

```
# hagrp -modify crsgrp SystemList -delete saturn
```

9 Remove the deleted node from the cluster system list:

```
# hasys -delete saturn
```

10 Save the new configuration to disk:

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

11 Verify that the node is removed from the VCS configuration.

```
# grep -i saturn main.cf
```

If the node is not removed, use the VCS commands as described in this procedure to remove the node.

Removing the node configuration from the CP server

After removing a node from a SF Oracle RAC cluster, perform the steps in the following procedure to remove that node's configuration from the CP server.

Note: The `cpsadm` command is used to perform the steps in this procedure. For detailed information about the `cpsadm` command, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

To remove the node configuration from the CP server

1. Log into the CP server as the root user.
2. View the list of VCS users on the CP server, using the following command:

   ```
   # cpsadm -s cp_server -a list_users
   ```

   Where *cp_server* is the virtual IP/ virtual hostname of the CP server.
3. Remove the VCS user associated with the node you previously removed from the cluster.

   For CP server in secure mode:

   ```
   # cpsadm -s cp_server -a rm_user \
   -e _HA_VCS_saturn@HA_SERVICES@saturn.nodes.example.com \
   -f cps_operator  -g vx
   ```

   For CP server in non-secure mode:

   ```
   # cpsadm -s cp_server  -a rm_user \
   -e cpsclient@saturn  -f cps_operator  -g vx
   ```

4. Remove the node entry from the CP server:

   ```
   # cpsadm -s cp_server -a rm_node  -h saturn -c rac_cluster101 -n 2
   ```

5. View the list of nodes on the CP server to ensure that the node entry was removed:

   ```
   # cpsadm -s cp_server -a list_nodes
   ```

Removing security credentials from the leaving node

If the leaving node is part of a cluster that is running in a secure mode, you must remove the security credentials from node saturn. Perform the following steps.

To remove the security credentials

1 Kill the `/opt/VRTSat/bin/vxatd` process.

2 Remove the root credentials on node saturn.

```
# vssat deletecred --domain type:domainname --prplname prplname
```

Updating the Storage Foundation for Databases (SFDB) repository after removing a node

If you are using Database Checkpoints, Database Flashsnap, or SmartTier for Oracle in your configuration, update the SFDB repository to remove the reference for the node after removing the node from the cluster.

Note: If you have not created an SFDB repository, you do not need to perform the following steps.

To update the SFDB repository after removing a node

1 As Oracle user, list the nodes in the cluster:

```
$ /opt/VRTSdbed/bin/dbed_rept_node -S $ORACLE_SID -o list
```

2 Run the following command after physically removing the node from the cluster.

For example:

```
$ /opt/VRTSdbed/bin/dbed_rept_node -S $ORACLE_SID -n NODE -o remove
```

This completes the removal of the node from the SFDB repository.

Sample configuration file for removing a node from the cluster

You may use this sample file as reference information to understand the configuration changes involved when you remove a node from a cluster.

The existing sample configuration before removing the node `saturn` is as follows:

- The existing cluster `rac_cluster101` comprises three nodes `galaxy`, `nebula`, and `saturn` and hosts a single database.
- The Oracle database is stored on CFS.

- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- Only one private IP address is configured for Oracle Clusterware. The private IP address is managed by the PrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.

Note: The following sample file shows in **bold** the configuration information that is removed when the node "saturn" is removed from the cluster.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"


cluster rac_cluster101 (
        UserNames = { admin = bopHo }
        Administrators = { admin }
        UseFence = SCSI3
        )


system galaxy (
        )
system nebula (
        )
system saturn (
       )
```

Note: In the following group oradb1_grp, the saturn node must be removed.

```
group oradb1_grp (
        SystemList = { galaxy = 0, nebula = 1, saturn = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula, saturn }
        )
```

Note: In the following Oracle resource, the saturn node information must be removed.

```
Oracle ora1 (
          Critical = 0
          Sid @galaxy = vrts1
          Sid @nebula = vrts2
          Sid @saturn = vrts3
          Owner = oracle
          Home = "/app/oracle/orahome"
          StartUpOpt = "SRVCTLSTART"
          ShutDownOpt = "SRVCTLSTOP"
          )

CFSMount oradata_mnt (
         Critical = 0
         MountPoint = "/oradata"
         BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
         )

CVMVolDg oradata_voldg (
         Critical = 0
         CVMDiskGroup = oradatadg
         CVMVolume = { oradatavol }
         CVMActivation = sw
         )

requires group cvm online local firm
ora1 requires oradata_mnt
oradata_mnt requires oradata_voldg
```

Note: In the following CVM and CVMCluster resources, the saturn node information must be removed.

```
group cvm (
        SystemList = { galaxy = 0, nebula = 1, saturn =2}
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula, saturn }
        )
```

```
  Application cssd (
          Critical = 0
          StartProgram = "/opt/VRTSvcs/rac/bin/cssd-online"
          StopProgram = "/opt/VRTSvcs/rac/bin/cssd-offline"
          CleanProgram = "/opt/VRTSvcs/rac/bin/cssd-clean"
          MonitorProgram = "/opt/VRTSvcs/rac/bin/cssd-monitor"
          OnlineRetryLimit = 20
          )

 CFSMount ocrvote_mnt (
          Critical = 0
          MountPoint = "/ocrvote"
          BlockDevice = "/dev/vx/dsk/ocrvotedg/ocrvotevol"
          MountOpt= "mincache=direct"
          )

CVMVolDg ocrvote_voldg (
         Critical = 0
         CVMDiskGroup = ocrvotedg
         CVMVolume = { ocrvotevol }
         CVMActivation = sw
         )


CFSfsckd vxfsckd (
         )



CVMCluster cvm_clus (
        CVMClustName = rac_cluster101
        CVMNodeId = { galaxy = 0, nebula = 1, saturn =2 }
        CVMTransport = gab
        CVMTimeout = 200
        )


CVMVxconfigd cvm_vxconfigd (
         Critical = 0
         CVMVxconfigdArgs = { syslog }
         )
```

Note: In the following PrivNIC resource, the saturn node information must be removed.

```
PrivNIC ora_priv (
              Critical = 0
              Device@galaxy = { lan1 = 0, lan2 = 1}
              Device@nebula = { lan1 = 0, lan2 = 1}
              Device@saturn = { lan1 = 0, lan2 = 1}
              Address@galaxy = "192.168.12.1"
              Address@nebula = "192.168.12.2"
              Address@saturn = "192.168.12.5"
              NetMask = "255.255.255.0"
              )


cssd requires ocrvote_mnt
cssd requires ora_priv
ocrvote_mnt requires ocrvote_voldg
ocrvote_mnt requires vxfsckd
ocrvote_voldg requires cvm_clus
vxfsckd requires cvm_clus
cvm_clus requires cvm_vxconfigd
```

Section 7

Configuration of disaster recovery environments

- Chapter 28. Configuring a campus cluster setup for disaster recovery
- Chapter 29. Setting up a replicated global cluster
- Chapter 30. Configuring a global cluster using VVR

Chapter 28

Configuring a campus cluster setup for disaster recovery

This chapter includes the following topics:

- Requirements for an SF Oracle RAC campus cluster
- Setting up an SF Oracle RAC campus cluster for disaster recovery
- Tuning guidelines for campus clusters
- Best practices for a campus cluster

Requirements for an SF Oracle RAC campus cluster

You will need the following to setup an SF Oracle RAC campus cluster:

- Hardware requirements for SF Oracle RAC:
  See "Hardware requirements" on page 46.
- License requirements: in addition to SF Oracle RAC with HA/DR, you will need:
  - FlashSnap license
  - Site awareness license

With keyless licensing, SF Oracle RAC enterprise keys enable all of the above features.

Setting up an SF Oracle RAC campus cluster for disaster recovery

Perform the following high-level tasks to setup an SF Oracle RAC campus cluster:

- Preparing to set up campus cluster configuration
- Configuring I/O fencing to prevent data corruption
- Preparing to install Oracle RAC Clusterware and database binaries
- Configuring VxVM disk groups for campus cluster
- Installing Oracle RAC Clusterware and database binaries
- Configuring VCS service groups

The sample configuration used to illustrate the configuration procedures includes a four-node SF Oracle RAC campus cluster with two nodes at each site. Each node has SF Oracle RAC 5.1 Service Pack 1 on HP-UX 11i v3.

Table 28-1 Sample setup for campus cluster

Site	Hardware description
Site 1: SFRAC1	Servers: galaxy and nebula Shared LUNs: disk01 disk02 disk03 disk04 (used as coordinator disk) disk5
Site 2: SFRAC2	Servers: mercury and jupiter Shared LUNs: disk06 disk07 disk08 disk09 (used as coordinator disk)
Site 3	Shared LUN disk10 (used as coordinator disk)

Preparing to set up a campus cluster

The following preparation must be completed before configuring the campus cluster.

To prepare to set up a campus cluster

1. Configure the physical infrastructure for campus cluster:
   - Set up access to the local storage arrays and to remote storage arrays on each node. The storage link will extend to the third site as well.
   - Set up the private heartbeat network
     See the *Veritas Cluster Server Administrator's Guide*
2. Install the operating system on all the nodes of the cluster.

   See your operating system documenation.
3. Install and configure SF Oracle RAC on all nodes on both the sites.

   See "About configuring SF Oracle RAC" on page 123.

   In the sample setup, install and configure SF Oracle RAC 5.1 Service Pack 1 on all four nodes.

Configuring VxVM disk groups for Oracle RAC on a campus cluster

After configuring I/O fencing for data integrity, you must configure the VxVM disk groups for a campus cluster before installing Oracle RAC by configuring VxVM disk groups for remote mirroring.

To configure VxVM disk groups for Oracle RAC on a campus cluster

1. Initialize the disks as CDS disks

```
# vxdisksetup -i disk01 format=cdsdisk
# vxdisksetup -i disk02 format=cdsdisk
# vxdisksetup -i disk03 format=cdsdisk
# vxdisksetup -i disk05 format=cdsdisk
# vxdisksetup -i disk06 format=cdsdisk
# vxdisksetup -i disk07 format=cdsdisk
# vxdisksetup -i disk08 format=cdsdisk
```

2. Set the site name for each host:

```
# vxdctl set site=sitename
```

   The site name is stored in the /etc/vx/volboot file. To display the site names:

```
# vxdctl list | grep siteid
```

For example, for a four node cluster with two nodes at each site, mark the sites as follows:

On the nodes at first site:

```
# vxdctl set site= SFRAC1
```

On the nodes at second site:

```
# vxdctl set site= SFRAC2
```

3 Set the site name for all the disks in an enclosure.

```
# vxdisk settag site=sitename encl:enclosure
```

4 Run the following command if you want to tag only the specific disks:

```
# vxdisk settag site=sitename disk
```

For example:

```
# vxdisk settag site=SFRAC1 disk01
# vxdisk settag site=SFRAC1 disk02
# vxdisk settag site=SFRAC1 disk03
# vxdisk settag site=SFRAC2 disk06
# vxdisk settag site=SFRAC2 disk08
```

5 Verify that the disks are registered to a site.

```
# vxdisk listtag
```

For example:

```
# vxdisk listtag
DEVICE          NAME                          VALUE
disk01           site                          SFRAC1
disk02           site                          SFRAC1
disk03           site                          SFRAC1
disk06           site                          SFRAC2
disk08           site                          SFRAC2
```

6 Create a disk group for OCR and Vote Disks and another for Oracle data, with disks picked from both the sites. While the example below shows a single disk group, you can create as many as you need.

```
# vxdg -s init ocrvotedg disk05 disk07
# vxdg -s init oradatadg disk01 disk06
```

For the disks used in ocrvotedg, do not set site consistency to **on**.

7 Enable site-based allocation on the disk groups for each site.

```
# vxdg -g oradata addsite SFRAC1

# vxdg -g oradata addsite SFRAC2
```

8 Set site consistency on the disk groups.

```
# vxdg -g oradatadg set siteconsistent=on

# vxedit -g oradatadg set dgdetpolicy=global
# vxedit -g oradatadg set dgfailpolicy=leave
# vxedit -g ocrvotedg set dgdetpolicy=global
# vxedit -g ocrvotedg set dgfailpolicy=leave
```

9 If you are using an enclosure, set the tag on the enclosure for both sites.

```
# vxdg -o retain -g oradatadg setting encl:3pardata0 site=SFRAC1

# vxdg -o retain -g oradatadg setting encl:3pardata1 site=SFRAC2
```

10 Create one or more mirrored volumes in the disk group.

```
# vxassist -g ocrvotedg make ocrvotevol 2048m nmirror=2

# vxassist -g oradatadg make oradatavol 10200m nmirror=2
```

With the Site Awareness license installed on all hosts, the volume created has the following characteristics by default.

- The all sites attribute is set to ON; the volumes have at least one mirror at each site.
- The volumes are automatically mirrored across sites.
- The read policy (rdpol) is set to siteread.
- The volumes inherit the site consistency value that is set on the disk group.

11 From the CVM master, start the volumes for all the disk groups.

```
# vxvol -g ocrvotedg startall
# vxvol -g oradatadg startall
```

12 Create a file system on each volume and mount the same.

```
# mkfs -F vxfs /dev/vx/rdsk/ocrvotedg/ocrvotevol
```

```
# mkfs -F vxfs /dev/vx/rdsk/oradatadg/oradatavol

# mount -F vxfs -o cluster /dev/vx/dsk/ocrvotedg/ocrvotevol /ocr

# mount - vxfs -o cluster /dev/vx/dsk/oradatadg/oradatavol /oradata
```

13 Touch two files, one for OCR and another for Vote Disk.

```
# touch /ocr/ocr /ocr/vote
```

Note: One Vote Disk is sufficient since it is already mirrored by VxVM.

Tuning guidelines for campus clusters

An important consideration while tuning an SF Oracle RAC campus cluster is setting the LLT peerinact time. Follow the guidelines below to determine the optimum value of peerinact time:

- Calculate the roundtrip time using lltping (1M).
- Evaluate LLT heartbeat time as half of the round trip time.
- Set the LLT peer trouble time as 2-4 times the heartbeat time.
- LLT peerinact time should be set to be more than 4 times the heart beat time.

Best practices for a campus cluster

The following best practices ensure a robust SF Oracle RAC campus cluster:

- Tag all the mirrored volumes in the campus cluster with appropriate site names. VxVM allocates storage from the correct site when creating or resizing a volume and when changing a volume's layout if the volume is tagged with site name.
- All volumes that have data required by the application must be evenly mirrored. Each site must have at least one mirror of all volumes hosting application data, including the FlashSnap log volume.
- Do not enable site consistency on VxVM snapshot volumes.
- Use redundant links for storage and private interconnects. DWDM can be used for storage and heartbeat together. Another redundant DWDM link can be used to prevent single point of failure. Separate switches and multiplexer / de-multiplexer devices should be used.

- Use Coordination Point Server as the third coordination point.
- Use the procedure for online replacement of coordination points, to replace disk based or Coordination Point Server based coordination points.

Chapter 29

Setting up a replicated global cluster

This chapter includes the following topics:

- Replication in the SF Oracle RAC environment
- Requirements for SF Oracle RAC global clusters
- About setting up a global cluster in an SF Oracle RAC environment
- Configuring a cluster at the primary site
- Configuring a cluster at the secondary site
- Configuring replication on clusters at both sites
- Modifying the ClusterService group for global clusters
- Defining the remote cluster and heartbeat objects
- Configuring the VCS service groups for global clusters

Replication in the SF Oracle RAC environment

You can set up a primary SF Oracle RAC cluster for replication to a secondary SF Oracle RAC cluster by configuring global VCS service groups and using a replication technology. The Oracle RAC cluster at the secondary site can be a single node cluster. For example, you can have a two-node cluster on the primary site and a two-node or single-node cluster on the secondary site.

You can use one of the following replication technologies:

- Veritas Volume Replicator (VVR), which provides host-based volume replication. Using VVR you can replicate data volumes on a shared disk group in SF Oracle RAC.
- Supported hardware-based replication technologies. Using hardware-based replication you can replicate data from a primary array to a secondary array.
- Using SF Oracle RAC with VVR you can run a fire drill to verify the disaster recovery capability of your configuration.
  See the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

Requirements for SF Oracle RAC global clusters

Review the requirements information to make sure your configuration is supported for SF Oracle RAC.

For product licensing information:

See "About Veritas product licensing" on page 73.

Supported software and hardware for SF Oracle RAC

For supported hardware and software:

- See "Important preinstallation information" on page 45.
- See the current compatibility list in the Veritas Technical Support website to confirm the compatibility of your hardware:
  http://entsupport.symantec.com/docs/283161

Supported replication technologies for SF Oracle RAC

SF Oracle RAC supports the following replication technologies through the use of Veritas replication agents:

Table 29-1 Supported replication options for SF Oracle RAC global clusters

Replication technology	Supported modes	Supported software
Veritas Volume Replicator (VVR) Supporting agents ■ RVGShared ■ RVGSharedPri ■ RVGLogOwner	■ Asynchronous replication ■ Synchronous replication	Host-based replication

Table 29-1 Supported replication options for SF Oracle RAC global clusters *(continued)*

Replication technology	Supported modes	Supported software
EMC SRDF Supporting agent: SRDF	■ Asynchronous replication ■ Synchronous replication	All versions of Solutions Enabler
Hitachi True Copy Supporting agent: HTC	■ Asynchronous replication ■ Synchronous replication	All versions of the Hitachi CCI
IBM Metro Mirror Supporting agent: MetroMirror	Synchronous replication	All versions of IBM DSCLI. The MetroMirror agent is supported for DS6000 and DS8000 arrays
IBM SVC SVC CopyServices	■ Asynchronous replication ■ Synchronous replication	SSH access to the SVC
EMC Mirror View Supporting agent:MirrorView	■ Asynchronous replication ■ Synchronous replication: only individual LUNs may be replicated	All versions of NaviCLI

Note: Check your vendor's compatibility list for the supported software versions. The support listed above only exists if the host, HBA, and array combination is in your vendor's hardware compatibility list. Check your array documentation.

Note: All arrays must support SCSI-3 persistent reservations for SF Oracle RAC.

You can use the Veritas replication agents listed in the table above for global clusters that run SF Oracle RAC. The Veritas replication agents provide application failover and recovery support to your replication configuration. The agents provide this support for environments where data is replicated between clusters.

VCS agents control the direction of replication. They do not monitor the progress or status of replication. The replication agents manage the state of replicated

devices that are attached to SF Oracle RAC nodes. The agents make sure that the system which has the resource online also has safe and exclusive access to the configured devices.

This information is current at the time this document is released. For more current information on the replicated agents, see:

- *Veritas Cluster Server Agent for EMC SRDF Installation and Configuration Guide*
- *Veritas Cluster Server Agent for Hitachi TrueCopy Installation and Configuration Guide*
- *Veritas Cluster Server Agent for IBM Metro Mirror Installation and Configuration Guide*
- *Veritas Cluster Server Agent for IBM SVC Installation and Configuration Guide*
- *Veritas Cluster Server Agent for EMC MirrorView Installation and Configuration Guide*
- *Veritas Cluster Server Agent for Oracle Data Guard Installation and Configuration Guide*
- Technical Support TechNote for the latest updates or software issues for replication agents:
  http://entsupport.symantec.com/docs/282004htm

About setting up a global cluster in an SF Oracle RAC environment

Configuring a global cluster for Oracle RAC requires the coordination of many component setup tasks. The procedures provided in this document are guidelines.

The tasks required to set up a global cluster:

- Configure an SF Oracle RAC cluster at the primary site
- Configure an SF Oracle RAC cluster at the secondary site
- Configure replication on clusters at both sites
- Configure VCS service groups for replication
- Test the HA/DR configuration
- Upon successful testing, bring the environment into production

Some SF Oracle RAC HA/DR configuration tasks may require adjustments depending upon your particular starting point, environment, and configuration. Review the installation requirements and sample cluster configuration files for primary and secondary clusters.

For requirements:

For instructions for configuring AT in a global cluster:

See the *Veritas Cluster Server Administrator's Guide*

Configuring a cluster at the primary site

You can use an existing SF Oracle RAC cluster or you can install a new SF Oracle RAC cluster for your primary site.

For planning information:

See "Typical configuration of SF Oracle RAC global clusters for disaster recovery" on page 43.

If you are using an existing cluster as the primary and you want to set up a global cluster, skip the steps below and proceed to configure your secondary cluster.

See "Configuring a cluster at the secondary site" on page 501.

Note: You must have a GCO license enabled for a global cluster. If you are using VVR for replication, you must have a VVR license enabled.

If you do not have an existing cluster and you are setting up two new sites for an SF Oracle RAC global cluster, follow the steps below.

To set up the cluster and database at the primary site

1. Install and configure servers and storage.
2. If you are using hardware-based replication, install the sofware for managing your array.
3. Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster. If you are using VVR for replication, you must have it enabled.
4. Install and configure SF Oracle RAC. Prepare for your installation according to your configuration needs.

   For preparation:

   For installation:

   See "About installing SF Oracle RAC " on page 87.
5. For a multi-node cluster, configure I/O fencing.

- Verify the shared storage on the secondary site supports SCSI-3 reservations.
- Set up coordinator disks
- Configure I/O fencing

For instructions for setting up fencing:

See "About planning to configure I/O fencing" on page 62.

6 Verify the CVM group is online on all nodes in the primary cluster:

```
# hagrp -state cvm
```

7 Prepare systems and storage for a global cluster. Identify the hardware and storage requirements before installing Oracle RAC Clusterware and RDBMS software.

You will need to set up:

- Local storage for Oracle RAC and CRS binaries
- Shared storage for OCR and Vote disk which is not replicated
- Replicated storage for database files

8 Install and configure the Oracle RAC binaries:

See "About preparing to install Oracle RAC" on page 275.

See "About installing Oracle RAC" on page 329.

Note: OCR and Vote disk must be on non-replicated shared storage.

After successful Oracle RAC installation and configuration, verify that CRS daemons and resources are up on all nodes.

```
$ crs_stat -t
```

9 Identify the disks that will be replicated, create the required CVM disk group, volume, and file system.

10 Create the database on the file system you created in the previous step.

11 Configure the VCS service groups for the database.

12 Verify that all VCS service groups are online.

Configuring a cluster at the secondary site

To set up a multi-node or single-node cluster on the secondary site:

- Set up the cluster
- Set up the database

The setup requirements for the secondary site parallel the requirements for the primary site with a few additions or exceptions as noted below.

Important requirements for global clustering:

- Cluster names on the primary and secondary sites must be unique.
- Make sure that you use the same OS user and group IDs for Oracle for installation and configuration on both the primary and secondary clusters.

Setting up the cluster on the secondary site

To set up the cluster on secondary site

1. Install and configure servers and storage.
2. If you are using hardware-based replication, install the sofware for managing your array.
3. Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster. If you are using VVR for replication, you must have it enabled.
4. Install and configure SF Oracle RAC. Prepare for your installation according to your configuration needs.

   For preparation:

   For installation:

   See "About installing SF Oracle RAC " on page 87.
5. For a multi-node cluster, configure I/O fencing.
   - Verify the shared storage on the secondary site supports SCSI-3 reservations.
   - Set up coordinator disks
   - Configure I/O fencing

   For instructions for setting up fencing:

   See "About planning to configure I/O fencing" on page 62.

6 For a single-node cluster, do not enable I/O fencing. Fencing will run in disabled mode.

7 Prepare systems and storage for a global cluster. Identify the hardware and storage requirements before installing Oracle RAC Clusterware and RDBMS software.

You will need to set up:

- Local storage for Oracle RAC and CRS binaries
- Shared storage for OCR and Vote disk which is not replicated
- Replicated storage for database files

8 Install and configure the Oracle RAC binaries:

See "About preparing to install Oracle RAC" on page 275.

See "About installing Oracle RAC" on page 329.

Note: OCR and Vote disk must be on non-replicated shared storage.

After successful Oracle RAC installation and configuration, verify that CRS daemons and resources are up on all nodes.

```
$ crs_stat -t
```

Setting up the database for the secondary site

To set up the database for the secondary site

1 Do not create the database. The database will be replicated from the primary site.

- If you are using hardware-based replication, the database, disk group, and volumes will be replicated from the primary site.
  Create the directory for the CFS mount point which will host the database data and control files.
- If you are using VVR for replication, create an identical disk group and volumes for the replicated content with the same names and size as listed on the primary site.

Create the directories for the CFS mount points as they are on the primary site. These will be used to host the database and control files when the failover occurs and the secondary is promoted to become the primary site.

2 Copy the init$ORACLE_SID.ora file from $ORACLE_HOME/dbs at the primary to $ORACLE_HOME/dbs at the secondary.

3 Create the following subdirectories on the secondary site as you did on the primary site:

For Oracle RAC 10g:

```
$ mkdir -p /$ORACLE_BASE/admin/adump
$ mkdir -p /$ORACLE_BASE/admin/database_name/bdump
$ mkdir -p /$ORACLE_BASE/admin/database_name/cdump
$ mkdir -p /$ORACLE_BASE/admin/database_name/dpdump
$ mkdir -p /$ORACLE_BASE/admin/database_name/hdump
$ mkdir -p /$ORACLE_BASE/admin/database_name/udump
$ mkdir -p /$ORACLE_BASE/admin/database_name/pfile
```

For Oracle 11gR1:

```
$ mkdir -p $ORACLE_BASE/admin
$ mkdir -p $ORACLE_BASE/admin $database_name
$ cd $ORACLE_BASE/admin/$database_name
$ mkdir adump dpdump hdump pfile
```

For oracle 11gR2 release only, on both the primary and secondary sites, edit the file:

```
$ORACLE_HOME/dbs/init$ORACLE_SID.ora
```

as

```
remote_listener = 'SCAN_NAME:1521'
SPFILE=<SPFILE NAME>
```

4 Configure listeners on the secondary site with same name as on primary. You can do this by one of the following methods:

- Copy the listener.ora and tnsnames.ora files from the primary site and update the names as appropriate for the secondary site.
- Use Oracle's netca utility to to configure the listener.ora and tnsnames.ora files on the secondary site.

5 On the secondary site, register the database using the `srvctl` command as Oracle user.

```
$ srvctl add database -d database_name -o oracle_home -p sp_file
```

To prevent automatic database instance restart, change the Management policy for the database (automatic, manual) to MANUAL using the `srvctl` command:

```
$ srvctl modify database -d database_name -y manual
```

6 Register the instances using srvctl command. Execute the following command on each node:

```
$ srvctl add instance -d database_name \
-i instance_name -n node-name
```

Configuring replication on clusters at both sites

You must configure replication for the database files. Once replication is configured, make sure it is functioning correctly by testing before proceeding.

To configure replication at both sites

1 If you are using hardware-based replication, make sure that the replication management software for managing replication is installed on all nodes in both clusters.

2 At both sites, identify the disks on which the database resides at the primary site and associate them with the corresponding disks at the secondary site.

For VVR:

See "Setting up replication using VVR on the primary site" on page 512.

For Hardware-based replication:

See your hardware documentation for details on setting up replication between the two sites.

3 Start replication between the sites.

For VVR:

See "Starting replication of Oracle RAC database volume" on page 519.

See your hardware documentation for the appropriate procedures.

Modifying the ClusterService group for global clusters

You have configured VCS service groups for SF Oracle RAC on each cluster. Each cluster requires an additional virtual IP address associated with the cluster for cross-cluster communication. The VCS installation and creation of the ClusterService group typically involves defining this IP address.

Configure a global cluster by setting:

- Heartbeat
- Wide area cluster (wac)
- GCO IP (gcoip)
- remote cluster resources

See the *Veritas Cluster Server User's Guide* for complete details on global clustering.

Modifying the global clustering configuration using the wizard

The global clustering wizard completes the following tasks:

- Validates the ability of the current configuration to support a global cluster environment.
- Creates the components that enable the separate clusters, each of which contains a different set of GAB memberships, to connect and operate as a single unit.
- Creates the ClusterService group, or updates an existing ClusterService group.

Run the global clustering configuration wizard on each of the clusters; you must have the global clustering license in place on each node in the cluster.

To modify the ClusterService group for global clusters using the global clustering wizard

1. On the primary cluster, start the GCO Configuration wizard:

   ```
   # /opt/VRTSvcs/bin/gcoconfig
   ```

2. The wizard discovers the NIC devices on the local system and prompts you to enter the device to be used for the global cluster. Specify the name of the device and press Enter.
3. If you do not have NIC resources in your configuration, the wizard asks you whether the specified NIC will be the public NIC used by all the systems. Enter y if it is the public NIC; otherwise enter n. If you entered n, the wizard prompts you to enter the names of NICs on all systems.

4 Enter the virtual IP address for the local cluster.

5 If you do not have IP resources in your configuration, the wizard prompts you for the netmask associated with the virtual IP. The wizard detects the netmask; you can accept the suggested value or enter another one.

The wizard starts running commands to create or update the ClusterService group. Various messages indicate the status of these commands. After running these commands, the wizard brings the ClusterService group online.

Defining the remote cluster and heartbeat objects

After configuring global clustering, add the remote cluster object to define the IP address of the cluster on the secondary site, and the heartbeat object to define the cluster-to-cluster heartbeat.

Heartbeats monitor the health of remote clusters. VCS can communicate with the remote cluster only after you set up the heartbeat resource on both clusters.

To define the remote cluster and heartbeat

1 On the primary site, enable write access to the configuration:

```
# haconf -makerw
```

2 Define the remote cluster and its virtual IP address.

In this example, the remote cluster is rac_cluster102 and its IP address is 10.11.10.102:

```
# haclus -add rac_cluster102 10.11.10.102
```

3 Complete step 1 and step 2 on the secondary site using the name and IP address of the primary cluster.

In this example, the primary cluster is rac_cluster101 and its IP address is 10.10.10.101:

```
# haclus -add rac_cluster101 10.10.10.101
```

4 On the primary site, add the heartbeat object for the cluster. In this example, the heartbeat method is ICMP ping.

```
# hahb -add Icmp
```

5 Define the following attributes for the heartbeat resource:

- ClusterList lists the remote cluster.
- Arguments enables you to define the virtual IP address for the remote cluster.

For example:

```
# hahb -modify Icmp ClusterList rac_cluster102
# hahb -modify Icmp Arguments 10.11.10.102 -clus rac_cluster102
```

6 Save the configuration and change the access to read-only on the local cluster:

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

7 Complete step 4-6 on the secondary site using appropriate values to define the cluster on the primary site and its IP as the remote cluster for the secondary cluster.

8 Verify cluster status with the `hastatus -sum` command on both clusters.

```
# hastatus -sum
```

9 Display the global setup by executing haclus -list command.

```
# haclus -list
     rac_cluster101
     rac_cluster102
```

Example of heartbeat additions to the main.cf file on the primary site:

```
.
.
remotecluster rac_cluster102 (
Cluster Address = "10.11.10.102"
)
heartbeat Icmp (
    ClusterList = { rac_cluster102 }
    Arguments @rac_cluster102 = { "10.11.10.102" }
    )

system galaxy (
    )
.
.
```

Example heartbeat additions to the main.cf file on the secondary site:

```
.
.
remotecluster rac_cluster101 (
    Cluster Address = "10.10.10.101"
    )

heartbeat Icmp (
    ClusterList = { rac_cluster101 }
    Arguments @rac_cluster101 = { "10.10.10.101" }
    )

system mercury (
    )
.
.
```

See the *Veritas Cluster Server User's Guide* for details for configuring the required and optional attributes of the heartbeat object.

Configuring the VCS service groups for global clusters

To configure VCS service groups for global clusters

1. Configure and enable global groups for databases and resources.
   - Configure VCS service groups at both sites.
   - Configure the replication agent at both sites.
   - Make the RAC service group a global service group, enabling failover across clusters.
   - For example:
2. To test real data in an environment where HA/DR has been configured, schedule a planned migration to the secondary site for testing purposes.

   For example:

   See "Migrating the role of primary site to the secondary site" on page 535.

   See "Migrating the role of new primary site back to the original primary site" on page 536.
3. Upon successful testing, bring the environment into production.

For more information see:

- *Veritas Cluster Server Installation Guide*
- *Veritas Cluster Server Agent for EMC SRDF Installation and Configuration Guide*
- *Veritas Cluster Server Agent for Hitachi TrueCopy Installation and Configuration Guide*
- *Veritas Cluster Server Agent for IBM Metro Mirror Installation and Configuration Guide*
- *Veritas Cluster Server Agent for EMC MirrorView Installation and Configuration Guide*
- *Veritas Cluster Server Agent for IBM SVC Installation and Configuration Guide*
- *Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide*
- Technical Support TechNote for the latest updates or software issues for replication agents:
  http://entsupport.symantec.com/docs/282004htm

For complete details on VVR in a shared disk environment:

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

Chapter 30

Configuring a global cluster using VVR

This chapter includes the following topics:

- About configuring global clustering using VVR
- Setting up replication using VVR on the primary site
- Setting up replication using VVR on the secondary site
- Starting replication of Oracle RAC database volume
- Configuring VCS to replicate the database volume using VVR
- Using VCS commands on SF Oracle RAC global clusters
- Using VVR commands on SF Oracle RAC global clusters

About configuring global clustering using VVR

Before configuring clusters for global clustering, make sure both clusters have product and database software installed and configured.

Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster and VVR enabled.

See "About Veritas product licensing" on page 73.

After setting up two clusters running SF Oracle RAC, you can configure a global cluster environment with VVR. You must modify both cluster configurations to support replication in the global cluster environment.

Configuring SF Oracle RAC for global clusters requires:

- Setting up both clusters as part of a global cluster environment.
  See "About setting up a global cluster in an SF Oracle RAC environment" on page 498.
- Setting up replication for clusters at both sites.
  See "Setting up replication using VVR on the primary site" on page 512.
  See "Setting up replication using VVR on the secondary site" on page 515.
- Starting replication of the database.
  See "Starting replication of Oracle RAC database volume" on page 519.
- Configuring VCS for replication on clusters at both sites.
  See "Configuring VCS to replicate the database volume using VVR" on page 521.

Setting up replication using VVR on the primary site

Setting up replication with VVR in a global cluster environment involves the following tasks:

- If you have not already done so, create a disk group on the storage on the primary site.
  For example:
- Creating the Storage Replicator Log (SRL) in the disk group for the database.
  See "Creating the SRL volume on the primary site" on page 512.
- Creating the Replicated Volume Group (RVG) on the primary site.
  See "Setting up the Replicated Volume Group (RVG) on the primary site" on page 513.

Creating the SRL volume on the primary site

Create the SRL. The SRL is a volume in the RVG. The RVG also holds the data volumes for replication.

- The data volume on the secondary site has the same name and the same size as the data volume on the primary site.
- The SRL on the secondary site has the same name and the same size as the SRL on the primary site.
- The data volume and SRL volume should exist in the same disk group.
- If possible, create SRLs on disks without other volumes.
- Mirror SRLs and data volumes in the absence of hardware-based mirroring.

To create the SRL volume on the primary site

1. On the primary site, determine the size of the SRL volume based on the configuration and amount of use.

   See the Veritas Volume Replicator documentation for details.

2. Using the following command, determine whether a node is the master or the slave:

   ```
   # vxdctl -c mode
   ```

3. From the master node, issue the following command:

   ```
   # vxassist -g oradatadg make rac1_srl 1500M nmirror=2 disk4 disk5
   ```

4. Using the following command, start the SRL volume by starting all volumes in the disk group:

   ```
   # vxvol -g oradatadg startall
   ```

Setting up the Replicated Volume Group (RVG) on the primary site

Before creating the RVG on the primary site, make sure the volumes and CVM group are active and online.

To review the status of replication objects on the primary site

1. Verify the volumes you intend to include in the group are active.
2. Review the output of the `hagrp -state cvm` command to verify that the CVM group is online.
3. On each site, verify vradmin is running:

```
#  ps -ef |grep vradmin
    root  536594  598036   0 12:31:25      0  0:00 grep vradmin
```

If vradmin is not running start it:

```
# vxstart_vvr
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
#  ps -ef |grep vradmin
    root  536782       1   0 12:32:47      -  0:00 /usr/sbin/vradmind
    root 1048622  598036   0 12:32:55      0  0:00 grep vradmin
# netstat -an |grep 4145
tcp4       0      0  *.4145                 *.*          LISTEN
udp4       0      0  *.4145                 *.*
```

To create the RVG

The command to create the primary RVG takes the form:

```
vradmin -g disk_group createpri rvg_name data_volume srl_volume
```

where:

- disk_group is the name of the disk group containing the database
- rvg_name is the name for the RVG
- data_volume is the volume that VVR replicates
- srl_volume is the volume for the SRL

For example, to create the rac1_rvg RVG, enter:

```
# vradmin -g oradatadg createpri rac1_rvg rac1_vol rac1_srl
```

The command creates the RVG on the primary site and adds a Data Change Map (DCM) for each data volume. In this case, a DCM exists for rac1_vol.

Setting up replication using VVR on the secondary site

To create objects for replication on the secondary site, use the `vradmin` command with the `addsec` option. To set up replication on the secondary site, perform the following tasks:

- If you have not already done so, create a disk group to hold data volume, SRL, and RVG on the storage on the secondary site.
  For example:
- Create volumes for the database and SRL on the secondary site.
  See "Creating the data and SRL volumes on the secondary site" on page 515.
- Edit the /etc/vx/vras/.rdg file on the secondary site.
  See "Editing the /etc/vx/vras/.rdg files" on page 516.
- Use resolvable virtual IP addresses that set network RLINK connections as host names of the primary and secondary sites.
  See "Setting up IP addresses for RLINKs on each cluster" on page 516.
- Create the replication objects on the secondary site.
  See "Setting up the disk group on secondary site for replication" on page 517.

Creating the data and SRL volumes on the secondary site

Note the following when creating volumes for the data and SRL:

- The sizes and names of the volumes must reflect the sizes and names of the corresponding volumes in the primary site.
- Create the data and SRL volumes on different disks in the disk group. Use the `vxdisk -g diskgroup list` command to list the disks in the disk group.
- Mirror the volumes.

To create the data and SRL volumes on the secondary site

1. In the disk group created for the Oracle RAC database, create a data volume of same size as that in primary for data; in this case, the rac_vol1 volume on the primary site is 6.6 GB:

```
# vxassist -g oradatadg make rac_vol1 6600M nmirror=2 disk1 disk2
```

2 Create the volume for the SRL, using the same name and size of the equivalent volume on the primary site. Create the volume on different disks from the disks for the database volume, but on the same disk group that has the data volume:

```
# vxassist -g oradatadg make rac1_srl 1500M nmirror=2 disk4 disk6
```

Editing the /etc/vx/vras/.rdg files

Editing the /etc/vx/vras/.rdg file on the secondary site enables VVR to replicate the disk group from the primary site to the secondary site. On each node, VVR uses the /etc/vx/vras/.rdg file to check the authorization to replicate the RVG on the primary site to the secondary site. The file on each node in the secondary site must contain the primary disk group ID, and likewise, the file on each primary system must contain the secondary disk group ID.

To edit the /etc/vx/vras/.rdg files

1 On a node in the primary site, display the primary disk group ID:

```
# vxprint -l diskgroup

.....
```

2 On each node in the secondary site, edit the /etc/vx/vras/.rdg file and enter the primary disk group ID on a single line.

3 On each cluster node of the primary cluster, edit the /etc/vx/vras/.rdg file and enter the secondary disk group ID on a single line.

Setting up IP addresses for RLINKs on each cluster

Creating objects with the vradmin command requires resolvable virtual IP addresses that set network RLINK connections as host names of the primary and secondary sites.

To set up IP addresses for RLINKS on each cluster

1 For each RVG running on each cluster, set up a virtual IP address on one of the nodes of the cluster. These IP addresses are part of the RLINK.

The example assumes for the cluster on the primary site:

- The public network interface is lan0:1
- The virtual IP address is 10.10.9.101

- The net mask is 255.255.255.0
- ```
  # ifconfig lan0:1 plumb
  # ifconfig lan0:1 inet 10.10.9.101 netmask 255.255.255.0
  # ifconfig lan0:1 up
  ```

2 Use the same commands with appropriate values for the interface, IP address, and net mask on the secondary site.

The example assumes for the secondary site:

- The public network interface is lan0:1
- virtual IP address is 10.11.9.102
- net mask is 255.255.255.0

3 Define the virtual IP addresses to correspond to a virtual cluster host name on the primary site and a virtual cluster host name on the secondary site.

Update the /etc/hosts file on all the nodes on both the primary and secondary sites.

The examples assume:

- rac_cluster101 has IP address 10.10.9.101
- rac_cluster102 has IP address 10.11.9.102

4 Use the ping command to verify the links are functional.

Setting up the disk group on secondary site for replication

Create the replication objects on the secondary site from the master node of the primary site, using the `vradmin` command.

To set up the disk group on the secondary site for replication

1 Issue the command in the following format from the cluster on the primary site:

```
# vradmin -g dg_pri addsec rvg_pri pri_host sec_host
```

where:

- dg_pri is the disk group on the primary site that VVR will replicate. For example: rac1_vol
- rvg_pri is the RVG on the primary site. For example: rac1_rvg
```

- pri_host is the virtual IP address or resolvable virtual host name of the cluster on the primary site.
  For example: rac_cluster101_1
  You could also use 10.10.9.101
- sec_host is the virtual IP address or resolvable virtual host name of the cluster on the secondary site.
  For example: rac_cluster102_1
  You could also use 10.11.9.102

For example, the command to add the cluster on the primary site to the Replicated Data Set (RDS) is:

```
# vradmin -g oradatadg addsec rac1_rvg \
      10.10.9.101
       10.11.9.102
```

On the secondary site, the above command performs the following tasks:

- Creates an RVG within the specified disk group using the same name as the one for the primary site
- Associates the data and SRL volumes that have the same names as the ones on the primary site with the specified RVG
- Adds a data change map (DCM) for the data volume
- If you use 10.10.9.101 and 10.11.9.102, creates cluster RLINKS for the primary and secondary sites with the default names; for example, the "primary" RLINK created for this example is *rlk_10.11.9.102_rac1_rvg* and the "secondary" RLINK created is *rlk_10.10.9.101_rac1__rvg*.

2 Verify the list of RVGs in the RDS by executing the following command.

```
# vradmin -g oradatadg -l printrvg
```

For example:

```
Replicated Data Set: rac1_rvg
Primary:
HostName: 10.180.88.187 <localhost>
RvgName: rac1_rvg
DgName: rac1_vol
datavol_cnt: 1
vset_cnt: 0
srl: rac1_srl
RLinks:
```

```
name=rlk_rac_cluster102_1_rac1_rvg, detached=on,
synchronous=off
Secondary:
HostName: 10.190.99.197
RvgName: rac1_rvg
DgName: oradatadg
datavol_cnt: 1
vset_cnt: 0
srl: rac1_srl
RLinks:
name=rlk_rac_cluster101_1_rac1_rvg, detached=on,
synchronous=off
```

Note: Once the replication is started the value of the detached flag will change the status from OFF to ON.

Starting replication of Oracle RAC database volume

When you have both the primary and secondary sites set up for replication, you can start replication from the primary site to the secondary site.

Start with the default replication settings:

- Mode of replication: synchronous=off
- Latency Protection: latencyprot=off
- SRL overflow protection: srlprot_autodcm
- Packet size: `packet_size=8400`
- Network protocol: `protocol=UDP`

Method of initial synchronization:

- Automatic synchronization
- Full synchronization with Checkpoint

For guidelines on modifying these settings and information on choosing the method of replication for the initial synchronization:

See the *Veritas Volume Replicator Administrator's Guide*

Starting replication using automatic synchronization

Use the `vradmin` command to start replication or the transfer of data from the primary site to the secondary site over the network. Because the cluster on the secondary site uses only one host name, the command does not require the *sec_host* argument.

To start replication using automatic synchronization

- From the primary site, use the following command to automatically synchronize the RVG on the secondary site:

  ```
  vradmin -g disk_group -a startrep pri_rvg sec_host
  ```

  where:

  - disk_group is the disk group on the primary site that VVR will replicate
  - pri_rvg is the name of the RVG on the primary site
  - sec_host is the virtual host name for the secondary site

  For example:

  ```
  # vradmin -g oradatadg -a startrep rac1_rvg
        rac_cluster102
  ```

Starting replication using full synchronization with Checkpoint

Use the `vradmin` command with the Checkpoint option to start replication using full synchronization with Checkpoint.

To start replication using full synchronization with Checkpoint

1. From the primary site, synchronize the RVG on the secondary site with full synchronization (using the `-c checkpoint` option):

   ```
   vradmin -g disk_group -full -c ckpt_name syncrvg pri_rvg sec_host
   ```

   where:

   - disk_group is the disk group on the primary site that VVR will replicate
   - ckpt_name is the name of the checkpoint on the primary site
   - pri_rvg is the name of the RVG on the primary site
   - *sec_host* is the virtual host name for the secondary site

For example:

```
# vradmin -g oradatadg -c rac1_ckpt syncrvg rac1_rvg
rac_cluster102
```

2 To start replication after full synchronization, enter the following command:

```
# vradmin -g oradatadg -c rac1_ckpt startrep rac1_rvg
rac_cluster102
```

Verifying replication status

Verify that replication is properly functioning.

To verify replication status

1 Check the status of VVR replication:

```
# vradmin -g disk_group_name repstatus rvg_name
```

2 Review the `flags` output for the status. The output may appear as `connected` and `consistent`. For example:

```
# vxprint -g oradatadg -l rlk_rac_cluster102_1_rac1_rvg
  Rlink: rlk_rac_cluster102_1_rac1_rvg
  info: timeout=500 packet_size=8400 rid=0.1078
      latency_high_mark=10000 latency_low_mark=9950
      bandwidth_limit=none
  state: state=ACTIVE
      synchronous=off latencyprot=off srlprot=autodcm
  .
  .
  protocol: UDP/IP
  checkpoint: rac1_ckpt
  flags: write enabled attached consistent connected
 asynchronous
```

Configuring VCS to replicate the database volume using VVR

After configuring both clusters for global clustering and setting up the Oracle RAC database for replication, configure VCS to provide high availability for the

database. Specifically, configure VCS agents to control the cluster resources, including the replication resources.

To view the sample main.cf files on your system:

```
# cd /etc/VRTSvcs/conf/sample_rac
```

The following files include CVM/VVR configuration examples:

```
sfrac_07_main.cf    sfrac_08_main.cf
```

The following sample main.cf files illustrate the VCS configuration changes after setting up an existing Oracle RAC database for replication:

See "sfrac07_main.cf and sample08_main.cf files" on page 618.

About modifying the VCS configuration for replication

The following resources must be configured or modified for replication:

- Log owner group
- RVG group
- CVMVolDg resource
- RVGSharedPri resource
- Oracle RAC database service group

For detailed examples of service group modification:

For more information on service replication resources:

See the *Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide*.

Log owner group

Create a log owner group including the RVGLogowner resources. The RVGLogowner resources are used by:

- RLINKs for the RVG
- RVGLogowner resource. The RVG and its associated disk group are defined as attributes for the RVGLogowner resource.

The RVG log owner service group has an online local firm dependency on the service group containing the RVG.

The VCS uses the following agents to control the folllowing resources:

- RVGLogowner agent to control the RVGLogowner resource

- RVGShared agent to control the RVGShared resource

RVG group

Create an RVG group that includes the RVGShared resource replication objects. Define the RVGShared resource and CVMVolDg resource together within a parallel service group. The group is defined as parallel because it may be online at the same time on all cluster nodes.

CVMVolDg resource

The CVMVolDg resource does not have volumes specified for the CVMVolume attribute; the volumes are contained in the RVG resource. The CVMVolume attribute for the CVMVolDg resource is empty because all volumes in the RVG are defined by the RVG attribute of the RVGShared resource. The RVG service group has an online local firm dependency on the CVM service group.

For a detailed description of the CVMVolDg agent in this guide:

See " CVMVolDg agent" on page 666.

RVGSharedPri resource

Add the RVGSharedPri resource to the existing Oracle RAC database service group. The CVMVolDg resource must be removed from the existing Oracle RAC database service group.

Oracle RAC database service group

The existing Oracle RAC database service group is a parallel group consisting of the Oracle RAC database resource, CVMVolDg resource, and CFSMount resource (if the database resides in a cluster file system). Define the Oracle RAC service group as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.

Configuration examples before and after modification

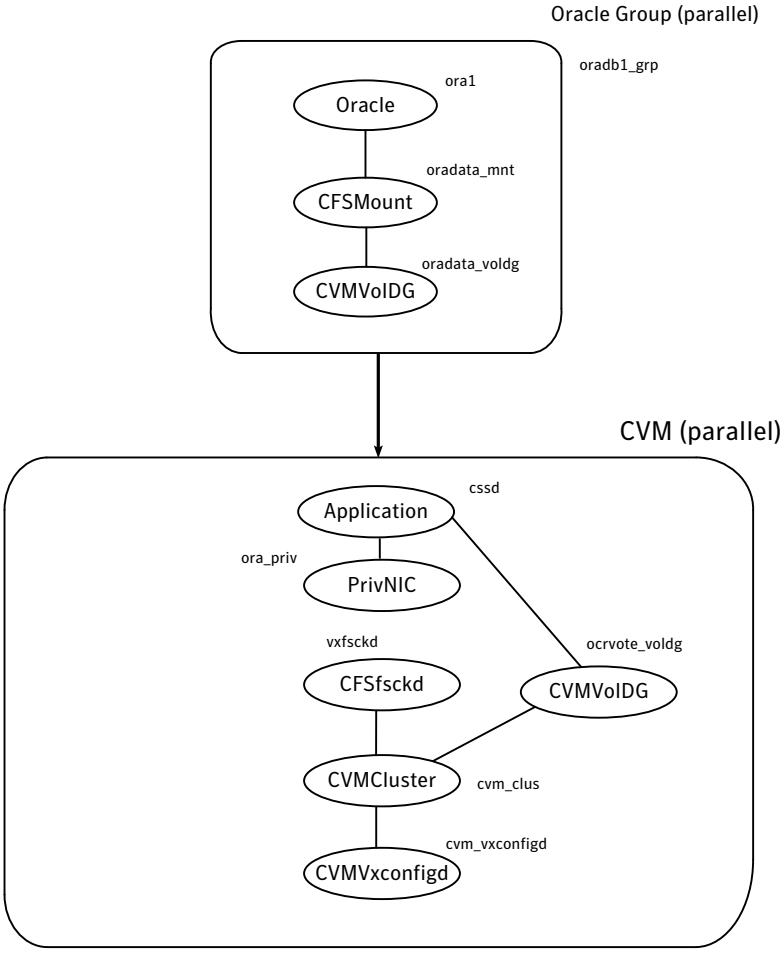
Review the following illustrations that display the changes to the VCS configuration, after setting up replication on the existing Oracle RAC database.

- Configuration before modification:
  Figure 30-1
- Configuration after modification:
  Figure 30-2

All of the dependencies between parent and child groups are online local firm. The CVM service group is the same in all illustrations because its definition requires no changes.

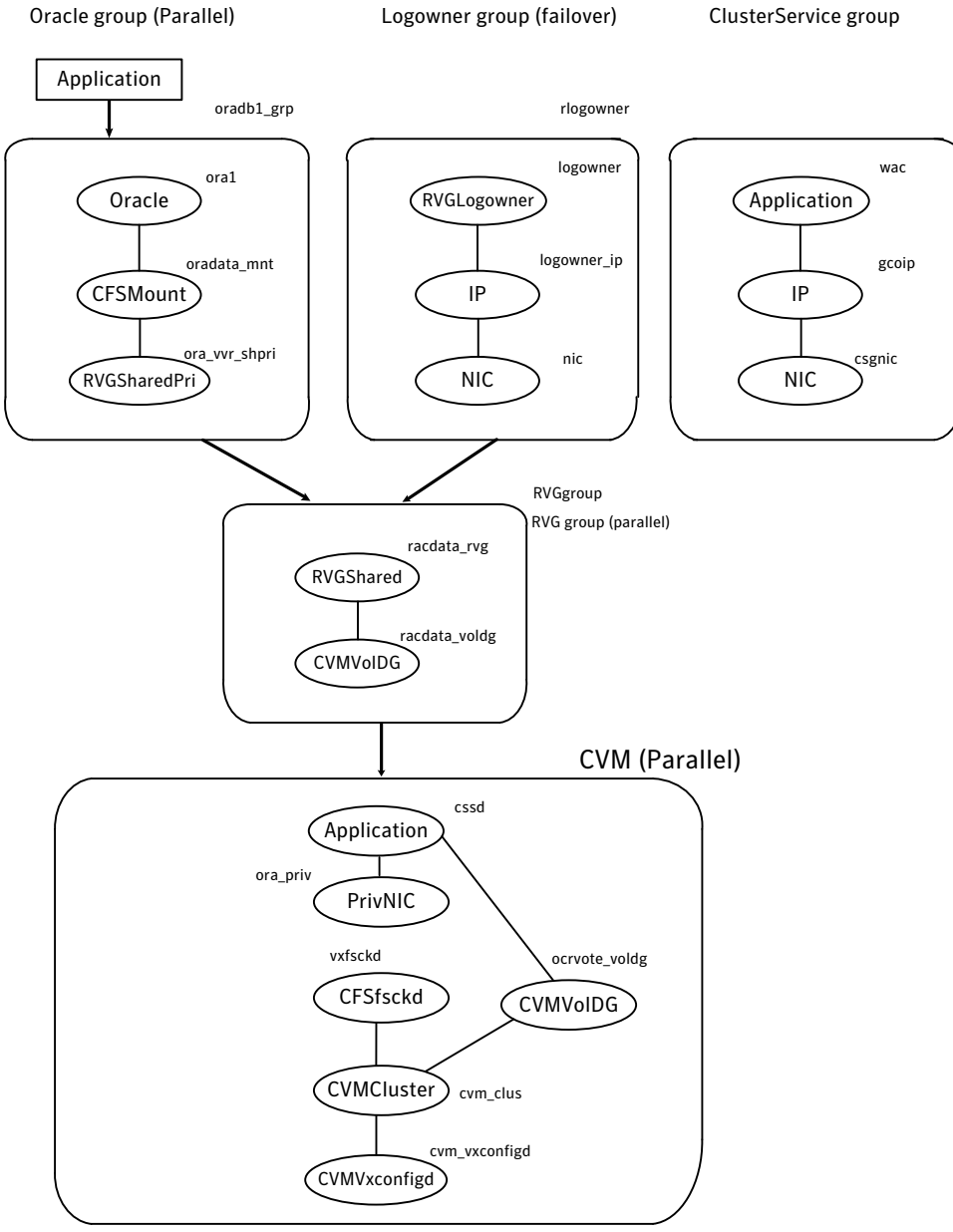
Configuration before modification for replication:

Figure 30-1 Illustration of dependencies before modification for replication (Oracle RAC 10g)



Configuration after modification for replication:

Figure 30-2 Illustration of dependencies after modification for replication (Oracle RAC 10g)



Modifying the VCS Configuration on the Primary Site

The following are the procedural highlights required to modify the existing VCS configuration on the primary site:

- Configure two service groups:
  - A log owner group including the RVGLogowner resource.
  - An RVG group including the RVGShared resource replication objects.
- Add the RVGSharedPri resource to the existing Oracle RAC database service group and define this group as a global group by setting the ClusterList and ClusterFailOverPolicy attributes.
- Move the CVMVolDg resource from the existing Oracle RAC database service group to the newly created RVG group.

To modify VCS on the primary site

1. Log into one of the nodes on the primary cluster.
2. Use the following command to save the existing configuration to disk, and make the configuration read-only while you make changes:

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

3. Use the following command to make a backup copy of the main.cf file:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.orig
```

4. Use vi or another text editor to edit the main.cf file. Review the sample configuration file after the SF Oracle RAC installation.

   Add a failover service group using the appropriate values for your cluster and nodes. Include the following resources:

   - RVGLogowner resource. The node on which the group is online functions as the log owner (node connected to the second cluster for the purpose of replicating data).
   - IP resource
   - NIC resources

   The following are examples of RVGLogowner service group for the different platforms.

```
group rlogowner (
    SystemList = { galaxy = 0, nebula = 1 }
```

```
    AutoStartList = { galaxy,nebula }
    )

    IP logowner_ip (
        Device = lan0
        Address = "10.10.9.101"
        NetMask = "255.255.255.0"
        )

    NIC nic (
        Device = lan0
        NetworkType = ether
        NetworkHosts = "10.10.8.1"
        )

RVGLogowner logowner (
     RVG = rac1_rvg
     DiskGroup = oradatadg
     )
requires group RVGgroup online local firm
logowner requires logowner_ip
logowner_ip requires nic
```

5 Add the RVG service group using the appropriate values for your cluster and nodes.

Example `RVGgroup` service group:

```
group RVGgroup (
     SystemList = { galaxy = 0, nebula = 1 }
     Parallel = 1
     AutoStartList = { galaxy,nebula }
     )

RVGShared racdata_rvg (
     RVG = rac1_rvg
     DiskGroup = oradatadg
     )
     CVMVolDg racdata_voldg (
         CVMDiskGroup = oradatadg
         CVMActivation = sw
         )
requires group cvm online local firm
racdata_rvg requires racdata_voldg
```

6 Modify the Oracle RAC service group using the appropriate values for your cluster and nodes:

- Define the Oracle RAC service group as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute. See the bolded attribute in the example that follows.
- Add the ClusterFailOverPolicy cluster attribute. Symantec recommends using the Manual value. See the bolded attribute in the example.
- Add the RVGSharedPri resource to the group configuration.
- Remove the CVMVolDg resource, if it has been configured in your previous configuration. This resource is now part of the RVG service group.
- Specify the service group (online, local, firm) to depend on the RVG service group.
- Remove the existing dependency of the Database service group on the CVM service group. Remove the line:

```
requires group CVM online local firm
```

- Remove the existing dependency between the CFSMount for the database and the CVMVoldg for the Oracle RAC database. Remove the line:

```
oradata_mnt requires oradata_voldg
```

The following is an example of an Oracle RAC database service group configured for replication:

```
group database_grp (
    SystemList = { galaxy = 0, nebula = 1 }
    ClusterList = { rac_cluster101 = 0, rac_cluster102 = 1 }
    Parallel = 1
    ClusterFailOverPolicy = Manual
    Authority = 1
    AutoStartList = { galaxy,nebula }
    )

    CFSMount oradata_mnt (
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/racdb_vol"
        )

    RVGSharedPri ora_vvr_shpri (
       RvgResourceName = racdata_rvg
```

```
        OnlineRetryLimit = 0
        )

Oracle rac_db (
    Sid @galaxy = vrts1
    Sid @nebula = vrts2
    Owner = Oracle
    Home = "/oracle/orahome"

    StartUpOpt = SRVCTLSTART
    ShutDownOpt = SRVCTLSTOP
    )
requires group RVGgroup online local firm
oradata_mnt requires ora_vvr_shpri
rac_db requires oradata_mnt
```

7 Save and close the main.cf file.

8 Use the following command to verify the syntax of the /etc/VRTSvcs/conf/config/main.cf file:

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

9 Stop and restart VCS.

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

Wait for port h to stop on all nodes, and then restart VCS with the new configuration on all primary nodes:

```
# hastart
```

Modifying the VCS Configuration on the Secondary Site

The following are highlights of the procedure to modify the existing VCS configuration on the secondary site:

- Add the log owner and RVG service groups.
- Add a service group to manage the Oracle RAC database and the supporting resources.
- Define the replication objects and agents, such that the cluster at the secondary site can function as a companion to the primary cluster.

The following steps are similar to those performed on the primary site.

To modify VCS on the secondary site

1. Log into one of the nodes on the secondary site as root.
2. Use the following command to save the existing configuration to disk, and make the configuration read-only while making changes:

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

3. Use the following command to make a backup copy of the main.cf file:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.orig
```

4. Use vi or another text editor to edit the main.cf file. Edit the CVM group on the secondary site.

   Review the sample configuration file after the SF Oracle RAC installation to see the CVM configuration.

   In our example, the secondary site has rac_cluster102 consisting of the nodes mercury and jupiter. To modify the CVM service group on the secondary site, use the CVM group on the primary site as your guide.

5. Add a failover service group using the appropriate values for your cluster and nodes. Include the following resources:

   - RVGLogowner resource. The node on which the group is online functions as the log owner (node connected to the second cluster for the purpose of replicating data).
   - IP resource
   - NIC resources

   Example `RVGLogowner` service group:

```
group rlogowner (
    SystemList = { mercury = 0, jupiter = 1 }
    AutoStartList = { mercury, jupiter }
    )

    IP logowner_ip (
       Device = lan0
       Address = "10.11.9.102"
       NetMask = "255.255.255.0"
       )
```

```
NIC nic (
        Device = lan0
        NetworkHosts = { "10.10.8.1" }
        NetworkType = ether
        )

RVGLogowner logowner (
        RVG = rac1_rvg
        DiskGroup = oradatadg
        )

requires group RVGgroup online local firm
logowner requires logowner_ip
logowner_ip requires nic
```

6 Add the RVG service group using the appropriate values for your cluster and nodes.

The following is an example `RVGgroup` service group:

```
group RVGgroup (
    SystemList = { mercury = 0, jupiter = 1 }
    Parallel = 1
    AutoStartList = { mercury, jupiter }
    )

RVGShared racdata_rvg (
    RVG = rac1_rvg
    DiskGroup = oradatadg
    )

    CVMVolDg racdata_voldg
        CVMDiskGroup = oradatadg
        CVMActivation = sw
        )

requires group cvm online local firm
racdata_rvg requires racdata_voldg
```

7 Add an Oracle RAC service group. Use the Oracle RAC service group on the primary site as a model for the Oracle RAC service group on the secondary site.

- Define the Oracle RAC service group as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.
- Assign this global group the same name as the group on the primary site; for example, *database_grp*.
- Include the ClusterList and ClusterFailOverPolicy cluster attributes. Symantec recommends using the Manual value.
- Add the RVGSharedPri resource to the group configuration.
- Remove the CVMVolDg resource, if it has been configured in your previous configuration. This resource is now part of the RVG service group.
- Specify the service group to depend (online, local, firm) on the RVG service group.

Example of the Oracle RAC group on the secondary site:

```
group database_grp (
    SystemList = { mercury = 0, jupiter = 1 }
    ClusterList = { rac_cluster102 = 0, rac_cluster101 = 1 }
    Parallel = 1
    OnlineRetryInterval = 300
    ClusterFailOverPolicy = Manual
    Authority = 1
    AutoStartList = { mercury, jupiter }
    )

    RVGSharedPri ora_vvr_shpri (
        RvgResourceName = racdata_rvg
        OnlineRetryLimit = 0
        )


    CFSMount oradata_mnt (
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/racdb_vol"
        Critical = 0
        )

RVGSharedPri ora_vvr_shpri (
        RvgResourceName = racdata_rvg
        OnlineRetryLimit = 0
        )
```

```
Oracle rac_db (
     Sid @mercury = vrts1
     Sid @jupiter = vrts2
     Owner = Oracle
     Home = "/oracle/orahome"
     Pfile @mercury = "/oracle/orahome/dbs/initvrts1.ora"
     Pfile @jupiter = "/oracle/orahome/dbs/initvrts2.ora"
     StartUpOpt = SRVCTLSTART
     ShutDownOpt = SRVCTLSTOP
     )

requires group RVGgroup online local firm
oradata_mnt requires ora_vvr_shpri
rac_db requires oradata_mnt
```

8 Save and close the `main.cf` file.

9 Use the following command to verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file:

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

10 Stop and restart VCS.

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

Wait for port h to stop on all nodes, and then restart VCS with the new configuration on all primary nodes:

```
# hastart
```

11 Verify that VCS brings all resources online. On one node, enter the following command:

```
# hagrp -display
```

The Oracle RAC, RVG, and CVM groups are online on both nodes of the primary site. The RVGLogOwner group is online on one node of the cluster. If either the RVG group or the RVGLogOwner group is partially online, manually bring the groups online using the `hagrp -online` command. This information applies to the secondary site, except for the Oracle RAC group which must be offline.

12 Verify the service groups and their resources that are brought online. On one node, enter the following command:

```
# hagrp -display
```

The Oracle RAC service group is offline on the secondary site, but the CVM, RVG log owner, and RVG groups are online.

This completes the setup for an SF Oracle RAC global cluster using VVR for replication. Symantec recommends testing a global cluster before putting it into production.

Using VCS commands on SF Oracle RAC global clusters

For information on the VCS commands for global clusters:

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

Using VVR commands on SF Oracle RAC global clusters

If you have two SF Oracle RAC clusters configured to use VVR for replication, the following administrative functions are available:

- Migration of the role of the primary site to the remote site
- Takeover of the primary site role by the secondary site

About migration and takeover of the primary site role

Migration is a planned transfer of the role of primary replication host from one cluster to a remote cluster. This transfer enables the application on the remote

cluster to actively use the replicated data. The former primary cluster becomes free for maintenance or other activity.

Takeover occurs when an unplanned event (such as a disaster) causes a failure, making it necessary for the applications using the replicated data to be brought online on the remote cluster.

Migrating the role of primary site to the secondary site

After configuring the replication objects within VCS, you can use VCS commands to migrate the role of the cluster on the primary site to the remote cluster. In the procedure below, VCS takes the replicated database service group, *database_grp*, offline on the primary site and brings it online on the secondary site; the secondary site now assumes the role of the primary site.

Note: The `hagrp -switch` command cannot migrate a parallel group within a cluster or between clusters in a global cluster environment.

To migrate the role of primary site to the remote site

1. From the primary site, use the following command to take the Oracle service group offline on all nodes.

   ```
   # hagrp -offline database_grp -any
   ```

   Wait for VCS to take all Oracle service groups offline on the primary site.

2. Verify that the RLINK between the primary and secondary is up to date. Use the `vxrlink -g` command with the status option and specify the RLINK for the primary cluster. You can use the command from any node on the primary cluster.

   For example:

   ```
   # vxrlink -g data_disk_group status rlk_rac_cluster101_priv_rac1_rvg
   ```

   Where rlk_rac_cluster101_priv_rac1_rvg is the RLINK.

3. On the secondary site, which is now the new primary site, bring the Oracle service group online on all nodes:

   ```
   # hagrp -online database_grp -any
   ```

Migrating the role of new primary site back to the original primary site

After migrating the role of the primary site to the secondary site, you can use VCS commands to migrate the role of the cluster on the new primary site to the original primary site. In the procedure below, VCS takes the replicated database service group, *database_grp*, offline on the new primary (former secondary) site and brings it online on the original primary site; the original primary site now resumes the role of the primary site.

Note: The `hagrp -switch` command cannot migrate a parallel group within a cluster or between clusters in a global cluster environment.

To migrate the role of new primary site back to the original primary site

1. Make sure that all CRS resources are online, and switch back the group *database_grp* to the original primary site.

   Issue the following command on the remote site:

   ```
   # hagrp -offline database_grp -any
   ```

2. Verify that the RLINK between the primary and secondary is up to date. Use the `vxrlink -g` command with the status option and specify the RLINK for the primary cluster. You can use the command from any node on the primary cluster.

   For example:

   ```
   # vxrlink -g data_disk_group status rlk_rac_cluster101_priv_rac1_rvg
   ```

   Where rlk_rac_cluster101_priv_rac1_rvg is the RLINK.

3. Make sure that *database_grp* is offline on the new primary site. Then, execute the following command on the original primary site to bring the *database_grp* online:

   ```
   # hagrp -online database_grp -any
   ```

Taking over the primary role by the remote cluster

Takeover occurs when the remote cluster on the secondary site starts the application that uses replicated data. This situation may occur if the secondary

site perceives the primary site as dead, or when the primary site becomes inaccessible (perhaps for a known reason). For a detailed description of concepts of taking over the primary role:

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

Before enabling the secondary site to take over the primary role, the administrator on the secondary site must "declare" the type of failure at the remote (primary, in this case) site and designate the failure type using one of the options for the `haclus` command.

Takeover options are:

- Disaster
- Outage
- Disconnect
- Replica

Disaster

When the cluster on the primary site is inaccessible and appears dead, the administrator declares the failure type as "disaster." For example, fire may destroy a data center, including the primary site and all data in the volumes. After making this declaration, the administrator can bring the service group online on the secondary site, which now has the role as "primary" site.

Outage

When the administrator of a secondary site knows the primary site is inaccessible for a known reason, such as a temporary power outage, the administrator may declare the failure as an "outage." Typically, an administrator expects the primary site to return to its original state.

After the declaration for an outage occurs, the RVGSharedPri agent enables DCM logging while the secondary site maintains the primary replication role. After the original primary site becomes alive and returns to its original state, DCM logging makes it possible to use fast fail back resynchronization when data is resynchronized to the original cluster.

Before attempting to resynchronize the data using the fast fail back option from the current primary site to the original primary site, take the precaution at the original primary site of making a snapshot of the original data. This action provides a valid copy of data at the original primary site for use in the case the current primary site fails before the resynchronization is complete.

See "Examples for takeover and resynchronization" on page 538.

See "Replica" on page 538.

Disconnect

When both clusters are functioning properly and the heartbeat link between the clusters fails, a split-brain condition exists. In this case, the administrator can declare the failure as "disconnect," which means no attempt will occur to take over the role of the primary site at the secondary site. This declaration is merely advisory, generating a message in the VCS log indicating the failure results from a network outage rather than a server outage.

Replica

In the rare case where the current primary site becomes inaccessible while data is resynchronized from that site to the original primary site using the fast fail back method, the administrator at the original primary site may resort to using a data snapshot (if it exists) taken before the start of the fast fail back operation. In this case, the failure type is designated as "replica".

Examples for takeover and resynchronization

The examples illustrate the steps required for an outage takeover and resynchronization.

To take over after an outage

1 From any node of the secondary site, issue the `haclus` command:

```
# haclus -declare outage -clus rac_cluster101
```

2 After declaring the state of the remote cluster, bring the Oracle service group online on the secondary site. For example:

```
# hagrp -online -force database_grp -any
```

To resynchronize after an outage

1 On the original primary site, create a snapshot of the RVG before resynchronizing it in case the current primary site fails during the resynchronization. Assuming the disk group is *data_disk_group* and the RVG is rac1_rvg, type:

```
# vxrvg -g data_disk_group -F snapshot rac1_rvg
```

See the *Veritas Volume Replicator Administrator's Guide* for details on RVG snapshots.

2 Resynchronize the RVG. From the CVM master node of the current primary site, issue the `hares` command and the `-action` option with the fbsync action token to resynchronize the RVGSharedPri resource. For example:

```
# hares -action ora_vvr_shpri fbsync -sys mercury
```

To determine which node is the CVM master node, type:

```
# vxdctl -c mode
```

3 Perform one of the following commands, depending on whether the resynchronization of data from the current primary site to the original primary site is successful:

- If the resynchronization of data is successful, use the `vxrvg` command with the `snapback` option to reattach the snapshot volumes on the original primary site to the original volumes in the specified RVG:

  ```
  # vxrvg -g data_disk_group snapback rac1_rvg
  ```

- A failed attempt at the resynchronization of data (for example, a disaster hits the primary RVG when resynchronization is in progress) could generate inconsistent data.
  You can restore the contents of the RVG data volumes from the snapshot taken in step 1:

  ```
  # vxrvg -g data_disk_group snaprestore rac1_rvg
  ```

Troubleshooting CVM and VVR components of SF Oracle RAC

The following topic is useful for troubleshooting the VVR component of SF Oracle RAC.

Updating the rlink

If the rlink is not up to date, use the `hares -action` command with the `resync` action token to synchronize the RVG.

The following command example is issued on any node (`galaxy`, in this case) in the primary cluster, specifying the RVGSharedPri resource, `ora_vvr_shpri`:

```
# hares -action ora_vvr_shpri resync -sys galaxy
```

VCS agents to manage wide-area failover

VCS agents now manage external objects that are part of wide-area failover. These objects include replication, DNS updates, and so on. These agents provide a robust framework for specifying attributes and restarts, and can be brought online upon fail over.

VCS provides agents for other array-based or application-based solutions. This section covers the replication agents that is bundled with VVR. See the VCS replication agent documentation for more details.

Note: See the Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide for more information about the RVG and RVGPrimary agents.

Note: The RVGSnapshot agent is not supported for SF Oracle RAC.

DNS agent

The DNS agent updates the canonical name-mapping in the domain name server after a wide-area failover. See the Veritas Cluster Server Bundled Agents Reference Guide for more information about the agent.

RVG agent

The RVG agent manages the Replicated Volume Group (RVG). Specifically, it brings the RVG online, monitors read-write access to the RVG, and takes the RVG offline. Use this agent when using VVR for replication.

RVGPrimary agent

The RVGPrimary agent attempts to migrate or take over a Secondary to a Primary following an application failover. The agent has no actions associated with the offline and monitor routines.

Section 8

Uninstallation of SF Oracle RAC

- Chapter 31. Preparing to uninstall SF Oracle RAC from a cluster
- Chapter 32. Uninstalling SF Oracle RAC from a cluster

Chapter 31

Preparing to uninstall SF Oracle RAC from a cluster

This chapter includes the following topics:

- About uninstalling SF Oracle RAC from a cluster
- Options for uninstalling SF Oracle RAC
- Preparing to uninstall SF Oracle RAC from a cluster

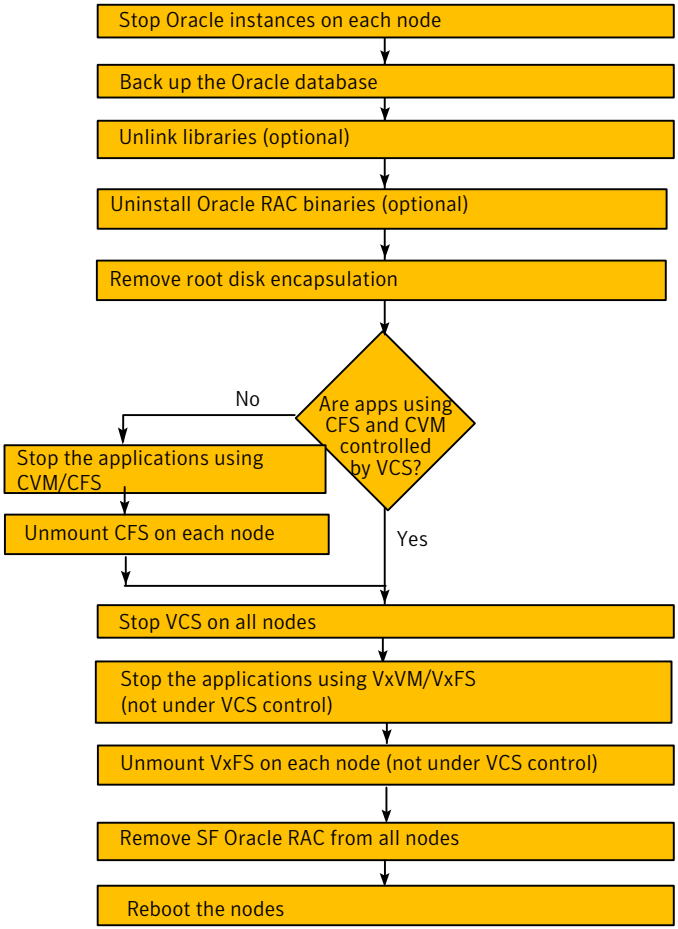
About uninstalling SF Oracle RAC from a cluster

You can uninstall SF Oracle RAC using the uninstallsfrac program.

Note: After you uninstall SF Oracle RAC, you cannot access the Oracle database as Veritas Volume Manager and Veritas File System are uninstalled from the cluster. Make sure that you back up the Oracle database before you uninstall SF Oracle RAC.

Figure 31-1 illustrates the steps that are required to uninstall SF Oracle RAC from a cluster.

Figure 31-1 SF Oracle RAC uninstallation



Options for uninstalling SF Oracle RAC

Table 31-1 lists the available options for uninstalling SF Oracle RAC:

Table 31-1 Options for uninstalling SF Oracle RAC

Options	Description
SF Oracle RAC uninstallation program	Use the uninstallsfrac program to uninstall SF Oracle RAC. See "Preparing to uninstall SF Oracle RAC from a cluster" on page 547.
Response file	Use a response file to automate or perform an unattended uninstallation of SF Oracle RAC. See "Uninstalling SF Oracle RAC using a response file" on page 564.

Preparing to uninstall SF Oracle RAC from a cluster

Perform the steps in the following procedure before you uninstall SF Oracle RAC from a cluster.

To prepare to uninstall SF Oracle RAC from a cluster

1. Stop Oracle instances.

   See "Stopping Oracle instances" on page 548.

2. Back up the Oracle database.

   See "Backing up the Oracle database" on page 549.

3. Unlink the SF Oracle RAC libraries from Oracle RAC libraries (optional).

   See "Unlinking the SF Oracle RAC libraries from Oracle RAC" on page 549.

4. Uninstalling Oracle RAC (optional)

   See "Uninstalling Oracle RAC (optional)" on page 551.

5. Stop the applications that use CFS (outside of VCS control).

   See "Stopping the applications that use CVM or CFS (outside of VCS control)" on page 551.

6. Unmount CFS file systems (outside of VCS control).

   See "Unmounting CFS file systems (outside of VCS control)" on page 551.

7. Stop VCS.

   See "Stopping VCS" on page 552.

8. Stop the applications that use VxFS (outside of VCS control).

   See "Stopping the applications that use VxVM or VxFS (outside of VCS control)" on page 553.

9 Unmount VxFS file systems (outside of VCS control).

See "Unmounting VxFS file systems (outside of VCS control)" on page 553.

10 Stop the AMF driver.

See "Stopping the AMF driver" on page 553.

Stopping Oracle instances

You need to stop Oracle Clusterware and the Oracle instances on the cluster nodes where you want to uninstall SF Oracle RAC. Before you stop the Oracle instances, stop the applications that are dependent on the service groups that contain Oracle.

The procedure in this section provides instructions to stop the instances on a two-node cluster; the nodes are galaxy and nebula. Depending on the VCS configuration, the procedure to stop Oracle instances may vary.

To stop Oracle instances

1 Log in as the superuser on one of the nodes in the cluster.

2 On each node, take the Oracle resources in the VCS configuration file (main.cf) offline.

```
# hagrp -offline oracle_group -sys node_name
```

For example:

```
# hagrp -offline ora1 -sys galaxy

# hagrp -offline ora1 -sys nebula
```

These commands stop the Oracle resources under VCS control.

If the database is not managed by VCS, stop the Oracle database as follows:

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

3 Verify that the state of the Oracle (if the database is managed by VCS) and CVM service groups are offline and online respectively.

```
# hagrp -state
Group       Attribute      System        Value
ora1        State          galaxy      |OFFLINE|
ora1        State          nebula      |OFFLINE|
cvm         State          galaxy      |ONLINE|
cvm         State          nebula      |ONLINE|
```

Backing up the Oracle database

If you plan to retain the Oracle database, you must back up the Oracle database.

For instructions on backing up the Oracle database, see the Oracle documentation.

Unlinking the SF Oracle RAC libraries from Oracle RAC

If you want to reuse the Oracle RAC binaries, unlink the SF Oracle RAC libraries from Oracle RAC.

Note: The Oracle RAC binaries that are located on Veritas File System will not be accessible after the uninstallation.

To unlink the SF Oracle RAC libraries from Oracle RAC libraries

1 Unlink the Veritas VCSMM library.

Perform this step on each node if the Oracle libraries are on local storage. If the Oracle libraries are installed on shared storage, perform the step on one node only.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
$ cd $CRS_HOME/lib
```

For Oracle RAC 11g Release 2:

```
$ cd $GRID_HOME/lib
```

For Oracle RAC 10g and Oracle RAC 11g (HP-UX (PA) architectures):

```
$ ln -sf $CRS_HOME/lib/libskgxns.sl libskgxn2.sl
```

For Oracle RAC 11g (HP-UX (IA) architectures):

```
$ ln -sf $CRS_HOME/lib/libskgxns.so libskgxn2.so
```

For Oracle RAC 10g and Oracle RAC 11g (HP-UX (IA) architectures):

```
$ ln -sf $CRS_HOME/lib/libskgxns.so libskgxn2.so

$ ln -sf $GRID_HOME/lib/libskgxns.so libskgxn2.so
```

2 For Oracle RAC 10g: Unlink the Veritas VCS IPC library.

Perform this step on each node if the Oracle libraries are on local storage. If the Oracle libraries are installed on shared storage, perform the step on one node only.

```
$ cd $ORACLE_HOME/lib

$ make -f ins_rdbms.mk rac_on
$ make -f ins_rdbms.mk ioracle
```

3 Unlink the Veritas ODM library.

Perform this step on each node if the Oracle libraries are on local storage. If the Oracle libraries are installed on shared storage, perform the step on one node only.

```
$ cd $ORACLE_HOME/lib
```

For Oracle RAC 10g:

```
$ ln -sf $ORACLE_HOME/lib/libodmd10.so libodm10.so
```

For Oracle RAC 11g:

```
$ ln -sf $ORACLE_HOME/lib/libodmd11.so libodm11.so
```

Uninstalling Oracle RAC (optional)

You cannot use the Oracle database after you uninstall SF Oracle RAC. However, you can continue using the Oracle RAC software, provided the Oracle Clusterware and database binaries are not installed on Veritas file system. To continue using Oracle RAC, unlink the SF Oracle RAC libraries from Oracle RAC as described in the preceding topic.

For instructions on uninstalling Oracle RAC, see the Oracle documentation.

Stopping the applications that use CVM or CFS (outside of VCS control)

You need to stop the applications that use CVM volumes or CFS mount points not controlled by VCS.

To stop the applications that use CVM or CFS (outside of VCS control)

1 Using native application commands, stop the applications that use CVM or a CFS.

2 Verify that no processes use the CFS mount point:

```
# fuser -c mount_point
```

Unmounting CFS file systems (outside of VCS control)

You need to unmount CFS file systems that are not under VCS control on all nodes.

To unmount CFS file systems not under VCS control

1. Determine the file systems that need to be unmounted by checking the output of the mount command. The command lists all the mounted clustered file systems. Consult the main.cf file for identifying the files that are under VCS control.

   ```
   # mount -v | grep vxfs | grep cluster
   ```

2. Unmount each file system that is not controlled by VCS:

   ```
   # umount mount_point
   ```

Stopping VCS

Stop VCS to take the service groups on all nodes offline.

The process also stops replication as the replication service group is also taken offline.

To stop VCS

1. Log in as the superuser on one of the cluster nodes.
2. Stop VCS on all nodes:

   ```
   # hastop -all
   ```

3. Verify the output of the `gabconfig -a` command to ensure that VCS has been stopped.

   In this command output, the VCS engine or high availability daemon (HAD) port h is not displayed. This output indicates that VCS has been stopped.

   ```
   # gabconfig -a
   GAB Port Memberships
   ===============================================================
   Port a gen 5c3d0b membership 01
   Port b gen 5c3d10 membership 01
   Port d gen 5c3d0c membership 01
   Port o gen 5c3d0f membership 01
   ```

Stopping the applications that use VxVM or VxFS (outside of VCS control)

You need to stop all applications that use VxVM volumes or VxFS mount points not under VCS control.

To stop the applications that use VxVM or VxFS (outside of VCS control)

1. Using native application commands, stop the applications that use VxVM or VxFS.
2. Verify that no processes use the VxFS mount point:

```
# fuser -c mount_point
```

Unmounting VxFS file systems (outside of VCS control)

You need to unmount VxFS file systems that are not under VCS control on all nodes.

Note: To avoid issues on rebooting, you must remove all entries of VxFS from the /etc/fstab file.

To unmount VxFS file systems not under VCS control

1. Determine the file systems that need to be unmounted by checking the output of the mount command. The command lists all the mounted file systems.

```
# mount -v | grep vxfs
```

2. Unmount each file system that is not under VCS control:

```
# umount mount_point
```

Stopping the AMF driver

If the AMF driver is loaded, stop the driver before you run the uninstallation program. Check the setting of the `AMF_START` and `AMF_STOP` attributes in the `/etc/rc.config.d/amf` file to determine if the driver is loaded. The driver is loaded if the `AMF_START` is set to 1.

To stop the AMF driver

1 Update the `AMF_START` and `AMF_STOP` settings in the `/etc/rc.config.d/amf` file as follows:

```
AMF_START=0
AMF_STOP=1
```

2 Stop the AMF driver:

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

Chapter 32

Uninstalling SF Oracle RAC from a cluster

This chapter includes the following topics:

- Uninstalling SF Oracle RAC from a cluster
- Uninstalling SF Oracle RAC with the Veritas Web-based installer
- Uninstalling SF Oracle RAC using a response file

Uninstalling SF Oracle RAC from a cluster

You can remove the SF Oracle RAC depots from all nodes in the SF Oracle RAC cluster using the uninstallsfrac program. The uninstallsfrac program can be accessed from the product disc or from the `/opt/VRTS/install` directory.

Perform the steps in the following procedure to remove SF Oracle RAC from a cluster.

To remove SF Oracle RAC from a cluster

1. Remove the CP server configuration using the removal script.

   See " Removing the CP server configuration using the removal script" on page 556.

2. Remove the SF Oracle RAC depots. You can remove the depots using the uninstallation program or using the response file.

   Using the uninstallation program:

   See "Removing the SF Oracle RAC depots" on page 560.

   Using the response file:

   See "Uninstalling SF Oracle RAC using a response file" on page 564.

3 Remove other configuration files (optional).

See "Removing other configuration files (optional)" on page 561.

4 Remove the Storage Foundation for Databases (SFDB) repository after removing the product.

See "Removing the Storage Foundation for Databases (SFDB) repository after removing the product" on page 562.

5 Reboot the nodes.

```
# shutdown -r now
```

Removing the CP server configuration using the removal script

This section describes how to remove the CP server configuration from a node or cluster hosting the CP server.

Warning: Ensure that no SF Oracle RAC cluster is using the CP server that will have its CP server configuration removed.

A configuration utility that is part of VRTScps package is used to remove the CP server configuration. When using the configuration utility, a configuration removal script is run and the following tasks are performed:

- All CP server configuration files are removed
- The VCS configuration for CP server is removed

After running the utility and script, you can then uninstall VCS from the node or cluster.

Note: The configuration script has to run only once per CP server (which can be on a single node or SFHA cluster), when removing the CP server configuration.

The configuration utility performs the following steps to remove the CP server configuration:

- Takes the the CP server service group (CPSSG) offline, if it is online
- Removes the CPSSG service group from the VCS configuration

The following procedure describes how to remove the CP server configuration.

To remove the CP server configuration

1 To run the configuration removal script, enter the following command on the node where you want to remove the CP server configuration:

```
root@mycps1.symantecexample.com # /opt/VRTScps/bin/configure_cps.pl
```

2 The Veritas Coordination Point Server Configuration utility appears with an option menu.

```
VERITAS COORDINATION POINT SERVER CONFIGURATION UTILITY
=======================================================

Select one of the following:

[1] Configure Coordination Point Server on single node VCS system

[2] Configure Coordination Point Server on SFHA cluster

[3] Unconfigure Coordination Point Server
```

3 Select option 3 to unconfigure the Coordination Point Server.

4 A warning appears and prompts you to confirm the action to unconfigure the Coordination Point Server.

Enter "y" to proceed.

```
WARNING: Unconfiguring Coordination Point Server stops the
vxcpserv process. VCS clusters using this server for
coordination purpose will have one less coordination point.

Are you sure you want to bring down the cp server? (y/n)
(Default:n) :y
```

5 After entering "y" to proceed, messages appear informing you of the progress in removing the CP server configuration.

When the CP server configuration has been unconfigured, a success message appears.

For an example of the messages from a single node VCS cluster:

```
A single node VCS cluster is currently configured.
Stopping the CP server ...

Removing the CP Server from VCS configuration..

Removing resource dependencies...
Deleting the resources configured under CPSSG service group...
Deleting the CPSSG service group...

Successfully unconfigured the Veritas Coordination Point Server.
```

For an example of the messages from a CP server on an SFHA cluster:

```
A multinode CP Server cluster is currently configured.
Stopping the CP server ...

Removing the CP Server from VCS configuration..

Removing resource dependencies...
Deleting the resources configured under CPSSG service group...
Deleting the CPSSG service group...

Successfully unconfigured the Veritas Coordination Point Server.
```

6 You are then prompted to delete the CP server database. Enter "y" to delete the database. For example:

```
Do you want to delete the CP Server database? (y/n) (Default:n) :
```

7 Enter "y" at the prompt to confirm the deletion of the CP server database.

```
Warning: This database won't be available if CP server
is reconfigured on the cluster. Are you sure you want to
proceed with the deletion of database? (y/n) (Default:n) :
```

8 Enter "y" to delete the CP server configuration file and log files. For example:

```
Do you want to delete the CP Server configuration file
(/etc/vxcps.conf) and log files (in /var/VRTScps)? (y/n)
(Default:n) : y
```

9 Run the `hagrp -state` command to ensure that the CPSSG service group has been removed from the node. For example:

```
root@mycps1.symantecexample.com # hagrp -state CPSSG

VCS WARNING V-16-1-40131 Group CPSSG does not exist
in the local cluster
```

Manually remove the CP server fencing configuration

The following procedure describes how to manually remove the CP server fencing configuration from the CP server. This procedure is performed as part of the process to stop and remove server-based IO fencing.

Note: This procedure must be performed after the SF Oracle RAC cluster has been stopped, but before the SF Oracle RAC cluster software is uninstalled.

This procedure is required so that the CP server database can be reused in the future for configuring server-based fencing on the same SF Oracle RAC cluster(s).

Perform the steps in the following procedure to manually remove the CP server fencing configuration.

Note: The `cpsadm` command is used in the following procedure. For detailed information about the `cpsadm` command, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

To manually remove the CP server fencing configuration

1. Unregister all SF Oracle RAC cluster nodes from all CP servers using the following command:

   ```
   # cpsadm -s cp_server -a unreg_node -u uuid -n nodeid
   ```

2. Remove the SF Oracle RAC cluster from all CP servers using the following command:

   ```
   # cpsadm -s cp_server -a rm_clus -u uuid
   ```

3. Remove all the SF Oracle RAC cluster users communicating to CP servers from all the CP servers using the following command:

   ```
   # cpsadm -s cp_server -a rm_user -e user_name -g domain_type
   ```

4. Proceed to uninstall the SF Oracle RAC cluster software.

Removing the SF Oracle RAC depots

The installer offers the option to remove the Veritas Volume Manager depots. The uninstallsfrac program can remove these depots only if the root disk is not under VxVM control and there are no open volumes.

The installer performs the following tasks:

- Removes the SF Oracle RAC depots.
- Removes the language depots, if installed.

Note: The following directories remain after uninstallation: `/opt/VRTS`, `/opt/VRTSperl`, `/etc/VRTSvcs`, `/var/VRTSvcs`, `/var/VRTSat_lhc`, `/var/VRTSat`. They contain logs and configuration information for future reference. You may or may not remove them.

To remove the SF Oracle RAC depots

1. Log in as the superuser on any node in the cluster.
2. Navigate to the directory that contains the uninstallsfrac program:

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

3 Start the uninstallsfrac program:

```
# ./uninstallsfrac galaxy nebula
```

The program displays the directory where the logs are created and the copyright message.

4 If you have VxVM installed, indicate whether or not you want to remove the VxVM depots from all nodes in the cluster. Enter **y** only if the root disk is outside of VxVM control.

The uninstallsfrac program performs the following tasks:

- Checks the operating system on each node
- Verifies the system-to-system communication
- Verifies the licenses
- Checks for the SF Oracle RAC depots installed on the nodes. This process involves identifying system uninstallation requirements and dependencies between depots to determine the safety and order of uninstalling depots.

5 Confirm to uninstall SF Oracle RAC.

```
All SF Oracle RAC processes that are currently running must be stopped.
Do you want to stop SF Oracle RAC processes now? [y,n,q,?] (y) y
```

Note: If you have not already unmounted the VxFS file systems, the installer will display a message asking that the file systems be unmounted. Make sure that you unmount the file systems before you proceed.

The program performs the following tasks:

- Stops the agents and performs verifications on each node to proceed with uninstallation
- Stops the SF Oracle RAC processes and uninstalls the SF Oracle RAC depots
- Displays the location of the uninstallation summary and log files for reference.

Removing other configuration files (optional)

You may want to remove the following configuration files that remain after you run the uninstallsfrac program:

```
/etc/vcsmmtab
/etc/vxfentab
```

```
/etc/vxfendg
/etc/llttab
/etc/gabtab
/etc/llthosts
```

To remove the configuration files:

```
# rm /etc/vcsmmtab
# rm /etc/vxfentab
# rm /etc/vxfendg
# rm /etc/llttab
# rm /etc/gabtab
# rm /etc/llthosts
```

Removing the Storage Foundation for Databases (SFDB) repository after removing the product

After removing the product, you can remove the SFDB repository file and any backups.

Removing the SFDB repository file will disable the SFDB tools.

To remove the SFDB repository

1. Change directories to the location of the local lookup information for the Oracle SID.

   For example:

   ```
   # cd /var/vx/vxdba/$ORACLE_SID
   ```

2. Identify the SFDB repository file and any associated links:

   For example:

   ```
   # ls -al
   ```

```
lrwxrwxrwx   1 oracle   oinstall      26 Jul 21 13:58 .sfdb_rept -> \
/ora_data1/TEST/.sfdb_rept
```

   ```
   # cd /ora_data1/TEST
   ```

   Follow the symlink of .sfdb_rept.

3 Remove the repository directory containing the repository file and all backups.

For example:

```
# rm -rf .sfdb_rept
```

4 Remove the local lookup directory for the Oracle SID:

```
# cd /var/vx/vxdba

# rm -rf $ORACLE_SID
```

This completes the removal of the SFDB repository.

Uninstalling SF Oracle RAC with the Veritas Web-based installer

This section describes how to uninstall with the Veritas Web-based installer.

To uninstall SF Oracle RAC

1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.

2 In an HA configuration, stop VCS processes on either the local system or all systems.

To stop VCS processes on the local system:

```
# hastop -local
```

To stop VCS processes on all systems:

```
# hastop -all
```

3 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 93.

4 On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.

5 Select **Veritas Storage Foundation for Oracle RAC** from the Product drop-down list, and click **Next**.

6 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Validate**.

7 After the validation completes successfully, click **Next** to uninstall SF Oracle RAC on the selected system.

8 If there are any processes running on the target system, the installer stops the processes. Click **Next**.

9 After the installer stops the processes, the installer removes the products from the specified system.

Click **Next**.

10 After the uninstall completes, the installer displays the location of the summary, response, and log files. If required, view the files to confirm the status of the removal.

11 Click **Finish**.

The Web-based installer prompts you for another task.

Uninstalling SF Oracle RAC using a response file

Perform the steps in the following procedure to uninstall SF Oracle RAC using a response file.

To uninstall SF Oracle RAC using a response file

1 Make sure that you have completed the pre-uninstallation tasks.

2 Create a response file using one of the available options.

For information on various options available for creating a response file:

See "About response files" on page 371.

Note: You must replace the host names in the response file with that of the systems from which you want to uninstall SF Oracle RAC.

For a sample response file:

See "Sample response file for uninstalling SF Oracle RAC" on page 566.

3 Navigate to the directory containing the SF Oracle RAC uninstallation program:

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

4 Start the uninstallation:

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

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

5 Remove other Veritas configuration files and depots that may be present.

6 Reboot the nodes:

```
# shutdown -r now
```

Response file variables to uninstall SF Oracle RAC

Table 32-1 lists the response file variables that you can define to uninstall SF Oracle RAC.

Table 32-1 Response file variables specific to uninstalling SF Oracle RAC

Variable	List or Scalar	Description
CFG{opt}{uninstall}	Scalar	Uninstalls SF Oracle RAC depots. (Required)
CFG{systems}	List	List of systems on which the product is to be uninstalled. (Required)
CFG{prod}	Scalar	Defines the product to be uninstalled. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *remsh* must be used instead of ssh as the communication method between systems. (Optional)

Table 32-1 Response file variables specific to uninstalling SF Oracle RAC *(continued)*

Variable	List or Scalar	Description
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)

Sample response file for uninstalling SF Oracle RAC

The following sample response file uninstalls SF Oracle RAC from nodes, galaxy and nebula.

```
our %CFG;

$CFG{opt}{uninstall}=1;
$CFG{prod}="SFRAC51";
$CFG{systems}=[ qw(galaxy nebula) ];

1;
```

Section 9

Installation reference

- Appendix A. SF Oracle RAC installation depots
- Appendix B. Installation scripts
- Appendix C. SF Oracle RAC installation and configuration sample values
- Appendix D. Sample configuration files
- Appendix E. Setting up inter-system communication
- Appendix F. Automatic Storage Management
- Appendix G. Creating a test database
- Appendix H. High availability agent information
- Appendix I. SF Oracle RAC deployment scenarios

Appendix A

SF Oracle RAC installation depots

This appendix includes the following topics:

- SF Oracle RAC installation depots

SF Oracle RAC installation depots

Table A-1 lists the depot name and contents for each SF Oracle RAC depot.

Table A-1 List of SF Oracle RAC depots

depot	Content	Configuration
VRTSat	Required to use Symantec Product Authentication Service. Contains the binaries for Symantec Product Authentication Service. Installs Symantec Product Authentication Service, which provides authentication services for other Symantec products. VRTSat contains a server and client component. The server provides services for a root broker, authentication broker, or both. The client allows Symantec products to communicate with the brokers.	Minimum

Table A-1 List of SF Oracle RAC depots *(continued)*

depot	Content	Configuration
VRTScps	Required for Coordination Point Server (CPS). Depends on VRTSvxfen. Contains the binaries for the Veritas Coordination Point Server.	Recommended
VRTSdbac	Depends on VRTSgab, VRTSllt, VRTSvcs, VRTSvxfen Contains the cluster membership and IPC components and VCS agents for Oracle RAC.	Minimum
VRTSgab	Depends on VRTSllt. Contains the binaries for Veritas Cluster Server group membership and atomic broadcast services.	Minimum
VRTSllt	Contains the binaries for Veritas 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
VRTSvcs	Depends on VRTSvxfen, VRTSgab, and VRTSllt. Contains the following components: ■ Contains the binaries for Veritas Cluster Server. ■ Contains the binaries for Veritas Cluster Server manual pages. ■ Contains the binaries for Veritas Cluster Server English message catalogs. ■ Contains the binaries for Veritas Cluster Server utilities. These utilities include security services.	Minimum
VRTSvcsag	Depends on VRTSvcs. Contains the binaries for Veritas Cluster Server bundled agents.	Minimum

Table A-1 List of SF Oracle RAC depots *(continued)*

depot	Content	Configuration
VRTSvcsea	Required for VCS with the high availability agent for Oracle. VRTSvcsea contains the binaries for Veritas high availability agents for DB2, Sybase, and Oracle.	Recommended
VRTSvlic	Contains the binaries for Symantec License Utilities.	Minimum
VRTSvxfen	Depends on VRTSgab. Contains the binaries for Veritas I/O fencing.	Minimum
VRTScavf	Veritas Cluster Server Agents for Storage Foundation Cluster File System	Minimum
VRTSdbed	Veritas Storage Foundation for Oracle	Minimum
VRTSfssdk	Veritas File System Software Developer Kit For VxFS APIs, the depot 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.	All
VRTSglm	Veritas Group Lock Manager for Storage Foundation Cluster File System	Minimum
VRTSgms	Veritas Group Messaging Services for Storage Foundation Cluster File System	Minimum
VRTSob	Veritas Enterprise Administrator	Recommended
VRTSodm	ODM Driver for VxFS Oracle Disk Manager allows Oracle to improve performance and manage system bandwidth.	Minimum
VRTSvxfs	Veritas File System binaries	Minimum
VRTSvxvm	Veritas Volume Manager binaries	Minimum
VRTSaslapm	Volume Manager ASL/APM	Minimum
VRTSsfmh	Veritas Storage Foundation Managed Host	Recommended

Appendix B

Installation scripts

This appendix includes the following topics:

- About installation scripts
- Installation script options

About installation scripts

Veritas Storage Foundation and High Availability Solutions 5.1 Service Pack 1 provides several installation scripts.

An alternative to the `installer` script is to use a product-specific installation script. If you obtained a Veritas product from an electronic download site, which does not include the installer, use the appropriate product installation script.

The following product installation scripts are available:

Veritas Cluster Server (VCS)	`installvcs`
Veritas Storage Foundation (SF)	`installsf`
Veritas Storage Foundation and High Availability (SFHA)	`installsfha`
Veritas Storage Foundation Cluster File System (SFCFS)	`installsfcfs`
Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)	`installsfrac`
Symantec Product Authentication Service (AT)	`installat`
Veritas Dynamic Multi-pathing	`installdmp`

To use the installation script, enter the script name at the prompt. For example, to install Veritas Storage Foundation, type `./installsf` at the prompt.

Installation script options

Table B-1 shows command line options for the installation script. For an initial install or upgrade, options are not usually required. The installation script options apply to all Veritas Storage Foundation product scripts, except where otherwise noted.

See "About installation scripts" on page 573.

Table B-1 Available command line options

Command Line Option	Function
system1 system2...	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.
–addnode	Adds a node to a high availability cluster.
–allpkgs	Displays all depots and patches required for the specified product. The depots and patches are listed in correct installation order. The output can be used to create scripts for command line installs, or for installations over a network.
–comcleanup	The `-comcleanup` option removes the ssh or remsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or remsh are abruptly terminated.
–configure	Configures the product after installation.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
-copyinstallscripts	Use this option when you manually install products and want to use the intallation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `-rootpath` option. The following examples demonstrate the usage for this option: ■ `./installer -copyinstallscripts` Copies the installation and uninstallation scripts for all products in the release to `/opt/VRTS/install`. It also copies the installation Perl libraries to `/opt/VRTSperl/lib/site_perl/`*`release_name`*. ■ `./install`*`product_name`* `-copyinstallscripts` Copies the installation and uninstallation scripts for the specified product and any subset products for the product to `/opt/VRTS/install`. It also copies the installation Perl libraries to `/opt/VRTSperl/lib/site_perl/`*`release_name`*. ■ `./installer -copyinstallscripts -rootpath` *`alt_root_path`* The path *alt_root_path* can be a directory like `/rdisk2`. In that case, this command copies installation and uninstallation scripts for all the products in the release to `/rdisk2/opt/VRTS/install`. CPI perl libraries are copied to `/rdisk2/opt/VRTSperl/lib/site_perl/`*`release_name`*, where the *release_name* is a string that starts with UXRT and includes the release version with no punctuation.
–fencing	Configures I/O fencing in a running cluster.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
–hostfile *full_path_to_file*	Specifies the location of a file that contains a list of hostnames on which to install.
–ignorepatchreqs	The `-ignorepatchreqs` option is used to allow installation or upgrading even if the prerequisite depots or patches are missed on the system.
–install	The `-install` option is used to install products on systems.
–installallpkgs	Specifies that all depots are installed.
–installminpkgs	Specifies that the minimum depot set is installed.
–installrecpkgs	Specifies that the required depot set is installed.
–keyfile *ssh_key_file*	Specifies a key file for secure shell (SSH) installs. This option passes `-i ssh_key_file` to every SSH invocation.
–license	Registers or updates product licenses on the specified systems.
–listpatches	The `-listpatches` option displays product patches in correct installation order.
–logpath *log_path*	Specifies a directory other than `/opt/VRTS/install/logs` as the location where installer log files, summary files, and response files are saved.
–makeresponsefile	The `-makeresponsefile` generates a response file without doing an actual installation. Text displaying install, uninstall, start, and stop actions are simulations. These actions are not being performed on the system.
–minpkgs	Displays the minimal depots and patches required for the specified product. The depots and patches are listed in correct installation order. Optional depots are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
–patchpath *patch_path*	Designates the path of a directory that contains all patches to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
–pkginfo	Displays a list of depots and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the -pkginfo option with the installvcs script to display VCS depots.
–pkgpath *package_path*	Designates the path of a directory that contains all depots to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
–pkgset	Discovers and displays the depot group (minimum, recommended, all) and depots that are installed on the specified systems.
–pkgtable	Displays product's depots in correct installation order by group.
–postcheck	Checks for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups.
–precheck	Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.
–recpkgs	Displays the recommended depots and patches required for the specified product. The depots and patches are listed in correct installation order. Optional depots are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option.
–redirect	Displays progress details without showing the progress bar.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
–requirements	The `-requirements` option displays required OS version, required patches, file system space, and other system requirements in order to install the product.
–responsefile *response_file*	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.
–rootpath *root_path*	Specifies an alternative root directory on which to install depots. On HP-UX operating systems, `-rootpath` passes `-I path` to `swinstall`.
–rsh	Specify this option when you want to use remsh and rcp for communication between systems instead of the default ssh and scp.
–security	Enable or disable Symantec Product Authentication Service in a VCS cluster that is running. You can specify this option with the `installvcs`, `installsfha` or `installsfcfs` scripts. For more information about Symantec Product Authentication Service in a VCS cluster, see the *Veritas Cluster Server Installation Guide*.
–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.
–start	Starts the daemons and processes for the specified product.
–stop	Stops the daemons and processes for the specified product.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
–tmppath *tmp_path*	Specifies a directory other than `/var/tmp` as the working directory for the installation scripts. This destination is where initial logging is performed and where depots are copied on remote systems before installation.
–uninstall	The `-uninstall` option is used to uninstall products from systems.
–upgrade	Specifies that an existing version of the product exists and you plan to upgrade it.
–version	Checks and reports the installed products and their versions. Identifies the installed and missing depots and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing depots and patches where applicable.

Appendix C

SF Oracle RAC installation and configuration sample values

This appendix includes the following topics:

- About the installation and configuration worksheets
- SF Oracle RAC worksheet
- Oracle RAC worksheet
- Replicated cluster using VVR worksheet
- Replicated cluster using SRDF worksheet
- Required installation information for Oracle Clusterware/Grid Infrastructure
- Required installation information for Oracle database

About the installation and configuration worksheets

The installation programs prompt you for information during the installation and configuration of SF Oracle RAC and Oracle RAC. The installation and configuration worksheets provide sample values that you can use as examples of the information required when you run the Veritas installation programs or the Oracle Universal Installer.

Symantec recommends using the worksheets to record values for your systems before you begin the installation and configuration process.

SF Oracle RAC worksheet

This section provides worksheets for installing and configuring SF Oracle RAC, its component products, and features.

Table C-1 contains the sample values that may be used when you install and configure SF Oracle RAC. Enter the SF Oracle RAC values for your systems in the following table:

Table C-1 SF Oracle RAC worksheet

Installation information	Sample value	Assigned value
Number of nodes in the cluster	2	
Host names for Primary cluster	galaxy and nebula **Note:** Do not use the underscore character in host names. Host names that use the underscore character are not compliant with RFC standards and cause issues.	
Host names for added or removed node	saturn **Note:** Do not use the underscore character in host names. Host names that use the underscore character are not compliant with RFC standards and cause issues.	
License keys	License keys can be one of the following types: ■ Valid license keys for each system in the cluster ■ Valid site license key ■ Valid demo license key If you want to configure global clusters and enable disaster recovery, you must enter appropriate license keys. **Note:** You can choose between SF Oracle RAC and SF Oracle RAC Disaster Recovery and High Availability options for license keys.	

Table C-1 SF Oracle RAC worksheet *(continued)*

Installation information	Sample value	Assigned value
SF Oracle RAC depots to be installed on the cluster	Install only the required depots if you do not want to configure any optional components or features. Default option is to install the recommended depots.	
Primary cluster name	rac_cluster101	
Primary cluster ID number	101	
Private network links	lan1, lan2	
Cluster Manager NIC (Primary NIC)	lan0	
Cluster Manager IP	10.10.12.1, 10.10.12.2	
Netmask for the virtual IP address	255.255.240.0	
VCS user name (not required if you configure your cluster in secure mode)	VCS usernames must not exceed 1024 characters. Example: smith	
VCS user password	VCS passwords must not exceed 512 characters.	
VCS user privileges	Users have three levels of privileges: A=Administrator, O=Operator, or G=Guest. Example: A	
Domain-based address of SMTP server	smtp.symantecexample.com	
Email address of SMTP notification recipients	admin@symantecexample.com	

Table C-1 SF Oracle RAC worksheet *(continued)*

Installation information	Sample value	Assigned value
Minimum severity of events for SMTP email notification	Events have four levels of severity: ■ I=Information ■ W=Warning ■ E=Error ■ S=SevereError Example: I The severity levels are defined as follows: ■ 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	
SNMP trap daemon port number the console	162	
System name for the SNMP console	system2	
Minimum severity of events for SNMP trap notification	Events have four levels of severity: ■ I=Information ■ W=Warning ■ E=Error ■ S=SevereError Example: I The severity levels are defined as follows: ■ 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	

Table C-1 SF Oracle RAC worksheet *(continued)*

Installation information	Sample value	Assigned value
Vxfen disks These values are required if SCSI-3 disks are used as coordination points for your configuration.	disk01, disk02, disk03	
Vxfen disk group	vxfencoordg	

Veritas Cluster Server component information

Table C-2 displays the information that is required to configure the Veritas Cluster Server component.

Table C-2 Veritas Cluster Server component information

Information	Example	Assigned values
Name of the cluster	The name must begin with a letter of the alphabet (a-z, A-Z) and contain only the characters a through z, A through Z, and 1 through 0, hyphen (-), and underscore (_). Example: rac_cluster101	
Unique ID number for the cluster	Number in the range of 0-65535. Within the site that contains the cluster, each cluster must have a unique ID. Example: 101	

Table C-2 Veritas Cluster Server component information *(continued)*

Information	Example	Assigned values
Device names of the NICs used by the private networks among systems	You can choose a network interface card that is not part of any aggregated interface, or you can choose an aggregated interface. The interface names that are associated with each NIC for each network link must be the same on all nodes. For example: ■ lan1 ■ lan2 Do not use the network interface card that is used for the public network, which is typically lan0.	

I/O fencing information

Table C-3 displays the information that is required to configure I/O fencing.

Table C-3 I/O fencing information

Information	Sample values	Assigned values
The name of three disks that form the coordinator disk group.	The following are examples of disk names: ■ c1t1d0 ■ c2t1d0 ■ c3t1d0	
The names for each disk in the coordinator disk group (if using DMP).	The following are examples: ■ /dev/vx/dmp/c1t1d0 ■ /dev/vx/dmp/c2t1d0 ■ /dev/vx/dmp/c3t1d0	

Cluster Volume Manager information

Table C-4 displays the information that is required to configure the Cluster Volume Manager.

Table C-4 Cluster Volume Manager information

Information	Examples	Assigned values
Do you want to configure enclosure-based naming scheme?	Enter Yes to configure an enclosure-based naming scheme. Enter No to not configure an enclosure-based naming scheme. **Note:** Dynamic Multipathing (DMP) is a prerequisite for enclosure-based naming schemes	

SF Oracle RAC secure mode cluster information

Table C-5 displays the information that is required to configure SF Oracle RAC clusters in secure mode.

Note: Configuring SF Oracle RAC in secure mode is optional.

Table C-5 SF Oracle RAC secure mode cluster information

Information	Examples	Assigned values
Which mode do you want to choose to configure Authentication Service?	Select one of the three modes: ■ Automatic mode ■ Semiautomatic mode using encrypted files ■ Semiautomatic mode without using encrypted files Default option is automatic mode.	

Table C-5 SF Oracle RAC secure mode cluster information *(continued)*

Information	Examples	Assigned values
Host name of the Symantec Product Authentication Service Root Broker System	Example: venus	

SF Oracle RAC add user information

Table C-6 displays the information that is required to add VCS users. If you configure SF Oracle RAC cluster in secure mode, you need to add VCS users.

Note: Adding VCS users is optional.

Table C-6 SF Oracle RAC add user information

Information	Examples	Assigned values
User name	smith	
User password	*****	
User privilege	Users have three levels of privileges: ■ A=Administrator ■ O=Operator ■ G=Guest Example: `A` VCS privilege levels include: ■ 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.	

Global cluster information

Table C-7 displays the information that is required to configure global clusters.

Note: Global clusters are an optional feature that requires a license.

Table C-7 Global cluster information

Information	Example	Assigned values
Name of the public NIC	You must specify appropriate values for the NIC when you are prompted. Example: `lan0`	
Virtual IP address of the NIC	You must specify appropriate values for the virtual IP address when you are prompted. Example: `10.10.12.1`	
Netmask for the virtual IP address	You must specify appropriate values for the netmask when you are prompted. Example: `255.255.255.0`	
NetworkHosts IP addresses	You must specify appropriate values for the NetworkHosts IP address when you are prompted. Example: `10.10.12.2`	

Veritas Volume Replicator information

Table C-8 displays the information that is required to configure Veritas Volume Replicator (VVR).

Note: Configuring Veritas Volume Replicator is optional. Veritas Volume Replicator is an advanced option. Users are prompted for this configuration information only if they have entered a VVR license.

Table C-8 Veritas Volume Replicator information

Information	Examples	Assigned values
Frequency of VVR statistics collection.	Enter a number to represent the frequency in seconds. Default is 10 seconds.	
Number of days to preserve the collected statistics.	Enter a number to represent the number of days. Default is 3 days.	

For additional Veritas Volume Replicator information, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

Oracle RAC worksheet

This section provides a worksheet with sample values for installing and configuring Oracle RAC.

Table C-9 displays examples of information required for Oracle RAC.

Table C-9 Required information for Oracle RAC

Information	Sample value	Assigned value
Oracle user name	oracle	
Grid user name (For Oracle RAC 11g Release 2)	grid	
Oracle user ID	1000	
Oracle group name	For inventory group as primary group: oinstall Default is oinstall. For dba group as secondary group: dba Default is dba. **Note:** You can have an optional secondary group "oper". Review your Oracle guide for details about this group.	

Table C-9 Required information for Oracle RAC *(continued)*

Information	Sample value	Assigned value
Oracle group ID	For inventory group as primary group: 1000 For dba group as secondary group: 1001	
Oracle user home directory	/home/oracle	
Grid user home directory	/home/grid	
DISPLAY environment variable value	10.20.12.150:0.0 **Note:** You can provide the host name or IP address of the system that you want to use to display the Oracle installer.	
VCS resource name for PrivNIC	ora_priv	
Private IP addresses for each node	■ On galaxy: 192.168.12.1 ■ On nebula: 192.168.12.2 **Note:** The IP addresses must not contain leading zeroes in any of the octets that comprise the address for example 0X.X.X.X or X0X.X.X, or X.X.0X.X, or X.X.X.0X. Make sure that the private IP addresses have a format as displayed in the above examples for galaxy and nebula.	
Private hostnames (set in /etc/hosts)	galaxy-priv, nebula-priv	

Table C-9 Required information for Oracle RAC *(continued)*

Information	Sample value	Assigned value
NIC address for network on each node	You have to choose an LLT device as a device for the Oracle Clusterware heartbeat. The interfaces specified should be exactly the same in name and total number as those which have been used for LLT configuration. For example, if the LLT devices are lan1, lan2: ■ On galaxy: lan1, lan2 ■ On nebula: lan1, lan2 Then the PrivNIC or MultiPrivNIC device names will be as follows: ■ Device@galaxy= { lan1 = 0, lan2 = 1 } ■ Device@nebula= { lan1 = 0, lan2 = 1 } If aggregated device names are configured under LLT, then the aggregated names must be used in PrivNIC or MultiPrivNIC agent. **Note:** If you configured aggregated interfaces for LLT, then you must set the Device attribute value to use the same aggregated interface names that you configured for LLT. For example, if LLT device names are: ■ On galaxy: aggr1 ■ On nebula: aggr1 Then the Device Attribute for the MultiPrivNIC agent would be as follows: ■ Device@galaxy = { aggr1 = 0 } ■ Device@nebula = { aggr1 = 0 }	
VCS resource name for MultiPrivNIC	multi_priv	

Table C-9 Required information for Oracle RAC *(continued)*

Information	Sample value	Assigned value
Private IP addresses for each node (MultiPrivNIC)	On galaxy: ■ 192.168.12.1 (Oracle Clusterware) ■ 192.168.2.1 (UDP to use for the CLUSTER_INTERCONNECT parameter) ■ 192.168.3.1 (Second UDP to use for the CLUSTER_INTERCONNECT parameter) On nebula: ■ 192.168.12.2 (Oracle Clusterware) ■ 192.168.2.2 (UDP to use for the CLUSTER_INTERCONNECT parameter) ■ 192.168.3.2 (Second UDP to use for the CLUSTER_INTERCONNECT parameter) **Note:** The IP addresses must not contain leading zeroes in any of the octets that comprise the address for example 0X.X.X.X or X.0X.X.X, or X.X.0X.X, or X.X.X.0X. Make sure that the private IP addresses have a format as displayed in the above examples for galaxy and nebula. Symantec recommends that all Oracle Clusterware and UDP cache-fusion links be LLT links. To avoid routing issues, ensure that the private IP addresses assigned to the first NIC (Clusterware and UDP 1) are using the same subnet. Additionally, ensure that the third IP address (UDP 2) for the second NIC is on a different subnet than the first NIC.	

Table C-9 Required information for Oracle RAC *(continued)*

Information	Sample value	Assigned value
Private hostnames (set in /etc/hosts)	On galaxy: ■ galaxy-priv ■ galaxy-priv1 On nebula: ■ nebula-priv ■ nebula-priv1	
Netmask for cluster	255.255.255.0	
Disk for each node that contains the Oracle Clusterware and database binaries	Disk_1	
VxVM disk group	■ On galaxy: bindg_galaxy ■ On nebula: bindg_nebula	
Volume for each local disk group	■ On galaxy: crsbinvol ■ On nebula: orabinvol	

File system on each local volume	■ On galaxy:
	`/dev/vx/rdsk/\`
	`bindg_galaxy/crsbinvol`
	`/dev/vx/rdsk/\`
	`bindg_galaxy/orabinvol`
	■ On nebula:
	`/dev/vx/rdsk/\`
	`bindg_nebula/crsbinvol`
	`/dev/vx/rdsk/\`
	`bindg_nebula/orabinvol`	

Oracle base directory (ORACLE_BASE)	■ Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: /u01/app/oracle ■ Oracle RAC 11g Release 2: /u01/app/gridbase	

Table C-9 Required information for Oracle RAC *(continued)*

Information	Sample value	Assigned value
Oracle home directory (ORACLE_HOME)	/u01/app/oracle/product/*release*/dbhome_1 where *release* is 10.2.0, 11.1.0, or 11.2.0 depending on the Oracle RAC version	
Oracle Clusterware home directory (CRS_HOME)	/u01/app/oracle/product/10.2.0/crshome	
Grid home directory (GRID_HOME)	/u01/app/grid/product/11.2.0/gridhome	
File system mount point (VxFS)	■ Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: /u01/app/oracle (for crsbinvol and orabinvol) ■ Oracle RAC 11g Release 2: /u01/app/grid (crsbinvol) /u01/app/oracle (orabinvol)	
File system mount point (CFS)	■ Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: /u01/app/oracle/product/10.2.0/crshome (for crsbinvol) /u01/app/oracle/product/10.2.0/dbhome_1 (for orabinvol) ■ Oracle RAC 11g Release 2: /u01/app/grid/product/11.2.0/gridhome (crsbinvol) /u01/app/oracle/product/11.2.0/dbhome_1 (orabinvol)	
Disk group for Oracle Database	oradatadg (Shared)	
Volume for Oracle Database	oradatavol	
Volume options for Oracle Database	layout=striped-mirror	
Mount point for Oracle Database	/oradata (Shared)	
VCS resource names for Oracle Database	oradata_voldg, oradata_mnt	

Table C-9 Required information for Oracle RAC *(continued)*

Information	Sample value	Assigned value
Global Database Name	db.symantecexample.com (database name.domain)	
SID prefix	ora1	
Shared disk group for OCR and voting disk	ocrvotedg	
Volume for shared disk group	■ CVM raw volumes OCR: ocrvol Voting disk: votevol ■ CFS ocrvotevol	
Volume options for OCR and voting disk	nmirror=2	
File system on shared volume (CFS)	/dev/vx/rdsk/ocrvotedg/ocrvotevol	
Mount point for shared file system	/ocrvote	
VCS resource names for Votedisk and OCR	ocrvote_voldg_ocrvotedg ocrvote_mnt_ocrvotedg	
Mount point for archive logs	/oradata	

Replicated cluster using VVR worksheet

Table C-10 contains the sample values that may be used when you install and configure CVM and VVR. If applicable, enter the CVM/VVR values for your systems in the following table:

Table C-10 Replicated cluster using VVR worksheet

Installation information	Sample value	Assigned value
Host names for Secondary Cluster	mercury, jupiter	
Secondary Cluster Name	rac_cluster102	

Table C-10 Replicated cluster using VVR worksheet *(continued)*

Installation information	Sample value	Assigned value
Secondary cluster ID number	102	
Primary Cluster Address	10.10.10.101	
Primary Cluster Logowner IP	10.10.9.101	
Secondary Cluster Address	10.11.10.102	
Secondary Cluster Logowner IP	10.11.9.102	
RVG Name	rac1_rvg	
Global Database Name	vrts	
Database Resource Name	ora1	
Database Group Name (depends on cvm, includes resources oracle agent etc.)	oradb1_grp	
Srl Volume Name	rac1_srl	
Resolvable Virtual Hostname of the cluster on Primary Site (for VVR)	rac_clus101_priv	
Resolvable Virtual Hostname of the cluster on Secondary Site (for VVR)	rac_clus102_priv	
Private IP addresses for Secondary Cluster	192.168.12.3 - 192.168.12.4	

Replicated cluster using SRDF worksheet

Table C-11 contains the sample values that may be used when you install and configure CVM and VVR. If applicable, enter the CVM/VVR values for your systems in the following table:

Table C-11 Replicated cluster using SRDF worksheet

Installation information	Sample value	Assigned value
Host names for Secondary Cluster	mercury, jupiter	
Secondary Cluster Name	rac_cluster102	
Secondary cluster ID number	102	
Primary Cluster Address	10.10.10.101	
Primary Cluster Logowner IP	10.10.9.101	
Secondary Cluster Address	10.11.10.102	
Secondary Cluster Logowner IP	10.11.9.102	
RVG Name	rac1_rvg	
Global Database Name	vrts	
Database Resource Name	ora1	
Database Group Name (depends on cvm, includes resources oracle agent etc.)	oradb1_grp	
Srl Volume Name	rac1_srl	
Resolvable Virtual Hostname of the cluster on Primary Site (for VVR)	rac_clus101_priv	
Resolvable Virtual Hostname of the cluster on Secondary Site (for VVR)	rac_clus102_priv	
Private IP addresses for Secondary Cluster	192.168.12.3 - 192.168.12.4	

Required installation information for Oracle Clusterware/Grid Infrastructure

This section describes the information required by the Oracle Universal Installer for installing the Oracle Clusterware/Grid Infrastructure software.

Table C-12 lists the information required by the Oracle Universal Installer when you install Oracle Clusterware.

Table C-12 Required installation information for Oracle Clusterware - Oracle RAC 10g Release 2/Oracle RAC 11g Release 1

OUI menu	Description
Specify Inventory Details and Credentials	Enter the full path of the inventory directory and the operating system group name. **Note:** Retain the directory paths and operating system group name suggested by the installer. Changing the information results in failure of certain post-verification tasks.
Specify Home Details	Enter the path to the CRS home directory. The Oracle Universal Installer performs product-specific prerequisite checks and verifies that your environment meets all of the minimum requirements for installing Oracle RAC. You must manually verify and confirm the items that are flagged with warnings and items that require manual checks. The OUI displays the full path of the oraInventory logs. Make a note of the log file path to verify the installation at a later time.
Specify cluster configuration	Verify the cluster name and the nodes to be managed by Oracle Clusterware.

Table C-12 Required installation information for Oracle Clusterware - Oracle RAC 10g Release 2/Oracle RAC 11g Release 1 *(continued)*

OUI menu	Description
Specify network interface usage	Identify the planned use for each interface: Public, Private, or Do Not use. **Note:** Make sure that the same private interfaces that you specified at the time of configuring PrivNIC and MultiPrivNIC are listed on the screen. **Note:** Mark the interfaces for the subnet containing the private IP addresses managed by the PrivNIC/MultiPrivNIC agents as 'Private'. The interfaces that are **Private** are stored in OCR as a 'cluster_interconnect' for database cache fusion traffic. Oracle recommends the use of a common private interface for both Oracle Clusterware and Oracle RAC database.
Specify Oracle Cluster Registry (OCR) information	Enter the full path of the location where you want to store the OCR information. For example, if you are storing the OCR information on CFS, enter: `/ocrvote/ocr`. **Note:** Store the OCR information at the root of the file system. If you place the OCR information under a directory on CFS, the configuration of the CSSD agent after Oracle RAC installation fails. If you are storing the OCR information on raw volumes, enter: `/dev/vx/rdsk/ocrvotedg/ocrvol` **Note:** Select the option **External Redundancy**. OCR mirroring is performed by CVM.

Table C-12 Required installation information for Oracle Clusterware - Oracle RAC 10g Release 2/Oracle RAC 11g Release 1 *(continued)*

OUI menu	Description
Specify voting disk location	Enter the full path of the location where you want to store the voting disk information. For example, if you are storing the voting disk information on CFS, enter: `/ocrvote/vote` **Note:** Store the voting disk information at the root of the file system. If you place the voting disk information under a directory on CFS, the configuration of the CSSD agent after Oracle RAC installation fails. If you are storing the voting disk information on raw volumes, enter: `/dev/vx/rdsk/ocrvotedg/votevol` **Note:** Select the option **External Redundancy**. Voting disk redundancy is provided by CVM.

Table C-13 lists the information required by the Oracle Universal Installer when you install Oracle Grid Infrastructure.

Table C-13 Required installation information for Oracle Grid Infrastructure - Oracle RAC 11g Release 2

OUI menu	Description
Select installation option	Select the option **Install and Configure Grid Infrastructure for a Cluster**.
Select installation type	Select the option **Advanced Installation**.
Specify cluster configuration	Enter the SCAN name for the cluster that will be used by the database clients to connect to databases within the cluster.
Grid Plug and Play information	Provide the following information: ■ Name of the cluster ■ SCAN name The SCAN address on the domain name server (DNS) must resolve to three addresses (recommended) or at least one address. ■ SCAN port

Table C-13 Required installation information for Oracle Grid Infrastructure - Oracle RAC 11g Release 2 *(continued)*

OUI menu	Description
Specify network interface usage	Identify the planned use for each interface: Public, Private, or Do Not use. **Note:** Make sure that the same private interfaces that you specified at the time of configuring PrivNIC and MultiPrivNIC are listed on the screen. **Note:** Mark the interfaces for the subnet containing the private IP addresses managed by the PrivNIC/MultiPrivNIC agents as 'Private'. The interfaces that are **Private** are stored in GPnP profile as a 'cluster_interconnect' for Oracle Grid Infrastructure communication and database cache fusion traffic.
Storage option information	Select the option **Shared File System**.
OCR storage option	Enter the full path of the location where you want to store the OCR information. For example, if you are storing the OCR information on CFS, enter: `/ocrvote/ocr`. **Note:** Select the option **External Redundancy** when you install Oracle Clusterware/Grid Infrastructure. Mirroring is performed by CVM. If you are storing the OCR information on an ASM disk group that uses CVM raw volumes, enter: `/dev/vx/rdsk/ocrvotedg/ocrvol` **Note:** Select the option **External** when you create the ASM disk group and instances. Mirroring is performed by CVM.

Table C-13 Required installation information for Oracle Grid Infrastructure - Oracle RAC 11g Release 2 *(continued)*

OUI menu	Description
Voting Disk storage option	Enter the full path of the location where you want to store the voting disk information. For example, if you are storing the voting disk information on CFS, enter: `/ocrvote/vote` **Note:** Select the option **External Redundancy** when you install Oracle Clusterware/Grid Infrastructure. Mirroring is performed by CVM. If you are storing the voting disk information on an ASM disk group that uses CVM raw volumes, enter: `/dev/vx/rdsk/ocrvotedg/votevol` **Note:** Select the option **External** when you create the ASM disk group and instances. Mirroring is performed by CVM.
Specify installation location	Enter the full path to the Oracle base directory and the Oracle Grid Infrastructure home directory.
Create inventory	Enter the full path to the Oracle inventory directory where you want to store the installation files.

Required installation information for Oracle database

This section describes the information required by the Oracle Universal Installer for installing the Oracle Clusterware/Grid Infrastructure software.

Table C-14 lists the information required by the Oracle Universal Installer when you install Oracle database software.

Table C-14 Required installation information for Oracle database - Oracle RAC 10g Release 2/Oracle RAC 11g Release 1

OUI menu	Description
Select installation type	Select **Enterprise Edition**.
Specify home details	Review or enter the ORACLE_HOME and ORACLE_BASE directory paths.

Table C-14 Required installation information for Oracle database - Oracle RAC 10g Release 2/Oracle RAC 11g Release 1 *(continued)*

OUI menu	Description
Specify Hardware Cluster Installation Mode	Select **Cluster Installation**. Select the nodes on which you want to install the Oracle RAC database software. The Oracle Universal Installer runs a product-specific prerequisite check. Any items that are flagged must be manually checked and configured. The OUI displays the full path of the oraInventory logs. Make a note of the log file path to verify the installation at a later time.
Select Configuration Option	Select the option **Install database software only**. **Note:** Do not select the option **Create a database**. Symantec recommends that you create the database later.

Table C-15 lists the information required by the Oracle Universal Installer when you install Oracle database software.

Table C-15 Required installation information for Oracle database - Oracle RAC 11g Release 2

OUI menu	Description
Select installation option	Select the option **Install database software only**.
Node selection	Select **Real Application Clusters database installation**. Select the nodes on which the Oracle RAC database software must be installed.
Select database edition	Select **Enterprise Edition**.
Specify installation location	Review or enter the ORACLE_BASE and ORACLE_HOME directory paths. The Oracle Universal Installer runs product-specific prerequisite checks. Any items that are flagged must be manually checked and configured.

Appendix D

Sample configuration files

This appendix includes the following topics:

- About VCS configuration file
- About the LLT and GAB configuration files
- About I/O fencing configuration files
- Sample configuration files

About VCS configuration file

This section provides a high-level overview of the contents of the VCS configuration file after the SF Oracle RAC installation. Review the configuration file after the SF Oracle RAC installation and before the Oracle installation.

The configuration file includes the following information:

- The "include" statements list the various VCS types files (`.cf`) for SF Oracle RAC.
  The files are located in the /etc/VRTSvcs/conf/config directory. These files define the agents that control the resources in the cluster.
- The cluster definition, with the cluster name provided during installation (for example, rac_cluster101), includes the names of users and administrators of the cluster. The UseFence = SCSI3 attribute is not automatically present; you must manually add it after the installation.
  See "Setting up disk-based I/O fencing manually" on page 155.
- The main.cf includes the cvm service group. The service group includes definitions for monitoring the CFS and the CVM resources. The CVMCluster agent resource definition indicates that the nodes use GAB for messaging operations.

The cvm group has the Parallel attribute set to 1. This value enables the resources to run in parallel on each node in the system list.

About the LLT and GAB configuration files

Low Latency Transport (LLT) and Group Membership and Atomic Broadcast (GAB) are VCS communication services. LLT requires `/etc/llthosts` and `/etc/llttab` files. GAB requires `/etc/gabtab` file.

Table D-1 lists the LLT configuration files and the information that these files contain.

Table D-1 LLT configuration files

File	Description
/etc/rc.config.d/lltconf	This file stores the start and stop environment variables for LLT: ■ LLT_START—Defines the startup behavior for the LLT module after a system reboot. Valid values include: 1—Indicates that LLT is enabled to start up. 0—Indicates that LLT is disabled to start up. ■ LLT_STOP—Defines the shutdown behavior for the LLT module during a system shutdown. Valid values include: 1—Indicates that LLT is enabled to shut down. 0—Indicates that LLT is disabled to shut down. The installer sets the value of these variables to 1 at the end of SF Oracle RAC configuration.

/etc/llthosts	The file `llthosts` is a database that contains one entry per system. This file links the LLT system ID (in the first column) with the LLT host name. This file must be identical on each node in the cluster. A mismatch of the contents of the file can cause indeterminate behavior in the cluster.
	For example, the file `/etc/llthosts` contains the entries that resemble:
	`0 galaxy`
	`1 nebula`

Table D-1 LLT configuration files *(continued)*

File	Description

/etc/llttab	The file `llttab` contains the information that is derived during installation and used by the utility `lltconfig(1M)`. After installation, this file lists the LLT network links that correspond to the specific system.
	
	For example, the file `/etc/llttab` contains the entries that resemble:
	
	`set-node galaxy`
	`set-cluster 2`
	`link lan1 /dev/lan:1 - ether - -`
	`link lan2 /dev/lan:2 - ether - -`
	
	The first line identifies the system. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines begin with the `link` command. These lines identify the two network cards that the LLT protocol uses.
	
	If you configured a low priority link under LLT, the file also includes a "link-lowpri" line.
	
	Refer to the `llttab(4)` manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the `llttab` file.

Table D-2 lists the GAB configuration files and the information that these files contain.

Table D-2 GAB configuration files

File	Description
/etc/rc.config.d/gabconf	This file stores the start and stop environment variables for GAB: ■ GAB_START—Defines the startup behavior for the GAB module after a system reboot. Valid values include: 1—Indicates that GAB is enabled to start up. 0—Indicates that GAB is disabled to start up. ■ GAB_STOP—Defines the shutdown behavior for the GAB module during a system shutdown. Valid values include: 1—Indicates that GAB is enabled to shut down. 0—Indicates that GAB is disabled to shut down. The installer sets the value of these variables to 1 at the end of SF Oracle RAC configuration.

Table D-2 GAB configuration files *(continued)*

File	Description
/etc/gabtab	After you install SF Oracle RAC, the file /etc/gabtab contains a `gabconfig(1)` command that configures the GAB driver for use. The file `/etc/gabtab` contains a line that resembles: `/sbin/gabconfig -c -nN` The `-c` option configures the driver for use. The `-nN` specifies that the cluster is not formed until at least *N* nodes are ready to form the cluster. Symantec recommends that you set N to be the total number of nodes in the cluster. **Note:** Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`. Using `-c -x` can lead to a split-brain condition.

About I/O fencing configuration files

Table D-3 lists the I/O fencing configuration files.

Table D-3 I/O fencing configuration files

File	Description
/etc/rc.config.d/vxfenconf	This file stores the start and stop environment variables for I/O fencing: ■ VXFEN_START—Defines the startup behavior for the I/O fencing module after a system reboot. Valid values include: 1—Indicates that I/O fencing is enabled to start up. 0—Indicates that I/O fencing is disabled to start up. ■ VXFEN_STOP—Defines the shutdown behavior for the I/O fencing module during a system shutdown. Valid values include: 1—Indicates that I/O fencing is enabled to shut down. 0—Indicates that I/O fencing is disabled to shut down. The installer sets the value of these variables to 1 at the end of SF Oracle RAC configuration.
/etc/vxfendg	This file includes the coordinator disk group information. This file is not applicable for server-based fencing.

Table D-3 I/O fencing configuration files *(continued)*

File	Description
/etc/vxfenmode	This file contains the following parameters: ■ vxfen_mode ■ scsi3—For disk-based fencing ■ customized—For server-based fencing ■ disabled—To run the I/O fencing driver but not do any fencing operations. ■ vxfen_mechanism This parameter is applicable only for server-based fencing. Set the value as cps. ■ scsi3_disk_policy You must configure the vxfen module to use DMP devices or iSCSI devices, and set the SCSI-3 disk policy as dmp. ■ security This parameter is applicable only for server-based fencing. 1—Indicates that Symantec Product Authentication Service is used for CP server communications. This setting is the default. 0—Indicates that communication with the CP server is in non-secure mode. **Note:** The CP server and the SF Oracle RAC clusters must have the same security setting. ■ List of coordination points This list is required only for server-based fencing configuration. Coordination points in a server-based fencing can include coordinator disks, CP servers, or a mix of both. If you use coordinator disks, you must create a coordinator disk group with the coordinator disk names. Refer to the sample file /etc/vxfen.d/vxfenmode_cps for more information on how to specify the coordination points. ■ single_cp This parameter is applicable only for server-based fencing which uses a single highly available CP server as its coordination point.

Table D-3 I/O fencing configuration files *(continued)*

File	Description

/etc/vxfentab	When I/O fencing starts, the vxfen startup script creates this `/etc/vxfentab` file on each node. The startup script uses the contents of the `/etc/vxfendg` and `/etc/vxfenmode` files. Any time a system is rebooted, the fencing driver reinitializes the `vxfentab` file with the current list of all the coordinator points.
	Note: The `/etc/vxfentab` file is a generated file; do not modify this file.
	An example of the /etc/vxfentab file in a disk-based fencing configuration on one node resembles as follows:
	`/dev/vx/rdmp/c1t1d0`
	`/dev/vx/rdmp/c2t1d0`
	`/dev/vx/rdmp/c3t1d0`
	For server-based fencing, the `/etc/vxfentab` file also includes the security settings information.
	For server-based fencing with single CP server, the `/etc/vxfentab` file also includes the single_cp settings information.

Sample configuration files

SF Oracle RAC provides several sample configuration files illustrating various scenarios. You may use the sample files as a guideline for setting up your cluster environment. These sample files are located at `/etc/VRTSvcs/conf/sample_rac/`.

This section briefly describes each of the sample files and illustrates the service group configuration for each of them. The section does not include a copy of the main.cf files.

The following sample files are discussed in this section:

- sfrac01_main.cf file
- sfrac02_main.cf file
- sfrac03_main.cf file
- sfrac04_main.cf file
- sfrac05_main.cf file
- sfrac06_main.cf file
- sfrac07_main.cf and sample08_main.cf files
- sfrac09_main.cf and sample10_main.cf files

- sfrac11_main.cf file
- sfrac12_main.cf and sample13_main.cf files
- sfrac14_main.cf file

sfrac01_main.cf file

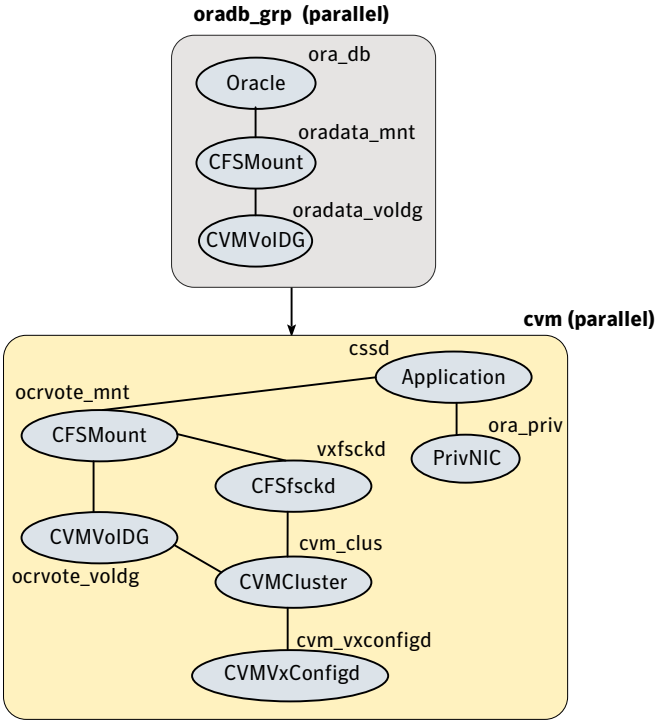
The sample configuration is applicable only for Oracle RAC 10g installations.

This sample file describes the following configuration:

- A two node SF Oracle RAC cluster hosting single database.
- The Oracle database is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the VCSIPC for database cache fusion.
- Only one private IP address is configured for Oracle Clusterware. The private IP address is managed by the PrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.

Figure D-1 illustrates the configuration.

Figure D-1 Service group configuration for sfrac01_main.cf file



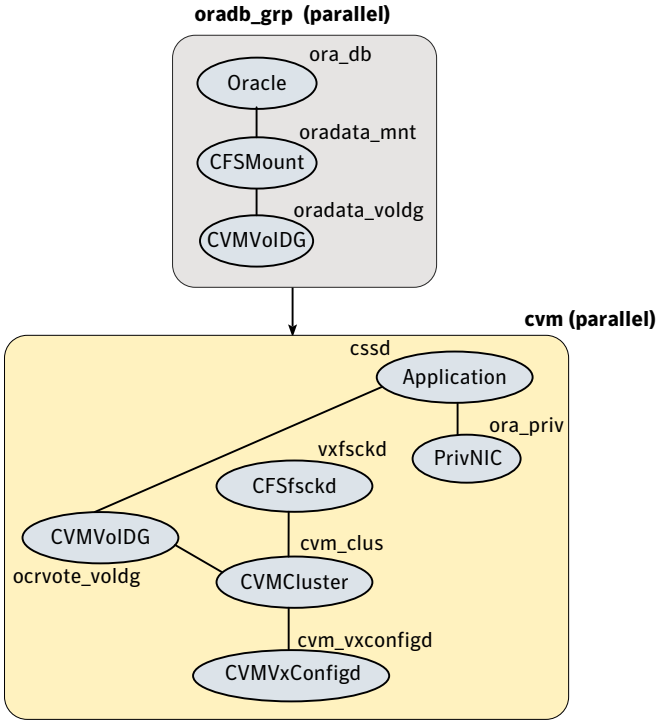
sfrac02_main.cf file

This sample file describes the following configuration:

- A two node SF Oracle RAC cluster hosting single database.
- The Oracle database is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the Oracle UDP IPC for database cache fusion.
- A common IP address is used by Oracle Clusterware and database cache fusion.
  The private IP address is managed by the PrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CVM raw volumes.

Figure D-2 illustrates the configuration.

Figure D-2 Service group configuration for sfrac02_main.cf file



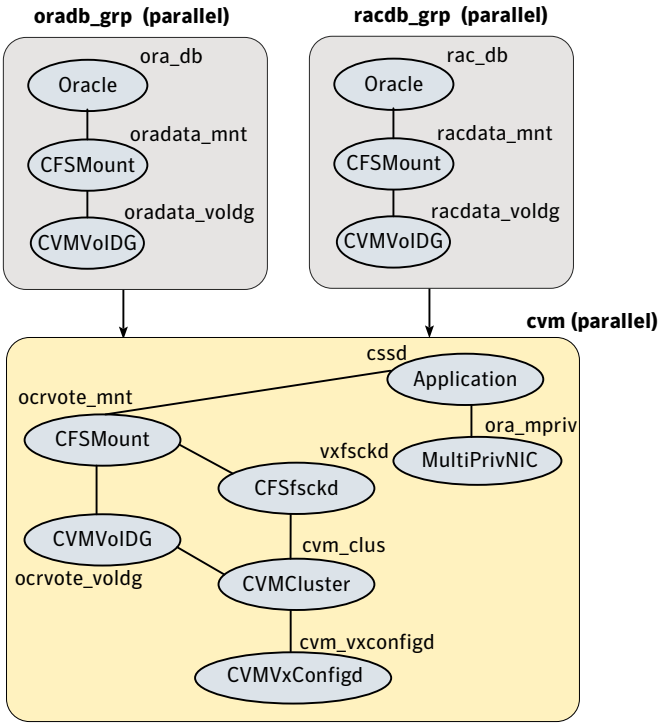
sfrac03_main.cf file

This sample file describes the following configuration:

- A two node SF Oracle RAC cluster hosting two databases.
- The Oracle database is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the Oracle UDP IPC for database cache fusion.
- One IP address (on lan1) is shared by Oracle Clusterware and one of the databases for cache fusion.
  The second IP address (on lan2) is used by the second database for cache fusion.
  The private IP addresses are managed by the MultiPrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.

Figure D-3 illustrates the configuration.

Figure D-3 Service group configuration for sfrac03_main.cf file



sfrac04_main.cf file

This sample file describes the following configuration:

- A two node SF Oracle RAC cluster hosting two databases.
- The Oracle database is stored on CFS.
- Database is not managed by VCS. Oracle Clusterware starts, stops, and monitors the databases.
  The CRSResource agent monitors the status of the database, the VIP resource, and the listener resource configured under Oracle Clusterware.

Note: The CFSMount and CVMVolDg resources for Oracle database can not be set as critical resources in the group.

The CRSResource agent appears FAULTED until Oracle Clusterware brings up the database.

- The database uses the Oracle UDP IPC for database cache fusion.
- One IP address (on lan1) is shared by Oracle Clusterware and one of the databases for cache fusion.
  The second IP address (on lan2) is used by the second database for cache fusion.
  The private IP addresses are managed by the MultiPrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.

Figure D-4 illustrates the configuration.

Figure D-4 Service group configuration for sfrac04_main.cf file

sfrac05_main.cf file

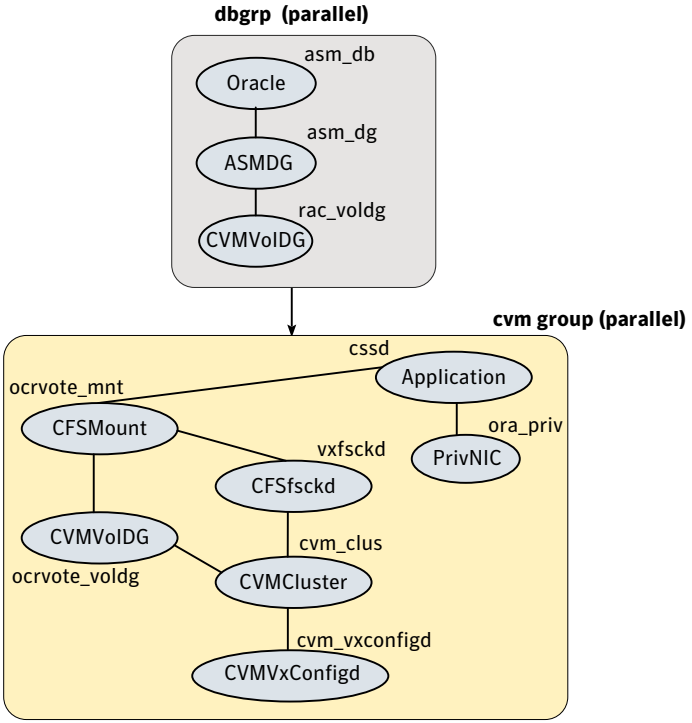
This sample file describes the following configuration:

- A two node SF Oracle RAC cluster hosting single database.
- The Oracle database is stored on ASM.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the Oracle UDP IPC for database cache fusion.

- A common IP address is used by Oracle Clusterware and database cache fusion. The private IP address is managed by the PrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.

Figure D-5 illustrates the configuration.

Figure D-5 Service group configuration for sfrac05_main.cf file



sfrac06_main.cf file

This sample file describes the following configuration:

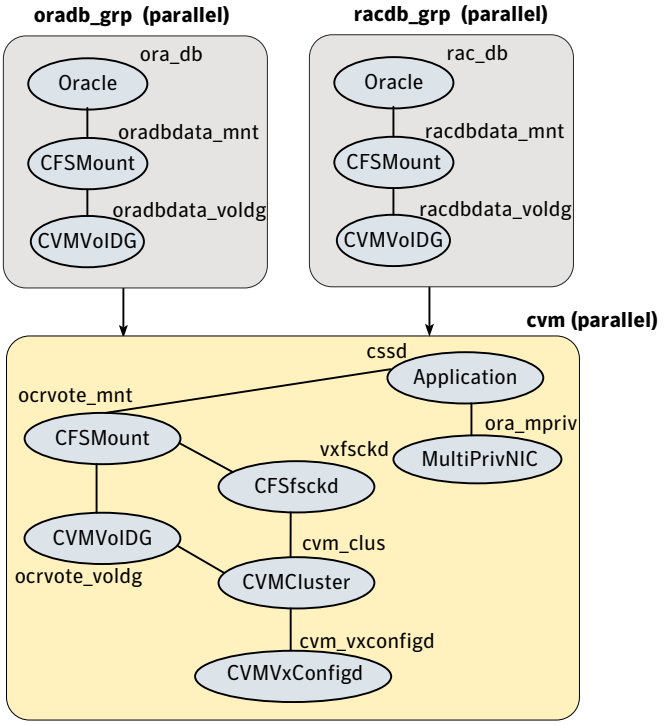
- A two node SF Oracle RAC cluster hosting two databases.
- The Oracle database is stored on CFS.
- The database is managed by the VCS agent for Oracle. The agent starts, stops, and monitors the database.
- The database uses Oracle UDP IPC for cache fusion. A dedicated link is used for each database .
- One private IP address (on lan1) is used by Oracle Clusterware.

The private IP address on lan2 is used by one of the databases for cache fusion. The private IP address on NIC3 is used by the other database for cache fusion. The private IP addresses are managed by the MultiPrivNIC agent for high availability.

- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.

Figure D-6 illustrates the configuration.

Figure D-6 Service group configuration for sfrac06_main.cf file



sfrac07_main.cf and sample08_main.cf files

The sample configuration, sfrac07_main.cf, describes a disaster recovery configuration for the primary site. The sample configuration, sample08_main.cf, describes a disaster recovery configuration for the secondary site. The configuration uses VVR for replicating data between the sites.

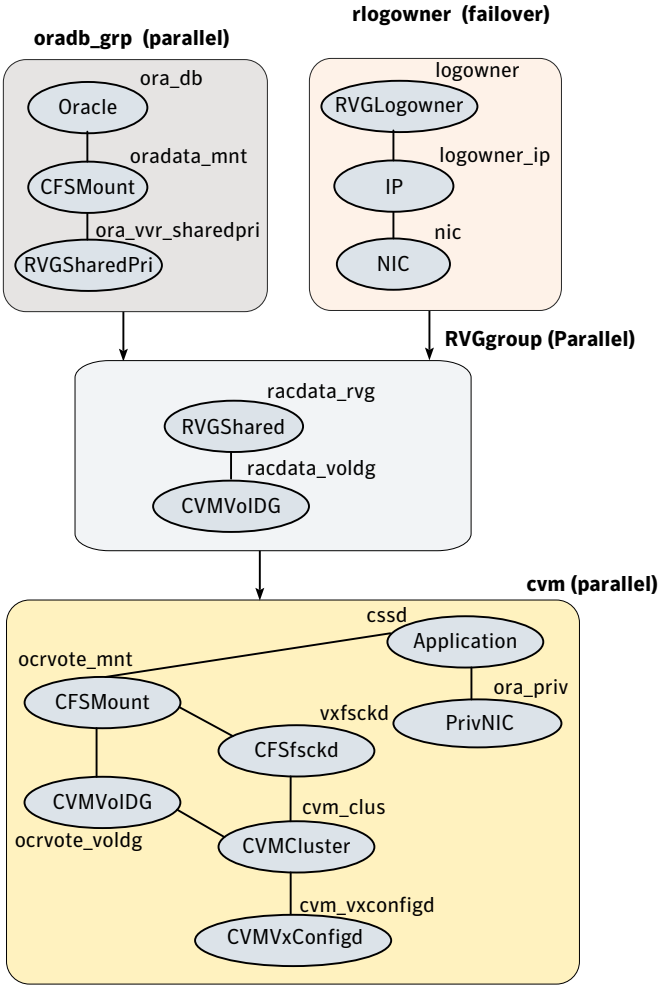
This sample file describes the following configuration:

- Two SF Oracle RAC clusters, comprising two nodes each, hosted at different geographical locations.

- A single Oracle database that is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the Oracle UDP IPC for database cache fusion.
- A common IP address is used by Oracle Clusterware and database cache fusion.
  The private IP address is managed by the PrivNIC agent for high availability.
- One virtual IP address must be configured under the `ClusterService` group on each site for inter-cluster communication.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.
- Veritas Volume Replicator (VVR) is used to replicate data between the sites.
- The shared volumes replicated across the sites are configured under the RVG group.
- The replication link used by VVR for communicating log information between sites are configured under the `rlogowner` group. This is a failover group that will be online on only one of the nodes in the cluster at each site.
- The database group will be online on the primary cluster. The RVGSharedPri resource determines where the database group will be brought online.
- The database group is configured as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.

Figure D-7 illustrates the configuration. The service group configuration is the same on the primary and secondary site. The availability of groups (online/offline) differ between the sites.

Figure D-7 Service group configuration for sfrac07_main.cf and sfrac08_main.cf files



sfrac09_main.cf and sample10_main.cf files

The sample configuration, sfrac09_main.cf, describes a disaster recovery configuration for the primary site. The sample configuration, sample10_main.cf, describes a disaster recovery configuration for the secondary site. The sample configuration uses EMC SRDF technology for replicating data between the sites.

Note: You can use other supported hardware-based replication technologies with this configuration.

This sample file describes the following configuration:

- Two SF Oracle RAC clusters, comprising two nodes each, hosted at different geographical locations.
- A single Oracle database that is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the Oracle UDP IPC for database cache fusion.
- A common IP address is used by Oracle Clusterware and database cache fusion. The private IP address is managed by the PrivNIC agent for high availability.
- One virtual IP address must be configured under the `ClusterService` group on each site for inter-cluster communication.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.
- EMC SRDF is used to replicate data between the sites.
- The SRDF disk groups that are replicated across the sites using SRDF technology and the replication mode are specified under the SRDF resource in the database group. The CVM disk group that comprises the SRDF disk group must be configured under the CVMVolDg resource in the database group.
- The database group will be online on the primary cluster. The SRDF resource determines where the database group will be brought online.
- The database group is configured as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.

Figure D-8 illustrates the configuration on the primary site.

Figure D-8 Service group configuration for sfrac09_main.cf file

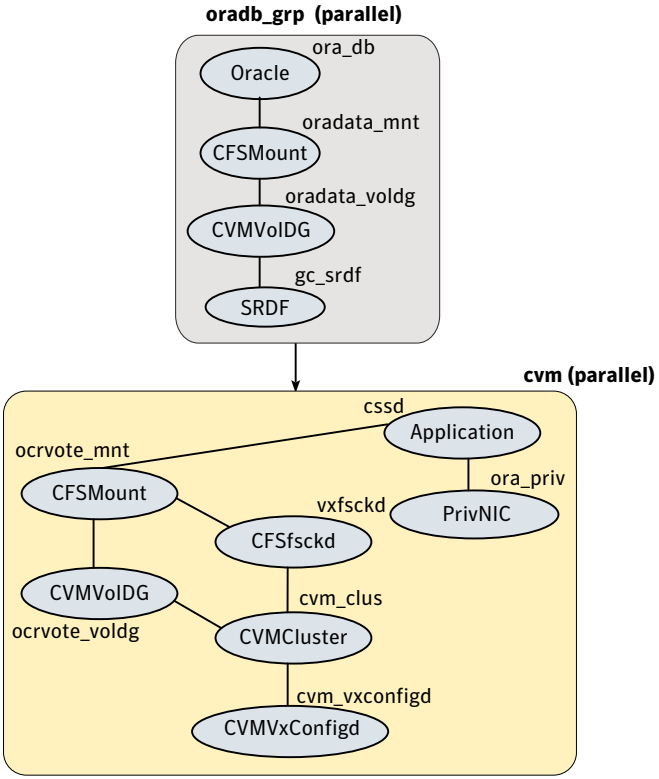
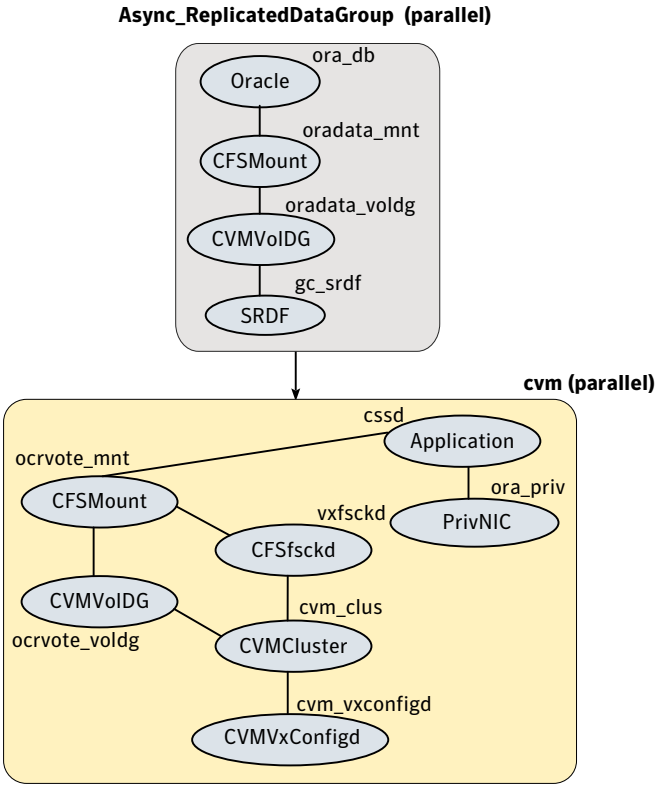


Figure D-9 illustrates the configuration on the secondary site.

Figure D-9 Service group configuration for sfrac10_main.cf file



sfrac11_main.cf file

This sample file describes the following configuration:

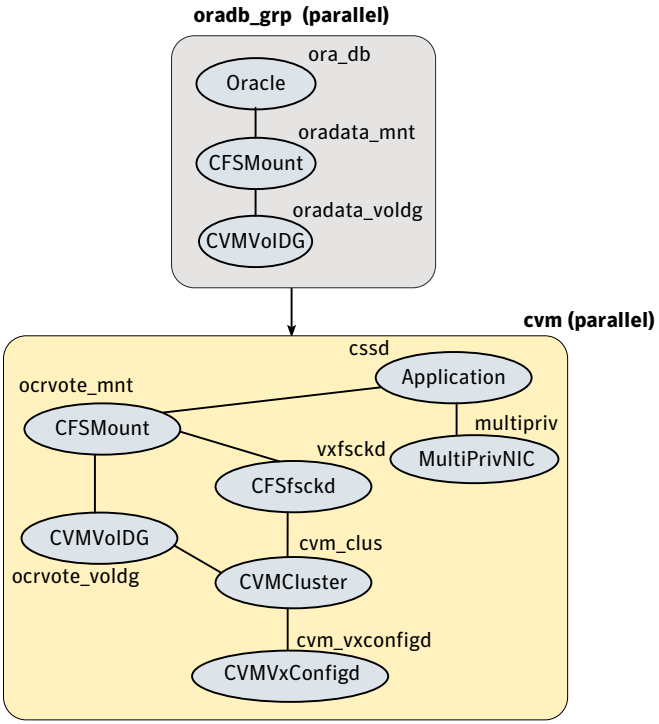
- An SF Oracle RAC campus cluster with four nodes hosted across two sites.
- Each site comprises two nodes of the cluster hosting a single database.
- The Oracle database is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the Oracle UDP IPC for database cache fusion.
- The IP address on lan1 is used by Oracle Clusterware.
  The second IP address on NIC2 is used for Oracle database cache fusion.

The private IP addresses are managed by the MultiPrivNIC agent for high availability.

- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.
- Group the hosts at each physical site into separate logical system zones using the SystemZones attribute.

Figure D-10 illustrates the configuration.

Figure D-10 Service group configuration for sfrac11_main.cf file



sfrac12_main.cf and sample13_main.cf files

The sample configuration, sfrac12_main.cf, describes a disaster recovery configuration for the primary site. The sample configuration, sample13_main.cf, describes a disaster recovery configuration for the secondary site with fire-drill capability. The sample configuration uses Hitachi True Copy technology for replicating data between the sites.

Note: You can use other supported hardware-based replication technologies with this configuration.

This sample file describes the following configuration:

- Two SF Oracle RAC clusters, comprising two nodes each, hosted at different geographical locations.
- A single Oracle database that is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the Oracle UDP IPC for database cache fusion.
- A common IP address is used by Oracle Clusterware and database cache fusion. The private IP address is managed by the PrivNIC agent for high availability.
- One virtual IP address must be configured under the `ClusterService` group on each site for inter-cluster communication.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.
- Hitachi True Copy is used to replicate data between the sites.
- The HTC disk groups that are replicated across the sites using HTC technology and the replication mode are specified under the HTC resource in the database group. The CVM disk group that comprises the HTC disk group must be configured under the CVMVolDg resource in the database group.
- The database group will be online on the primary cluster. The HTC resource determines where the database group will be brought online.
- The database group is configured as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.
- The database group oradb_grp_fd on the secondary is configured for fire drill.
- When the group oradb_grp_fd is brought online, the HTCSnap creates a snapshot of the disk group configured under the HTC resource in the database group oradg_grp.
  Further, the Oracle database and the associated volumes and mount points configured under the service group oradb_grp_fd are brought online using the snapshots created by HTCSnap.

Figure D-11 illustrates the configuration on the primary site.

Figure D-11 Service group configuration for sfrac12_main.cf file

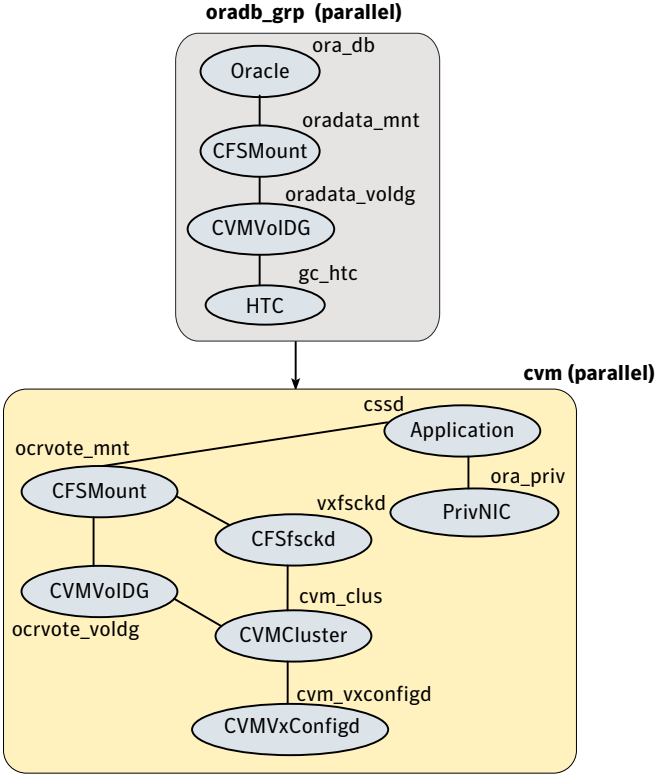
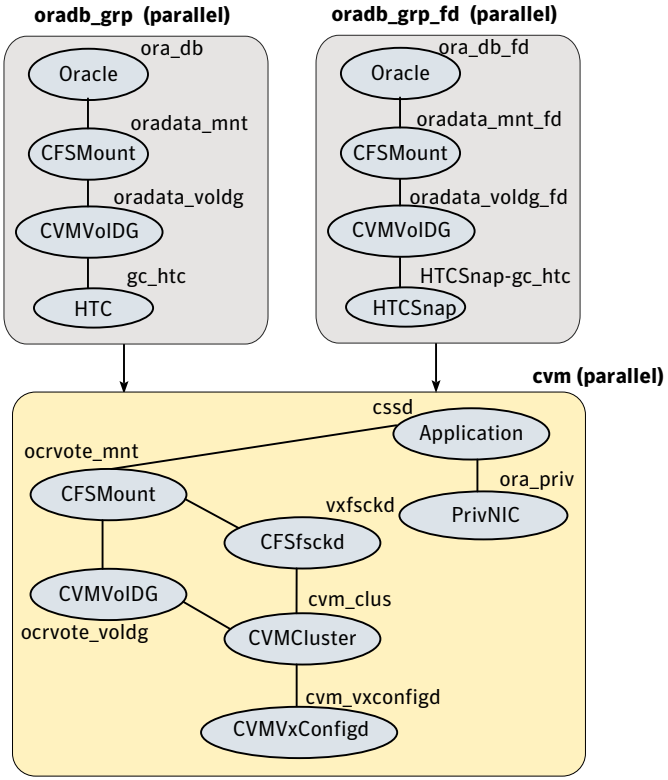


Figure D-12 illustrates the configuration on the secondary site.

Figure D-12 Service group configuration for sfrac13_main.cf file



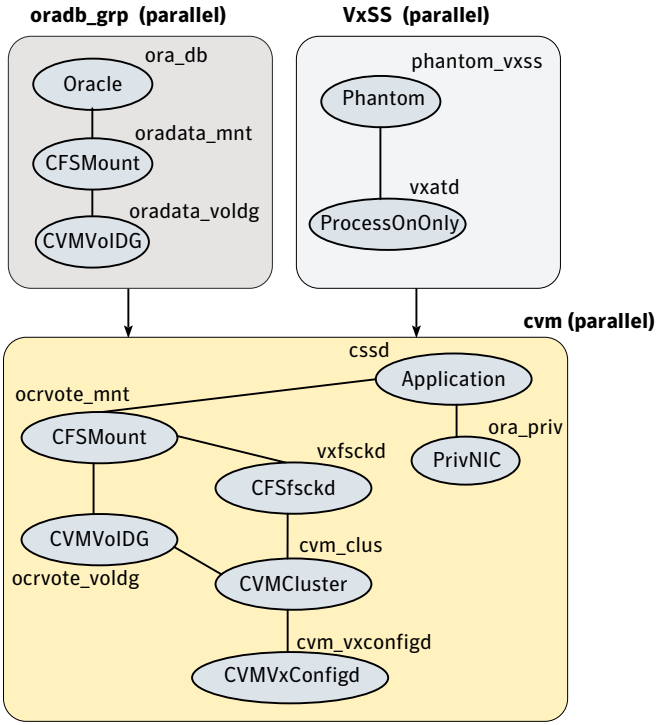
sfrac14_main.cf file

This sample file describes the following configuration:

- A two node SF Oracle RAC cluster hosting single database.
- The Oracle database is stored on CFS.
- The database is managed by the VCS agent for Oracle.
  The agent starts, stops, and monitors the database.
- The database uses the Oracle UDP IPC for database cache fusion.
- A common IP address is used by Oracle Clusterware and database cache fusion.
  The private IP address is managed by the PrivNIC agent for high availability.
- The Oracle Cluster Registry (OCR) and voting disk are stored on CFS.
- The cluster is configured as a secure cluster by setting the SecureClus attribute to 1. The VxSS group starts the authentication daemon vxatd.

Figure D-13 illustrates the configuration.

Figure D-13 Service group configuration for sfrac14_main.cf file



Sample configuration files for CP server

This following are example main.cf files for a CP server that is hosted on a single node, and a CP server that is hosted on an SFHA cluster.

- The main.cf file for a CP server that is hosted on a single node:
  See "Sample main.cf file for CP server hosted on a single node that runs VCS" on page 629.
- The main.cf file for a CP server that is hosted on an SFHA cluster:
  See "Sample main.cf file for CP server hosted on a two-node SFHA cluster" on page 631.

Note: The CP server supports Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with SF Oracle RAC clusters. The following example main.cf files use IPv4 addresses.

Sample main.cf file for CP server hosted on a single node that runs VCS

The following is an example of a single CP server node main.cf.

For this CP server single node main.cf, note the following values:

- Cluster name: cps1
- Node name: mycps1

```
include "types.cf"

// cluster name:  cps1
// CP server: mycps1

cluster cps1 (
     UserNames = { admin = bMNfMHmJNiNNlVNhMK, haris = fopKojNvpHouNn,
             "mycps1.symantecexample.com@root@vx" = aj,
             "root@mycps1.symantecexample.com" = hq }
     Administrators = { admin, haris,
             "mycps1.symantecexample.com@root@vx",
             "root@mycps1.symantecexample.com" }
     SecureClus = 1
     HacliUserLevel = COMMANDROOT
     )

system mycps1 (
     )

group CPSSG (
      SystemList = { mycps1 = 0 }
      AutoStartList = { mycps1 }
      )

      IP cpsvip (
            Device @mycps1 = lan0
            Address = "10.209.3.1"
            NetMask = "255.255.252.0"
            )

      NIC cpsnic (
            Device @mycps1 = lan0
            )
```

```
        Process vxcpserv (
              PathName = "/opt/VRTScps/bin/vxcpserv"
              ConfInterval = 30
              RestartLimit = 3
              )

 cpsvip requires cpsnic
 vxcpserv requires cpsvip


 // resource dependency tree
 //
 // group CPSSG
 // {
 // Process vxcpserv
 //     {
 //     IP cpsvip
 //         {
 //         NIC cpsnic
 //         }
 //     }
 // }


group VxSS (
      SystemList = { mycps1 = 0 }
      Parallel = 1
      AutoStartList = { mycps1 }
      OnlineRetryLimit = 3
      OnlineRetryInterval = 120
      )

      Phantom phantom_vxss (
            )

      ProcessOnOnly vxatd (
            IgnoreArgs = 1
            PathName = "/opt/VRTSat/bin/vxatd"
            )



 // resource dependency tree
```

```
//
//    group VxSS
//    {
//    Phantom phantom_vxss
//    ProcessOnOnly vxatd
//    }
```

Sample main.cf file for CP server hosted on a two-node SFHA cluster

The following is an example of a main.cf, where the CP server is hosted on an SFHA cluster.

For this CP server hosted on an SFHA cluster main.cf, note the following values:

- Cluster name: cps1
- Nodes in the cluster: mycps1, mycps2

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"


// cluster: cps1
// CP servers:
// mycps1
// mycps2

cluster cps1 (
     UserNames = { admin = ajkCjeJgkFkkIskEjh,
            "mycps1.symantecexample.com@root@vx" = JK,
            "mycps2.symantecexample.com@root@vx" = dl }
     Administrators = { admin, "mycps1.symantecexample.com@root@vx",
            "mycps2.symantecexample.com@root@vx" }
     SecureClus = 1
     )

system mycps1 (
     )

system mycps2 (
     )

group CPSSG (
```

```
        SystemList = { mycps1 = 0, mycps2 = 1 }
        AutoStartList = { mycps1, mycps2 } )

        DiskGroup cpsdg (
              DiskGroup = cps_dg
              )

        IP cpsvip (
              Device @mycps1 = lan0
              Device @mycps2 = lan0
              Address = "10.209.81.88"
              NetMask = "255.255.252.0"
              )

        Mount cpsmount (
              MountPoint = "/etc/VRTScps/db"
              BlockDevice = "/dev/vx/dsk/cps_dg/cps_volume"
              FSType = vxfs
              FsckOpt = "-y"
              )

        NIC cpsnic (
             Device @mycps1 = lan0
             Device @mycps2 = lan0
             )

        Process vxcpserv (
              PathName = "/opt/VRTScps/bin/vxcpserv"
              )

        Volume cpsvol (
              Volume = cps_volume
              DiskGroup = cps_dg
              )

    cpsmount requires cpsvol
    cpsvip requires cpsnic
    cpsvol requires cpsdg
    vxcpserv requires cpsmount
    vxcpserv requires cpsvip


    // resource dependency tree
```

```
//
// group CPSSG
// {
// Process vxcpserv
//     {
//     Mount cpsmount
//         {
//         Volume cpsvol
//             {
//             DiskGroup cpsdg
//             }
//         }
//     IP cpsvip
//         {
//         NIC cpsnic
//         }
//     }
// }


group VxSS (
      SystemList = { mycps1 = 0, mycps2 = 1 }
      Parallel = 1
      AutoStartList = { mycps1, mycps2 }
      OnlineRetryLimit = 3
      OnlineRetryInterval = 120
      )

      Phantom phantom_vxss (
            )

      ProcessOnOnly vxatd (
            IgnoreArgs = 1
            PathName = "/opt/VRTSat/bin/vxatd"
            )



// resource dependency tree
//
// group VxSS
// {
// Phantom phantom_vxss
```

```
// ProcessOnOnly vxatd
// }
```

Appendix E

Setting up inter-system communication

This appendix includes the following topics:

- About configuring ssh or remsh using the Veritas installer
- Setting up inter-system communication

About configuring ssh or remsh using the Veritas installer

The installer can configure passwordless secure shell (ssh) or remote shell (remsh) communications among systems. The installer uses the ssh or remsh daemon that comes bundled with the operating system. During an installation, you choose the communication method that you want to use. You then provide the installer with the superuser passwords for the systems where you plan to install. Note that for security reasons, the installation program neither stores nor caches these passwords. The ssh or remsh communication among the systems is removed when the installation process completes, unless the installation abruptly terminates. If installation terminated abruptly, use the installation script's `-comcleanup` option to remove the ssh or remsh configuration from the systems.

See "Installation script options" on page 574.

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

- When the root broker is outside of the cluster that you plan to configure.
- When you add new nodes to an existing cluster.

- When the nodes are in a sub-cluster during a phased upgrade.
- When you perform installer sessions using a response file.

Setting up inter-system communication

If you manually need to set up a communication mode, refer to these procedures. You must have root privilege to issue ssh or remsh 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, remsh must be configured in such a way to not prompt for passwords.

If system communication is not possible between systems using ssh or remsh, contact Symantec Support. See http://support.symantec.com.

Setting up ssh on cluster systems

Use the Secure Shell (ssh) to install SF Oracle RAC 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, remsh, and rcp.

Configuring ssh

The procedure to configure ssh uses OpenSSH example file names and commands.

Note: You can configure ssh in other ways. Regardless of how ssh is configured, complete the last step in the example to verify the configuration.

To configure ssh

1. Log on to the system from which you want to install SF Oracle RAC.
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 /.ssh/authorized_keys file on all systems where you plan to installSF Oracle RAC.

If the local system is part of the cluster, make sure to edit the authorized_keys 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.

You are ready to install VCS on several systems in one of the following ways:

- Run the installvcs program on any one of the systems
- Run the installvcs program on an independent system outside the cluster

9 To verify that you can connect to the systems where you plan to install SF Oracle RAC, type:

```
# ssh -x -l root north ls
# ssh -x -l root south ifconfig lan0
```

The commands should execute on the remote system without having to enter a passphrase or password.

Appendix F

Automatic Storage Management

This appendix includes the following topics:

- About ASM in SF Oracle RAC environments
- ASM configuration with SF Oracle RAC
- Configuring ASM in SF Oracle RAC environments
- Sample configuration file Veritas CVM and ASM main.cf file

About ASM in SF Oracle RAC environments

ASM is an integrated storage management solution from Oracle RAC that combines file system and volume management capabilities.

ASM can be configured with Cluster Volume Manager (CVM) for better performance and availability. CVM mirrored volumes with dynamic multipathing improves data access performance and offers continuous data availability in large heterogeneous SAN environments. You can create CVM disk groups and volumes for use as ASM disks groups and configure the ASM disk groups to be managed by the Veritas ASMDG agent. The ASMDG agent mounts, unmounts, and monitors the ASM disk groups.

Depending on the Oracle RAC version installed, the following are supported on ASM for that version:

Oracle RAC 10g Release 2/Oracle RAC 11g Release 1	Data files, control files, online redo logs, archive log files, and backup files

Oracle RAC 11g Release 2	Oracle Cluster Registry devices (OCR), voting disk, data files, control files, online redo logs, archive log files, and backup files

Depending on the Oracle RAC version installed, the following are not supported on ASM for that version:

Oracle RAC 10g Release 2/Oracle RAC 11g Release 1	Oracle binaries, trace files, alert logs, export files, tar files, core files, Oracle Cluster Registry devices (OCR), voting disk, application binaries and application data
Oracle RAC 11g Release 2	Oracle binaries, trace files, alert logs, export files, tar files, core files, application binaries and application data

ASM configuration with SF Oracle RAC

Configure ASM disk groups over CVM volumes in SF Oracle RAC environments. The CVM volumes are mirrored for high availability of data and leverage dynamic multipathing to access the shared storage.

Figure F-1 illustrates the configuration of ASM disk groups over CVM.

Figure F-1 ASM disk groups over CVM

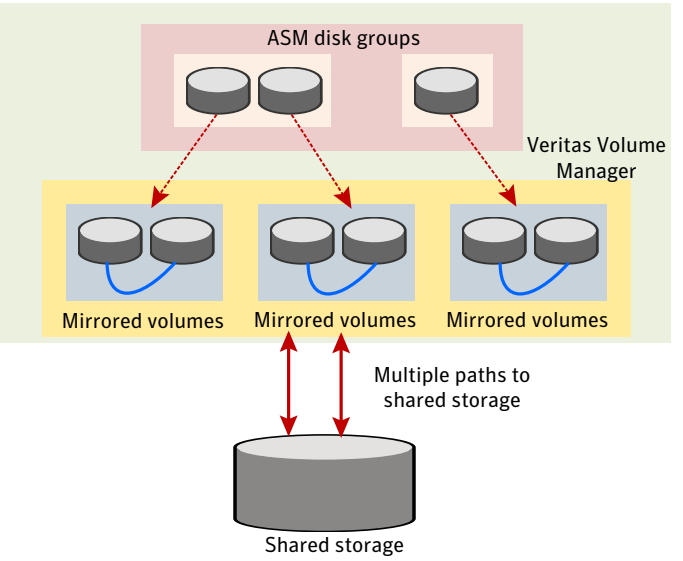


Figure F-2 illustrates the following supported configuration for all supported versions of Oracle RAC:

- ASM disk groups configured over CVM volumes
- Oracle Clusterware and database binaries stored locally
- Oracle database files stored on ASM configured over CVM
  The Oracle databases are managed by Oracle Clusterware.
- Oracle Cluster Registry and voting disk stored on CFS

Figure F-2 Supported Oracle RAC configuration (all supported Oracle RAC versions)

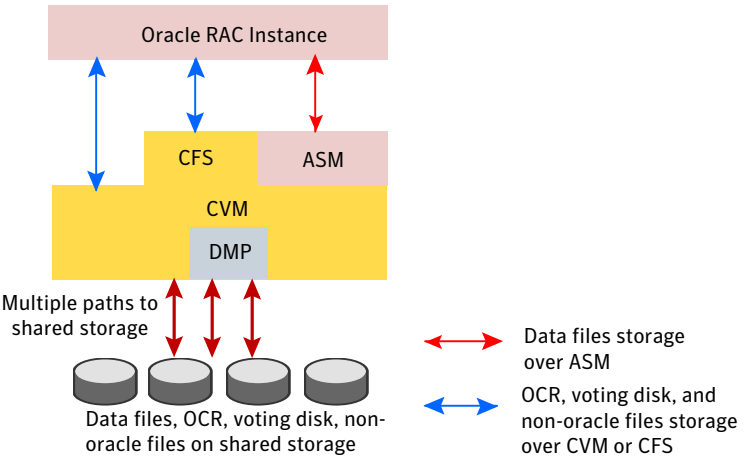
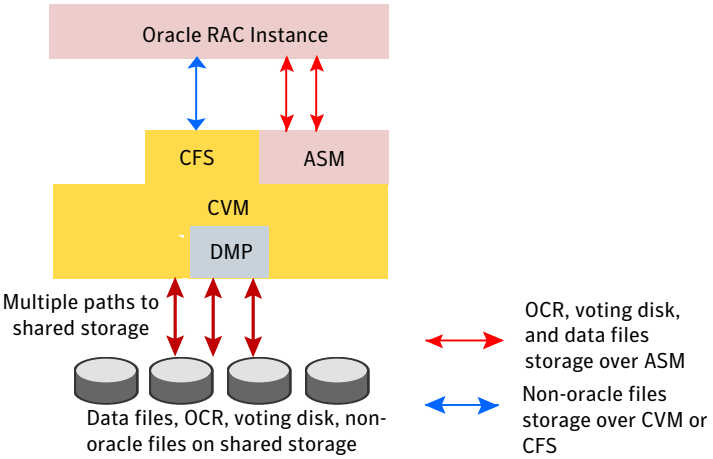


Figure F-3 illustrates the following supported configuration for Oracle RAC 11g Release 2:

- ASM disk groups configured over CVM volumes
- Oracle Clusterware and database binaries stored locally
- Oracle database files stored on ASM configured over CVM
  The Oracle databases are managed by Oracle Clusterware.
- Oracle Cluster Registry and voting disk stored on ASM over CVM volumes

Figure F-3 Supported Oracle RAC configuration (Oracle RAC 11g Release 2)



Configuring ASM in SF Oracle RAC environments

Before you configure ASM, review the planning guidelines for ASM:

See "Planning for Oracle ASM over CVM" on page 60.

Note: Make sure that you have installed SF Oracle RAC and Oracle RAC before configuring ASM.

Depending on the Oracle RAC version, the ASM home directory varies as follows:

Oracle RAC 10g Release 2/Oracle RAC 11g Release 1	Use a home directory distinct from the ORACLE_HOME directory.
Oracle RAC 11g Release 2	The ASM home directory is the same as the Oracle Grid Infrastructure home directory (GRID_HOME).

To configure ASM in SF Oracle RAC installations

1 Set up ASM.

See "Setting up Automatic Storage Management" on page 643.

2 For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: In the ASM home directory, relink the Oracle libraries with Veritas libraries.

Note: When the SF Oracle RAC installer prompts you for the path to the ORACLE_HOME directory, make sure to enter the path to the ASM_HOME directory, which is distinct from the Oracle home directory.

See "Relinking the SF Oracle RAC libraries with Oracle RAC" on page 350.

3 For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1: Unlink the Veritas ODM library from the ASM home directory.

For Oracle RAC 11g Release 2:

Unlink the Veritas ODM library from the ORACLE_HOME directory.

See "Unlinking the SF Oracle RAC ODM library" on page 645.

4 Create the required database storage on ASM by creating CVM disk groups and volumes for use as ASM disks.

See "Creating database storage on ASM" on page 646.

5 Create ASM disk groups and instances.

See "Creating ASM disk groups and instances" on page 647.

6 Verify the ASM setup.

See "Verify the ASM setup" on page 648.

7 Create the Oracle database. For instructions, see the Oracle RAC documentation.

8 Configure VCS service groups for the Oracle database.

See "Configuring VCS service groups for database instances on ASM" on page 648.

Setting up Automatic Storage Management

Perform this step only for Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1 installations.

Set up ASM in a directory distinct from the Oracle database home (ORACLE_HOME) directory. A separate ASM home directory enables you to upgrade or uninstall the software independent of the Oracle database home.

The following procedure describes how to set up ASM using the Oracle Universal Installer. Symantec recommends that you set up ASM locally on each node.

To set up ASM using the Oracle Universal Installer

1 Log in as the Oracle user. On the first node, set the DISPLAY variable.

- For Bourne Shell (bash), type:

```
$ DISPLAY=10.20.12.150:0.0 export DISPLAY
```

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

```
$ setenv DISPLAY 10.20.12.150:0.0
```

2 Start the Oracle Universal Installer.

```
$ cd /dvd_mount

$ ./runInstaller
```

3 Enter the following information when prompted by the Oracle Universal Installer:

Select installation type	Select **Enterprise Edition**.
Specify home details	Enter the full path of the ASM home directory. **Note:** Oracle recommends that the ASM home directory be different from the ORACLE_HOME directory used for installing the Oracle database. Oracle Home location: The installation destination ($ORACLE_HOME). Depending on where you install Oracle binaries, this location is either on shared storage or an identical location on each of the local cluster nodes.
Specify Hardware Cluster Installation Mode	Select **Cluster Installation**. Select the nodes on which you want to install the Oracle RAC database software.

4 Click **Next**.

The Oracle Universal Installer runs a product-specific prerequisite check. Any items that are flagged must be manually checked and configured.

5 On the **Select Configuration Option** screen, select the option **Install database software only**.

Note: Do not select the option **Configure Automatic Storage Management (ASM)**. Symantec recommends that you configure ASM later.

6 Review the configuration summary presented by the Oracle Universal Installer. The Oracle Universal Installer begins the installation.

7 Run the root.sh script as prompted by the Oracle Universal Installer.

Unlinking the SF Oracle RAC ODM library

ODM is a disk management interface for data files that reside on the Veritas File system.

You need to unlink the ODM library from the ORACLE_HOME directory for ASM before you configure the database storage on ASM with SF Oracle RAC.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1, the Oracle home directory for ASM is separate from the ORACLE_HOME directory.

For Oracle RAC 11g Release 2, the Oracle home directory for ASM is the same as the GRID_HOME directory.

Note: Depending on the Oracle version installed, provide the appropriate path for $ORACLE_HOME.

Perform the steps in the procedure on each node in the cluster.

To unlink the Veritas ODM library

1 Log in as the Oracle user.

2 Shut down the ASM instance if it is running:

```
$ srvctl stop asm -n galaxy

$ srvctl stop asm -n nebula
```

3 Change to the Oracle home directory for ASM:

```
$ cd $ORACLE_HOME/lib
```

4 Unlink the Veritas ODM libraries:

For Oracle RAC 10g:

```
$ ln -sf libodmd10.so libodm10.so
```

For Oracle RAC 11g:

```
$ ln -sf libodmd11.so libodm11.so
```

Creating database storage on ASM

This step creates the database storage on ASM using CVM volumes. To create the storage for Oracle databases on ASM, first create the required CVM disk groups and volumes. Then, use these CVM volumes to create ASM disk groups for storing the database files.

To create database storage on ASM

1 Log in as the root user to the CVM master:

To determine the CVM master:

```
# vxdctl -c mode
```

2 Initialize the disks as VxVM disks:

```
# vxdisksetup -i c1t1d0
```

3 Set the activation mode for the disk group on all nodes:

```
# vxdg -g ora_asm_dg set activation=sw
```

4 Create the CVM disk group and volume:

```
# vxdg -s init ora_asm_dg c1t1d0

# vxassist -g ora_asm_dg make ora_asm_vol 2000M
```

5 Set the permissions for the Oracle user on the volume:

```
# vxedit -g ora_asm_dg  \
set group=dba user=oracle mode=660 ora_asm_vol
```

Configure ASM using DBCA (Oracle RAC 10g Release 2/Oracle RAC 11g Release 1), ASMCA (Oracle RAC 11g Release 2), or OEM.

Creating ASM disk groups and instances

Depending on the Oracle RAC version, use one of the following ways to create ASM disk groups:

Oracle RAC 10g Release 2/Oracle RAC 11g Release 1	Database Configuration Assistant (DBCA) Oracle Enterprise Manager (OEM) Manual
Oracle RAC 10g Release 2	ASM Configuration Assistant (ASMCA) Manual

The following tasks are performed:

- The ASM disk group and instance is created.
- The ASM instance is started and the disk group is mounted on all nodes in the cluster. The default ASM instance name is +ASM*n* where n is the instance number depending on the number of ASM instances.

Note: For ASM instances that use a pfile, if you restart a node, make sure that the underlying volumes are available before the ASM disk group is mounted. Then, update the ASM init.ora parameter with the full path that contains the VxVM volumes created for ASM.

For ASM instances that use an spfile, the parameter is updated automatically by the Oracle Configuration Assistant.

In either case, dependencies must be managed manually. Symantec recommends the use of the ASMDG agent for easier management of ASM disk groups.

SF Oracle RAC requires the following settings when you create ASM disk groups and instances:

Type of parameter file for the ASM instance	server parameter file (spfile)
Disk Discovery Path	Enter the full path that contains the VxVM volumes created for ASM, for example `/dev/vx/rdsk/ora_asm_dg/ora_asm_vol`.

Redundancy	Select the option **External**. Mirroring is performed by CVM.
Select member disks	Select the VxVM disks you want to use; You may need to select the **Force** checkbox next to the ASM disks you want to use if the disk group creation fails.

For detailed instructions, see the Oracle documentation.

Verify the ASM setup

Verify that the database services for ASM are up and running after the installation.

To verify the ASM installation

1. Change to the Oracle Clusterware/Grid Infrastructure home directory:

   For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

   ```
   # cd $CRS_HOME/bin
   ```

   For Oracle RAC 11g Release 2:

   ```
   # cd $GRID_HOME/bin
   ```

2. Verify the status of ASM on all the nodes in the cluster:

   ```
   # ./srvctl status asm
   ASM instance +ASM1 is running on node galaxy
   ```

   The sample output shows that there is one ASM instance running on the local node.

Configuring VCS service groups for database instances on ASM

This section describes how to configure the Oracle service group using the CLI for databases on ASM.

For sample service group illustration:

See "sfrac05_main.cf file" on page 616.

For a sample configuration file describing the configuration, see the file `sfrac05_main.cf` in the directory `/etc/VRTSvcs/conf/sample_rac/`.

The following procedure assumes that you have created the database.

To configure the Oracle service group using the CLI

1 Change the cluster configuration to read-write mode:

```
# haconf -makerw
```

2 Add the service group to the VCS configuration:

```
# hagrp -add dbgrp
```

3 Modify the attributes of the service group:

```
# hagrp -modify dbgrp Parallel 1

# hagrp -modify dbgrp SystemList galaxy 0  nebula 1

# hagrp -modify dbgrp AutoStartList galaxy nebula
```

4 Add the CVMVolDg resource for the service group:

```
# hares -add oradata_voldg CVMVolDg dbgrp
```

5 Modify the attributes of the CVMVolDg resource for the service group:

```
# hares -modify oradata_voldg CVMDiskGroup ora_asm_dg
# hares -modify oradata_voldg CVMActivation sw
# hares -modify oradata_voldg CVMVolume ora_asm_vol
```

6 Add the ASMDG resource for the service group:

```
# hares -add asmdg ASMDG dbgrp
```

7 Modify the attributes of the ASMDG resource for the service group.

Note: The $ASM_HOME variable refers to the ASM home directory.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1, the ASM home directory is distinct from the ORACLE_HOME directory.

For Oracle RAC 10g Release 2/Oracle RAC 11g Release 1:

```
# hares -modify asmdg DiskGroups ASM_RAC_DG
# hares -modify asmdg Home "$ASM_HOME"
# hares -local asmdg  Sid
# hares -modify asmdg Sid "+ASM1" -sys galaxy
# hares -modify asmdg Sid "+ASM2" -sys nebula
# hares -modify asmdg Owner oracle
```

For Oracle RAC 11g Release 2:

```
# hares -modify asmdg DiskGroups ASM_RAC_DG
# hares -modify asmdg Home "$ASM_HOME"
# hares -local asmdg  Sid
# hares -modify asmdg Sid "+ASM1" -sys galaxy
# hares -modify asmdg Sid "+ASM2" -sys nebula
# hares -modify asmdg Owner grid
```

8 Add the Oracle RAC database instance to the service group:

```
# hares -add asmdb Oracle dbgrp
```

9 Modify the attributes of the Oracle resource for the service group:

```
# hares -modify asmdb Owner oracle
# hares -local asmdb Sid
# hares -modify asmdb Sid oradb1 -sys galaxy
# hares -modify asmdb Sid oradb2 -sys nebula
# hares -modify asmdb Home "$ORACLE_HOME"
# hares -modify asmdb StartUpOpt SRVCTLSTART
# hares -modify asmdb ShutDownOpt SRVCTLSTOP
```

10 Set the dependencies between the ASMDG resource and the CVMVolDg resource for the Oracle service group:

```
# hares -link asmdg oradata_voldg
```

11 Set the dependencies between the Oracle resource and the ASMDG resource for the Oracle service group:

```
# hares -link asmdb asmdg
```

12 Create an online local firm dependency between the dbgrp service group and the cvm service group:

```
# hagrp -link dbgrp cvm online local firm
```

13 Enable the Oracle service group:

```
# hagrp -enableresources dbgrp
```

14 Change the cluster configuration to the read-only mode:

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

15 Bring the Oracle service group online on all the nodes:

```
# hagrp -online dbgrp -any
```

Sample configuration file Veritas CVM and ASM main.cf file

A sample configuration file (sfrac05_main.cf) illustrating ASM configuration in SF Oracle RAC is available at `/etc/VRTSvcs/conf/sample_rac/`.

For an illustration of the service group configuration:

See "sfrac05_main.cf file" on page 616.

Appendix G

Creating a test database

This appendix includes the following topics:

- About creating a test database
- Creating a database for Oracle

About creating a test database

A test database can be created and used for both testing and troubleshooting purposes.

The following optional procedures describe the methods for creating a test database on shared storage.

Use you own tools or refer to the guidelines below on using the Oracle DBCA (Database Creation Assistant) tool to create a database on shared raw VxVM volumes or shared VxFS file systems.

Creating a database for Oracle

Before you begin to create the database, ensure that the following prerequisites are met:

- The CRS daemons must be running.
  To verify the status of Oracle Clusterware, type the following command:

  ```
  # $CRS_HOME/bin/crs_stat
  ```

- All private IP addresses on each node must be up.
  Use the `ping` command to verify that all private IP addresses on each node are up.

Refer to your Oracle documentation for instructions on how to install the Oracle database.

You can create the database on one of the following types of storage:

- Shared raw volume
  See "Creating the database storage on raw volumes" on page 654.
- Cluster File System (CFS)
  See "Creating the database storage on CFS" on page 655.
- ASM
  See "Creating database storage on ASM" on page 646.

Creating the database storage on raw volumes

You can create the database storage on shared raw volume.

To create the database storage on shared raw volumes

1. Log in as root user.
2. On the master node, create a shared disk group:

   ```
   # vxdg -s init oradatadg Disk_1
   ```

3. Create a volume in the shared group for each of the required tablespaces.

   Refer to the Oracle documentation to determine the tablespace requirements.

   For example, type:

   ```
   # vxassist -g oradatadg make VRT_galaxy 1000M
   # vxassist -g oradatadg make VRT_spfile1 10M
   .
   .
   ```

4 Define the access mode and permissions for the volumes storing the Oracle data.

For each volume listed in $ORACLE_HOME/raw_config, use the `vxedit`(1M) command:

```
# vxedit -g disk_group set group=group user=user mode=660 volume
```

For example:

```
# vxedit -g oradatadg set group=dba user=oracle mode=660 \
VRT_galaxy
```

In this example, VRT_galaxy is the name of one of the volumes. Repeat the command to define access mode and permissions for each volume in the oradatadg.

5 Create the database using the Oracle documentation.

Creating the database storage on CFS

If you plan to use a cluster file system to store the Oracle database, use the following procedure to create the file system.

To create the database storage on CFS

1 Create a disk group (for example, oradatadg):

```
# vxdg -s init oradatadg Disk_1
```

2 Create a single shared volume (for example, oradatavol) that is large enough to contain a file system for all tablespaces.

For example, assuming 6.8 GB is required for database storage, type:

```
# vxassist -g oradatadg make oradatavol 6800M
```

3 Set the activation mode (sw) to allow shared access to the disk group:

```
# vxdg -g oradatadg set activation=sw
```

4 Start the volume in the disk group:

```
# vxvol -g oradatadg startall
```

5 Create a VxFS file system in this volume. From one node, type:

```
# mkfs -F vxfs -o largefiles /dev/vx/rdsk/oradatadg/oradatavol
```

6 Create a mount point for the shared file system:

```
# mkdir /oradata
```

7 From the same node, mount the file system:

```
# mount -F vxfs -o cluster /dev/vx/dsk/oradatadg/oradatavol \
/oradata
```

8 Set "oracle" as the owner of the file system, and set "755" as the permissions:

```
# chown oracle:oinstall /oradata
# chmod 755 /oradata
```

9 On the other node(s), complete step 6 and step 7.

10 Create the database using the Oracle documentation.

Appendix H

High availability agent information

This appendix includes the following topics:

- About agents
- CVMCluster agent
- CVMVxconfigd agent
- CVMVolDg agent
- CFSMount agent
- CFSfsckd agent
- PrivNIC agent
- MultiPrivNIC agent
- CSSD agent
- VCS agents for Oracle
- CRSResource agent

About agents

An agent is defined as a process that starts, stops, and monitors all configured resources of a type, and reports their status to Veritas Cluster Server (VCS). Agents have both entry points and attributes. Entry points are also known as agent functions and are referred to as "agent functions" throughout the document.

Attributes contain data about the agent. An attribute has a definition and a value. You change attribute values to configure resources, which are defined as the individual components that work together to provide application services to the public network. For example, a resource may be a physical component such as a disk or a network interface card, a software component such as Oracle or a Web server, or a configuration component such as an IP address or mounted file system.

Attributes are either optional or required, although sometimes the attributes that are optional in one configuration may be required in other configurations. Many optional attributes have predefined or default values, which you should change as required. A variety of internal use only attributes also exist. Do not modify these attributes—modifying them can lead to significant problems for your clusters. Attributes have type and dimension. Some attribute values can accept numbers, others can accept alphanumeric values or groups of alphanumeric values, while others are simple boolean on/off values.

The entry points and attributes for each SF Oracle RAC agent are described in this appendix.

VCS agents included within SF Oracle RAC

SF Oracle RAC includes the following VCS agents:

- CVMCluster agent
- CVMVxconfigd agent
- CVMVolDg agent
- CFSMount agent

An SF Oracle RAC installation automatically configures the CVMCluster resource and the CVMVxconfigd resource.

You must configure the CVMVolDg agent for each shared disk group. If the database uses cluster file systems, configure the CFSMount agent for each volume in the disk group.

Use the information in this appendix about the entry points and attributes of the listed agents to make necessary configuration changes. For information on how to modify the VCS configuration:

See the *Veritas Cluster Server Administrator's Guide*

VCS agents for Oracle included within SF Oracle RAC

SF Oracle RAC includes the following VCS agents for Oracle:

- Oracle agent

The Oracle agent monitors the database processes.

- Netlsnr agent
  The Netlsnr agent brings the listener services online, monitors their status, and takes them offline.
- PrivNIC agent
  The PrivNIC agent provides high availability to a single private IP address across LLT Ethernet interfaces for a system.
- MultiPrivNIC agent
  The MultiPrivNIC agent provides high availability to multiple private IP addresses across LLT Ethernet interfaces for a system.
- CSSD agent
  The CSSD (Cluster Synchronization Services daemon) agent provides the resources to monitor Oracle Clusterware. The agent ensures that the dependency of cssd on the OCR and the VOTE resources and the PrivNIC (optional) resource are satisfied.
- ASMDG agent
  The ASMDG agent mounts and unmounts the ASM disk groups onto an ASM instance.

See the *Veritas Cluster Server Agent for Oracle Installation and Configuration Guide*

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	Dimension	Description
CVMClustName	string-scalar	Name of the cluster.
CVMNodeAddr	string-association	List of host names and IP addresses.
CVMNodeId	string-association	Associative list. The first part names the system; the second part contains the LLT ID number for the system.
CVMTransport	string-scalar	Specifies the cluster messaging mechanism. Default = gab **Note:** Do not change this value.
PortConfigd	integer-scalar	The port number that is used by CVM for vxconfigd-level communication.
PortKmsgd	integer-scalar	The port number that is used by CVM for kernel-level communication.
CVMTimeout	integer-scalar	Timeout in seconds used for CVM cluster reconfiguration. Default = 200

CVMCluster agent type definition

The following type definition is included in the file, `CVMTypes.cf`:

```
type CVMCluster (
        static int InfoTimeout = 0
        static int NumThreads = 1
        static int OnlineRetryLimit = 2
        static int OnlineTimeout = 400
        static str ArgList[] = { CVMTransport, CVMClustName,
           CVMNodeAddr, CVMNodeId, PortConfigd, PortKmsgd,
           CVMTimeout }
        NameRule = ""
        str CVMClustName
        str CVMNodeAddr{}
        str CVMNodeId{}
        str CVMTransport
        int PortConfigd
        int PortKmsgd
        int CVMTimeout
  )
```

Note: The attributes `CVMNodeAddr`, `PortConfigd`, and `PortKmsgd` are not used in an SF Oracle RAC 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 = rac_cluster101
        CVMNodeId = { galaxy = 0, nebula = 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 Oracle RAC installation configures the `syslog` option for the CVMVxconfigd agent.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

Entry points for CVMVxconfigd agent

Table H-3 describes the entry points for the CVMVxconfigd agent.

Table H-3 CVMVxconfigd entry points

Entry Point	Description
Online	Starts the `vxconfigd` daemon
Offline	N/A
Monitor	Monitors whether `vxconfigd` daemon is running
imf_init	Initializes the agent to interface with the AMF kernel module. This function runs when the agent starts up.
imf_getnotification	Gets notification about the `vxconfigd` process state. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification. If the `vxconfigd` process fails, the function initiates a traditional CVMVxconfigd monitor entry point.
imf_register	Registers or unregisters the `vxconfigd` process id (pid) with the AMF kernel module. This function runs after the resource goes into steady online state.

Attribute definition for CVMVxconfigd agent

Table H-4 describes the modifiable attributes of the CVMVxconfigd resource type.

Table H-4 CVMVxconfigd agent attribute

Attribute	Dimension	Description
CVMVxconfigdArgs	keylist	List of the arguments that are sent to the `online` entry point. Symantec recommends always specifying the `syslog` option.

Table H-4 CVMVxconfigd agent attribute *(continued)*

Attribute	Dimension	Description
IMF	integer-association	

Table H-4 CVMVxconfigd agent attribute *(continued)*

Attribute	Dimension	Description
		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. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 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: ■ 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 oracle_imf_register agent function to register the resource with the AMF kernel driver. The value of the

Table H-4 CVMVxconfigd agent attribute *(continued)*

Attribute	Dimension	Description
		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. For more details of IMF attribute for the agent type, refer to the *Veritas Cluster Server Administrator's Guide*.

CVMVxconfigd agent type definition

The following type definition is included in the CVMTypes.cf file:

```
type CVMVxconfigd (
         static int FaultOnMonitorTimeouts = 2
         static int RestartLimit = 5
         static str ArgList[] { CVMVxconfigdArgs }
         static str Operations = OnOnly
         keylist CVMVxconfigdArgs
         )
```

CVMVxconfigd agent sample configuration

The following is an example definition for the `CVMVxconfigd` resource in the CVM service group:

```
CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )
```

CVMVolDg agent

The CVMVolDg agent manages the CVM disk groups and CVM volumes and volume sets within the disk groups by performing the following functions:

- Imports the shared disk group from the CVM master node
- Starts the volumes and volume sets in the disk group
- Monitors the disk group, volumes, and volume sets
- Optionally, deports the disk group when the dependent applications are taken offline. The agent deports the disk group only if the appropriate attribute is set.

Configure the CVMVolDg agent for each disk group used by a Oracle service group. A disk group must be configured to only one Oracle service group.If cluster file systems are used for the database, configure the CFSMount agent for each volume or volume set in the disk group.

Entry points for CVMVolDg agent

Table H-5 describes the entry points used by the CVMVolDg agent.

Table H-5 CVMVolDg agent entry points

Entry Point	Description
Online	Imports the shared disk group from the CVM master node, if the disk group is not already imported. Starts all volumes and volume sets in the shared disk group specified by the CVMVolume attribute. Sets the disk group activation mode to shared-write if the value of the CVMActivation attribute is sw. You can set the activation mode on both slave and master systems.
Offline	Removes the temporary files created by the online entry point. If the `CVMDeportOnOffline` attribute is set to 1 and if the shared disk group does not contain open volumes on any node in the cluster, the disk group is deported from the CVM master node.

Table H-5 CVMVolDg agent entry points *(continued)*

Entry Point	Description
Monitor	Determines whether the disk group, the volumes, and the volume sets are online. 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. **Note:** If the CFSMount resource goes offline and the file system on the volume set is unmounted, the agent retains the online state of the volume set even if the file system metadata volume in the volume set is offline. This is because the CVMVolDg agent is unable to determine whether or not the volumes that are offline are metadata volumes.
Clean	Removes the temporary files created by the online entry point.

Attribute definition for CVMVolDg agent

Table H-6 describes the user-modifiable attributes of the CVMVolDg resource type.

Table H-6 CVMVolDg agent attributes

Attribute	Dimension	Description
CVMDiskGroup (required)	string-scalar	Shared disk group name.
CVMVolume (required)	string-keylist	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.
CVMActivation (required)	string-scalar	Activation mode for the disk group. Default = `sw (shared-write)` This is a localized attribute.

Table H-6 CVMVolDg agent attributes *(continued)*

Attribute	Dimension	Description
CVMVolumeIoTest(optional)	string-keylist	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.
CVMDeportOnOffline (optional)	integer-scalar	Indicates whether or not the shared disk group must be deported when the last online CVMVolDg resource for a disk group is taken offline. The value 1 indicates that the agent will deport the shared disk group from the CVM master node, if not already deported, when the last online CVMVolDg resource for the disk group is taken offline. The value 0 indicates that the agent will not deport the shared disk group when the CVMVolDg resource is taken offline. The default value is set to 0. **Note:** If multiple CVMVolDg resources are configured for a shared disk group, set the value of the attribute to either 1 or 0 for all of the resources. The CVM disk group is deported based on the order in which the CVMVolDg resources are taken offline. If the CVMVolDg resources in the disk group contain a mixed setting of 1 and 0 for the `CVMDeportOnOffline` attribute, the disk group is deported only if the attribute value is 1 for the last CVMVolDg resource taken offline. If the attribute value is 0 for the last CVMVolDg resource taken offline, the disk group is not deported. The deport operation fails if the shared disk group contains open volumes.

CVMVolDg agent type definition

The CVMTypes.cf file includes the CVMVolDg type definition:

```
type CVMVolDg (
        static keylist RegList = { CVMActivation, CVMVolume }
        static int OnlineRetryLimit = 2
        static int OnlineTimeout = 400
        static str ArgList[] = { CVMDiskGroup, CVMVolume, CVMActivation,
        CVMVolumeIoTest, CVMDGAction, CVMDeportOnOffline }
        str CVMDiskGroup
        str CVMDGAction
        keylist CVMVolume
        str CVMActivation
        keylist CVMVolumeIoTest
        int CVMDeportOnOffline
        temp int voldg_stat
)
```

CVMVolDg agent sample configuration

Each Oracle service group requires a CVMVolDg resource type to be defined. The following is a sample configuration:

```
CVMVolDg 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 *Veritas 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 `fsclustadm` command.
Clean	Generates a null operation for a cluster file system mount.
imf_init	Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for the agent. This function runs when the agent starts up.
imf_ getnotification	Gets notification about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification.
imf_register	Registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into steady state (online or offline).

Attribute definition for CFSMount agent

Table H-8 lists user-modifiable attributes of the CFSMount Agent resource type.

Table H-8 CFSMount Agent attributes

Attribute	Dimension	Description
MountPoint	string-scalar	Directory for the mount point.
BlockDevice	string-scalar	Block device for the mount point.
NodeList	string-keylist	List of nodes on which to mount. If NodeList is NULL, the agent uses the service group system list.

Table H-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description
IMF	integer-association	

Table H-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description
		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. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 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: ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources

Table H-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description
		■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the oracle_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.

MountOpt
(optional)
	string-scalar	Options for the mount command. To create a valid MountOpt attribute string:
		■ Use the VxFS type-specific options only.
		■ Do not use the -o flag to specify the VxFS-specific options.
		■ Do not use the `-F` vxfs file system type option.
		■ Be aware the cluster option is not required.
		■ Specify options in comma-separated list:
		`ro`
		`ro,cluster`
		`blkclear,mincache=closesync`

Policy (optional)	string-scalar	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.

Table H-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description
Primary (Not set by user)	string-scalar	Information only. Stores the primary node name for a VxFS file system. The value is automatically modified in the configuration file when an unmounted file system is mounted or another node becomes the primary node. The user does not set this attribute and user programs do not rely on this attribute.

CFSMount agent type definition

The `CFSTypes.cf` file includes the CFSMount agent type definition:

```
type CFSMount (
    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 = nebula;
        )
```

CFSfsckd agent

The CFSfsckd agent starts, stops, and monitors the `vxfsckd` process. The CFSfsckd agent executable is `/opt/VRTSvcs/bin/CFSfsckd/CFSfsckdAgent`. The type definition is in the `/etc/VRTSvcs/conf/config/CFSTypes.cf` file. The configuration is added to the `main.cf` file after running the `cfscluster config` command.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

Entry points for CFSfsckd agent

Table H-9 describes the CFSfsckd agent entry points.

Table H-9 CFSfsckd agent entry points

Entry Points	Description
Online	Starts the vxfsckd process.
Offline	Kills the vxfsckd process.
Monitor	Checks whether the vxfsckd process is running.
Clean	A null operation for a cluster file system mount.
imf_init	Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for the agent. This function runs when the agent starts up.
imf_ getnotification	Gets notification about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification.
imf_register	Registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into steady state (online or offline).

Attribute definition for CFSfsckd agent

Table H-10 lists user-modifiable attributes of the CFSfsckd Agent resource type.

Table H-10 CFSfsckd Agent attributes

Attribute	Dimension	Description
IMF	integer-association	

Table H-10 CFSfsckd Agent attributes *(continued)*

Attribute	Dimension	Description
		Resource-type level attribute that determines whether the CFSfsckd agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 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: ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources

Table H-10 CFSfsckd Agent attributes *(continued)*

Attribute	Dimension	Description
		■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the oracle_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.

CFSfsckd agent type definition

The CFSfsckd type definition:

```
type CFSfsckd (
        static int RestartLimit = 1
        str ActivationMode{}
)
```

CFSfsckd agent sample configuration

This is a sample of CFSfsckd configuration:

```
CFSfsckd vxfsckd (
)
```

PrivNIC agent

The PrivNIC agent provides high availability to a single private IP address across LLT Ethernet interfaces for a system. Private IP addresses are required by Oracle Clusterware and the Oracle database to provide communication between the cluster nodes.

Note: The PrivNIC agent operates over LLT links. To use the agent, the Oracle Clusterware interconnects and the Oracle RAC database communication links must be configured as LLT links.

The PrivNIC agent relies on LLT to monitor the LLT Ethernet interfaces. It queries LLT for the number of visible nodes on each of the LLT Ethernet interfaces.

The PrivNIC agent provides a reliable alternative when operating system limitations prevent you from using NIC bonding to provide increased bandwidth using multiple network interfaces. In the event of a NIC failure or link failure, the agent fails over the private IP address from the failed link to the connected or available LLT link. If the preferred link becomes available, the IP address is failed back to the preferred link.

Functions of the PrivNIC agent

Table H-11 describes the PrivNIC agent's monitor entry point.

Note: Because the resource is persistent, only the monitor entry point is required.

Table H-11 PrivNIC agent entry point

Entry Point	Description
Monitor	The PrivNIC agent queries LLT to create a list of nodes visible on every LLT network interface. The PrivNIC agent then applies various filters to this list to arrive at a most desired failover decision and calculates a "winner" device on which to configure the IP address. The "winner"device is compared to the currently active device where the IP address is currently configured. If the active and "winner" devices are different, the PrivNIC agent initiates a failover to the "winner" device.

Attributes of the PrivNIC agent

Table H-12 describes the user-modifiable attributes of the PrivNIC agent.

Table H-12 Required attributes for PrivNIC agent

Attribute	Dimension	Description

Device	string - association	Specifies the network interface device as shown by the `ifconfig` command and the network ID associated with the interface. Network IDs of the interfaces connected to the same physical network must match. The interface with the lower network-id has the higher preference for failover. Interfaces specified in the PrivNIC configuration should be exactly the same in name and total number as those which have been used for LLT configuration.
		At least one interface device must be specified.
		Example:
		`Device@galaxy = {lan1=0, lan2=1, lan3=2}`
		`Device@nebula = {lan0=0, lan1=1, lan2=2}`

Address	string-scalar	The numerical private IP address. Checks are performed to determine if this is a valid IP address. When configuring private IPv4 addresses for Oracle Clusterware, make sure that there are no leading zeroes in any of the octets that comprise the IP address, for example X.X.X.01 or X.X.0X.1 or X.0X.X.1 or 0X.X.X.1. Ensure that the IPv4 addresses have the format as " X.X.X.1". The following is an example of an IPv4 address: `Address = "192.168.12.1"`
NetMask	string - association	The numerical netmask for the private IP address. For example: `Address = "255.255.255.0"`

Optional attributes of the PrivNIC agent

Table H-13 Optional attributes for PrivNIC agent

Attribute	Dimension	Description

DeviceTag	string - association	Associates an LLT device "tag" with device via the network-id. If an LLT device tag (as specified in the `/etc/lltab` file) differs from the name of the network interface as shown in "ifconfig," then DeviceTag must be specified for that interface.
		For example: `/etc/lltab` contains:
		`link lan0 /dev/lan:0 - ether - -`
		`link lan1 /dev/lan:1 - ether - -`
		`link-lowpri lan0 /dev/lan:0 - ether - -`
		In the above case, DeviceTag does not need to be specified. However, if `/etc/lltab` contains:
		`link link1 /dev/lan:1 - ether - -`
		`link link2 /dev/lan:2 - ether - -`
		`link-lowpri spare /dev/lan:0 - ether - -`
		And,
		`Device@galaxy = { lan1=0, lan2=1, lan0=2 }`
		DeviceTag needs to be specified as:
		`DeviceTag@galaxy = { link1=0, link2=1, spare=2 }`

GabPort	string-scalar	A single lower-case letter specifying the name of the GAB port to be used for filtering. "o" is the default. NULL disables GAB port filtering. Example: `GabPort = "b"`
UseVirtualIP	integer-scalar	The default is 0, which specifies that the agent use the physical interface for configuring the private IP address when possible. The value 1 specifies that the agent always use the virtual interface for configuring the private IP address. The value 2 (which includes the functionality of the value 1) specifies the agent should complain if the private IP address already exists on a physical interface.

Table H-13 Optional attributes for PrivNIC agent *(continued)*

Attribute	Dimension	Description
UseSystemList	integer-scalar	The value 1 specifies that the agent use the SystemList of the service group to filter the node list. Default = 0.
ExcludeNode	integer-vector	List of nodes to permanently exclude from calculation.

States of the PrivNIC agent

Table H-14 lists the states of the PrivNIC agent.

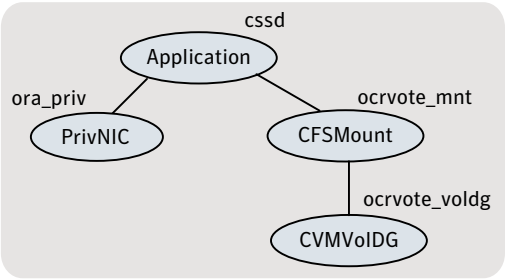
Table H-14 States of the PrivNIC agent

State	Description
Online	Indicates that the private IP address is available.
Unknown	Indicates the inability to determine the state of the resource due to incorrect attribute settings or other configuration issues.

Sample service group configuration with the PrivNIC agent

Figure H-1 illustrates a basic service group configuration with the PrivNIC agent.

Figure H-1 Basic service group configuration with the PrivNIC agent



This configuration shows the dependency of the CSSD resource on the private IP address configured as a PrivNIC resource along with the OCR and voting disk volume and mount point dependencies.

For sample deployment scenarios, see the appendix *SF Oracle RAC deployment scenarios*.

Type definition of the PrivNIC resource

The following extract shows the type definition of the PrivNIC resource in the `PrivNIC.cf` file:

```
type PrivNIC (
        static str ArgList[] = { Device, DeviceTag, Address,
               NetMask, UseVirtualIP, GabPort, UseSystemList,
               ExcludeNode }
        static int OfflineMonitorInterval = 60
        static int MonitorTimeout = 300
        static str Operations = None

        str Device{}
        str DeviceTag{}
        str Address = ""
        str NetMask = ""
        int UseVirtualIP = 0
        str GabPort = "o"
        int UseSystemList = 0
        int ExcludeNode[]
)
```

Sample configuration of the PrivNIC resource

The following extract from the configuration file illustrates the configuration of a PrivNIC resource.

```
group cvm (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )



        PrivNIC ora_priv (
                Critical = 0
                Device@galaxy = { lan1 = 0, lan2 = 1 }
                Device@nebula = { lan1 = 0, lan2 = 1 }
                Address@galaxy = "192.168.12.1"
                Address@nebula = "192.168.12.2"
```

```
    NetMask = "255.255.255.0"
    )
```

For more examples, see the sample configuration files located at `/etc/VRTSvcs/conf/sample_rac/`.

MultiPrivNIC agent

The MultiPrivNIC agent provides high availability to multiple private IP addresses across LLT Ethernet interfaces for a system. In the event of a NIC failure or link failure, the agent fails over the private IP address from the failed link to one of the available LLT links. To use the agent, the Oracle Clusterware interconnects and the Oracle RAC database communication links must be configured as LLT links.

The MultiPrivNIC agent is a reliable alternative in scenarios where operating system limitations prevent you from using NIC bonding to provide increased bandwidth and high availability using multiple network interfaces. Even if link aggregation solutions in the form of bonded NICs are implemented, the MultiPrivNIC agent can be used to provide additional protection against the failure of aggregated links by failing over the IP addresses to the available alternate links. These alternate links can be simple NIC interfaces or bonded NICs.

The SF Oracle RAC installer supports the configuration of MultiPrivNIC resources when you prepare to install Oracle RAC.

Managing high availability of private interconnects

The MultiPrivNIC agent operates over LLT links and relies on LLT to monitor the cluster interfaces. It queries LLT to count and report the number of visible nodes on each of the LLT interfaces. In the event that a preferred link goes down, the IP address is failed over to the private link on which maximum number of peer nodes are visible. If multiple links see maximum nodes and if load-balancing is enabled, the agent considers the current traffic on all devices and calculates a "winner" device with lower traffic. If load balancing is not enabled, the IP address is failed over to the link with the lower network-id.

The failover decision for an IP address is made only when the link hosting the IP address fails. If the preferred link becomes available, the IP address is failed back to the preferred link regardless of whether load-balancing is enabled or disabled.

Functions of the MultiPrivNIC agent

Table H-15 describes the MultiPrivNIC agent's monitor entry point.

Note: Because the resource is persistent, only the monitor entry point is required.

Table H-15 MultiPrivNIC agent entry point

Entry point	Description
Monitor	The MultiPrivNIC agent queries LLT to create a list of the visible nodes on each LLT network interface. The agent applies various filters to this list and calculates a winner device on which to configure the IP address. If the active device on which the IP address is configured does not see the same number of nodes as the winner device, the agent fails over the IP address to the winner device.

Attributes of the MultiPrivNIC agent

Table H-16 below describes the user-modifiable attributes of the MultiPrivNIC resource type.

Table H-16 MultiPrivNIC agent attribute definitions

Attribute	Dimension	Description

Device	string-association	The device attribute specifies the network interface displayed by the `ifconfig` command and the network ID associated with the interface.
		The network IDs of the interfaces connected to the same physical network must match. The interfaces specified in the MultiPrivNIC configuration should be exactly the same in name and total number as those which have been used for LLT configuration.
		An example of the device attribute is as follows:
		`Device@galaxy = {lan1=0, lan2=1, lan3=2}`
		`Device@nebula = {lan1=0, lan2=1, lan3=2}`

Table H-16 MultiPrivNIC agent attribute definitions *(continued)*

Attribute	Dimension	Description

Address	string-association	The numerical private IP address and its preferred device.
		
		The agent verifies that the IP addresses are valid addresses. When you configure private IP addresses, ensure that the addresses do not have a leading 0 in any of the octets that comprise the IP address. The IP address must be in the format " X.X.X.1".
		
		In the following example, 0 and 1 indicates the ID of the device on which the IP address is hosted. If the device is unavailable, the agent automatically reconfigures the IP address on one of the available devices. The available device is determined based on the UseLoadBalance attribute setting.
		
		An example of the address attribute is as follows:
		
		`Address @galaxy =`
		`{ "192.168.12.1" =0,`
		`"192.168.2.1" =0,`
		`"192.168.3.1" =1 }`
		`Address @nebula =`
		`{ "192.168.12.2" =0,`
		`"192.168.2.2" =0,`
		`"192.168.3.2" =1 }`

Netmask	string-association	The netmask attribute is the numerical netmask for the private IP address. For example, Address = "255.255.255.0".

Table H-16 MultiPrivNIC agent attribute definitions *(continued)*

Attribute	Dimension	Description
UseLoadBalance		A boolean value 0 or 1. In the event that the preferred device is unavailable and multiple links see maximum nodes during failover: ■ Setting the attribute to 1 fails over the IP address to the device with lower traffic. ■ Setting the attribute to 0 fails over the IP address to the device with lower network ID. **Note:** If the preferred device becomes available, the IP address is failed back to the preferred device regardless of the value of UseLoadBalance.

States of the MultiPrivNIC agent

Table H-17 lists the states of the MultiPrivNIC agent.

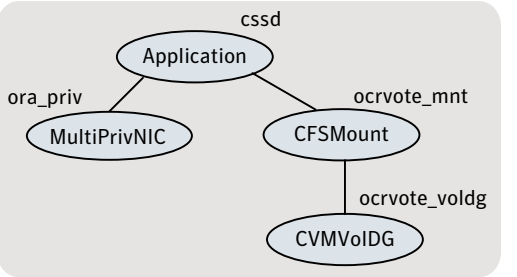
Table H-17 States of the MultiPrivNIC agent

State	Description
Online	Indicates that the private IP addresses are available.
Unknown	Indicates the inability to determine the state of the resource due to incorrect attribute settings or other configuration issues.

Sample service group configuration with the MultiPrivNIC agent

Figure H-2 illustrates a sample service group configuration with the MultiPrivNIC agent.

Figure H-2 Basic service group configuration with MultiPrivNIC agent



The illustrated configuration shows the dependency of the CSSD resource on the private IP address configured as a MultiPrivNIC resource along with the OCR and voting disk volume and mount point dependencies.

For sample deployment scenarios, see the appendix *SF Oracle RAC deployment scenarios*.

Type definition of the MultiPrivNIC resource

The following extract shows the type definition of the MultiPrivNIC resource in the `MultiPrivNIC.cf` file:

```
type MultiPrivNIC (
        static int MonitorTimeout = 300
        static int OfflineMonitorInterval = 60
        static str ArgList[] = { Device, DeviceTag, Address, NetMask,
                                 UseVirtualIP, GabPort, UseSystemList,
                                 ExcludeNode, UseLoadBalance }
        static str Operations = None
        str Device{}
        str DeviceTag{}
        str Address{}
        str NetMask
        int UseVirtualIP
        str GabPort = o
        int UseSystemList
        int ExcludeNode[]
        int UseLoadBalance
)
```

Sample configuration of the MultiPrivNIC resource

The following extract from the configuration file illustrates the configuration of a MultiPrivNIC resource.

```
MultiPrivNIC multi_priv (
                 Critical = 0
                 Device @galaxy = { lan1= 0, lan2 = 1 }
                 Device @nebula = { lan1= 0, lan2 = 1 }
                 Address @galaxy = { "192.168.12.1" =0, "192.168.2.1" =0,
                                     "192.168.3.1" =1 }
                 Address @nebula = { "192.168.12.2" =0, "192.168.2.2" =0,
                                     "192.168.3.2" =1 }
```

```
NetMask = "255.255.255.0"
)
```

For more examples, see the sample configuration files located at `/etc/VRTSvcs/conf/sample_rac/`.

In the above example, the interface next to the IP address is the preferred device for that particular IP address. If the same number of nodes are visible on each of the LLT interfaces, the IP addresses are configured on the preferred interfaces.

CSSD agent

The CSSD agent starts, stops, and monitors Oracle Clusterware/Grid Infrastructure. It ensures that the OCR, the voting disk and the private IP address resources required by Oracle Clusterware/Grid Infrastructure are online before Oracle Clusterware/Grid Infrastructure starts. For this purpose, the cssd resource must be configured as a parent of the resources that manage the OCR, the voting disk, and the private IP address used by Oracle Clusterware/Grid Infrastructure. Using the CSSD agent in SF Oracle RAC installations ensures adequate handling of inter-dependencies and thus prevents the premature startup of Oracle Clusterware/Grid Infrastructure, which causes cluster failures.

For Oracle RAC 10g Release 2 and Oracle RAC 11g Release 1, during system startup, the Oracle Clusterware init scripts invoke the clsinfo script provided by Veritas software. The clsinfo script ensures that the dependent resources of cssd resource configured under VCS are online, thus ensuring that the OCR, the voting disk, and the private IP address resources are online before the cssd resource comes online. After the underlying resources are online, the CSSD agent starts Oracle Clusterware.

For Oracle RAC 11g Release 2, the automatic startup of Oracle Clusterware/Grid Infrastructure must be disabled when the system starts. This prevents the premature startup of Oracle Clusterware/Grid Infrastructure during system startup. Thus, VCS ensures that Oracle Clusterware/Grid Infrastructure is started using the CSSD agent only when all the dependent resources of the cssd resource configured under VCS are online.

During system shutdown, the agent stops Oracle Clusterware/Grid Infrastructure before the OCR and voting disk resources are taken offline by VCS. This ensures that Oracle Clusterware/Grid Infrastructure does not panic the nodes in the cluster due to unavailability of the required resources.

Note: It is mandatory to use CSSD agent in SF Oracle RAC installations. You must configure the CSSD agent after installing Oracle Clusterware/Grid Infrastructure.

Functions of the CSSD agent

Table H-18 describes the functions of the CSSD agent.

Table H-18 CSSD agent functions

Function	Description
Online	Starts Oracle Clusterware.
Offline	Stops Oracle Clusterware.
Monitor	Checks the status of Oracle Clusterware.

Attributes of the CSSD agent

Table H-19 lists the required attributes of the CSSD agent:

Table H-19 Required attributes for CSSD resource

Attribute Name	Required Value
Critical	0
StartProgram	/opt/VRTSvcs/rac/bin/cssd-online
StopProgram	/opt/VRTSvcs/rac/bin/cssd-offline
CleanProgram	/opt/VRTSvcs/rac/bin/cssd-clean
MonitorProgram	/opt/VRTSvcs/rac/bin/cssd-monitor

States of the CSSD agent

Table H-20 describes the states of the CSSD agent.

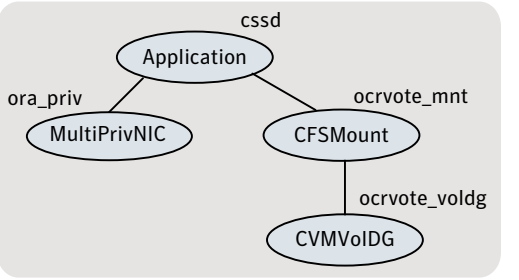
Table H-20 CSSD agent states

State	Description
Online	Indicates that Oracle Clusterware is running.
Offline	Indicates that Oracle Clusterware is not running.
Unknown	Indicates the inability to determine the state of the resource due to incorrect attribute settings or other configuration issues.

Sample service group configurations with the CSSD agent

Figure H-3 illustrates a basic service group configuration with the CSSD agent.

Figure H-3 Basic service group configuration with the CSSD agent



In this basic configuration, the OCR and voting disk volumes/mount points and IP addresses are configured under the CSSD resource. This ensures that these resources are online before the CSSD agent starts Oracle Clusterware.

Note: Depending on whether the Oracle database is started by Oracle Clusterware or by the VCS agent for Oracle, you must configure the Oracle database mounts such that they are online before the database starts.

For more sample configurations:

See "Sample configuration files" on page 610.

Type definition of the CSSD resource

The CSSD agent is an application agent. You can determine the name of the CSSD resource.

The following extract shows the type definition of the CSSD resource in the `types.cf` file.

```
type Application (
        static keylist SupportedActions =
        { "program.vfd", "user.vfd", "cksum.vfd", getcksum }
        static str ArgList[] =
        { User, StartProgram, StopProgram, CleanProgram,
          MonitorProgram, PidFiles, MonitorProcesses }
        static int ContainerOpts{} = { RunInContainer=1, PassCInfo=0 }
        str User
        str StartProgram
```

```
        str StopProgram
        str CleanProgram
        str MonitorProgram
        str PidFiles[]
        str MonitorProcesses[]
)
```

Sample configuration of the CSSD resource

The following extract from the `main.cf` file illustrates a sample CSSD agent configuration:

```
Application cssd (
    Critical = 0
    StartProgram = "/opt/VRTSvcs/rac/bin/cssd-online"
    StopProgram = "/opt/VRTSvcs/rac/bin/cssd-offline"
    CleanProgram = "/opt/VRTSvcs/rac/bin/cssd-clean"
    MonitorProgram = "/opt/VRTSvcs/rac/bin/cssd-monitor"
    )
```

VCS agents for Oracle

The VCS agents for Oracle include the following agents that work together to make Oracle highly available:

- The Oracle agent monitors the Oracle database processes.
  See "Oracle agent functions" on page 693.
  See "Resource type definition for the Oracle agent" on page 699.
- The Netlsnr agent monitors the listener process.
  See "Netlsnr agent functions" on page 705.
- The ASMDG agent monitors the Oracle ASM disk groups.
  See "ASMDG agent functions" on page 711.
  See "Resource type definition for the ASMDG agent" on page 711.

Refer to the *Veritas Cluster Server Agent for Oracle Installation and Configuration Guide* for more details on the agent functions and the resource types.

Oracle agent functions

The Oracle agent monitors the database processes.

Table H-21 lists the Oracle agent functions.

Table H-21 Oracle agent functions

Agent operation	Description
Online	Starts the Oracle database. The agent uses the default startup option STARTUP_FORCE. For RAC clusters, you must manually change the value of the StartUpOpt attribute to SRVCTLSTART. If you set the option to SRVCTLSTART, the agent uses the following `srvctl` command to start the Oracle database: `srvctl start database -d database_name`
Offline	Stops the Oracle database. The agent uses the default shutdown option IMMEDIATE. For RAC clusters, you must manually change the value of the ShutDownOpt attribute to SRVCTLSTOP. If you set the option to SRVCTLSTOP, the agent uses the following `srvctl` command to stop the Oracle database: `srvctl stop database -d database_name`
Monitor	Verifies the status of the Oracle processes. The Oracle agent provides two levels of monitoring: basic and detail. See "Monitor options for the Oracle agent" on page 695.
oracle_imf_init	Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for Oracle agent. This function runs when the agent starts up.
oracle_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.
oracle_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).

Table H-21 Oracle agent functions *(continued)*

Agent operation	Description
Clean	Forcibly stops the Oracle database. If you set the shutdown option to SRVCTLSTOP, the agent uses the following `srvctl` command: `srvctl stop database -d database_name` If the process does not respond to the `srvctl` command, then the agent does the following: ■ Scans the process table for the processes that are associated with the configured instance ■ Kills the processes that are associated with the configured instance
Info	Provides the static and dynamic information about the state of the database. See "Info entry point for SF Oracle RAC agent for Oracle" on page 697.
Action	Performs the predefined actions on a resource. See "Action entry point for SF Oracle RAC agent for Oracle" on page 697.

Monitor options for the Oracle agent

The Oracle agent provides two levels of monitoring: basic and detail. By default, the agent does a basic monitoring.

The basic monitoring mode has the following options:

- Process check
- Health check

The MonitorOption attribute of the Oracle resource determines whether the agent must perform basic monitoring in Process check or Health check mode.

Table H-22 describes the basic monitoring options.

Table H-22 Basic monitoring options

Option	Description
0 (Default)	Process check The agent scans the process table for the ora_dbw0, ora_smon, ora_pmon, and ora_lgwr processes to verify that Oracle is running. In this mode, the agent also supports intelligent resource monitoring.
1	Health check (supported on Oracle 10g and later) The agent uses the Health Check APIs from Oracle to monitor the SGA and retrieve the information about the instance. If you want to use the Oracle agent's intentional offline functionality, you must enable Health check monitoring. The agent does not support intelligent resource monitoring in this mode.

Review the following considerations if you want to configure basic monitoring:

- Basic monitoring of Oracle processes is user-specific. As a result, an Oracle instance started under the context of another user cannot be detected as online. For example, if an Oracle instance is started under the user "oraVRT" and the agent is configured for a user "oracle", the agent will not detect the instance started by "oraVRT" as online.
  This could lead to situations where issuing a command to online a resource on a node might online an already running instance on that node (or any other node).
  So, Symantec recommends that instances started outside SF Oracle RAC control be configured with the correct Owner attribute corresponding to the OS user for that instance.
- Within a failover service group, when the administrator onlines an Oracle resource on a node and if the Oracle instance is online on any other node within a cluster, the instance would come up. However, the database does not get mounted. In such circumstances, this failure is detected only by health check monitoring option of basic monitoring or detail monitoring. Detail monitoring updates the database table after detecting a failure whereas health check monitoring does not.
  If health check monitoring option of basic monitoring or detail monitoring is not configured, then such a conflict would go undetected.

In the detail monitoring mode, the agent performs a transaction on a test table in the database to ensure that Oracle functions properly. The agent uses this test table for internal purposes. Symantec recommends that you do not perform any

other transaction on the test table. The DetailMonitor attribute of the Oracle resource determines whether the agent must perform detail monitoring.

Info entry point for SF Oracle RAC agent for Oracle

The Veritas Cluster Server agent for Oracle supports the Info entry point, which provides static and dynamic information about the state of the database.

To invoke the Info entry point, type the following command:

```
# hares -value resource ResourceInfo [system]\
 [-clus cluster | -localclus]
```

The entry point retrieves the following static information:

- Version
- InstanceNo
- InstanceName
- DatabaseName
- HostName
- StartupTime
- Parallel
- Thread
- InstanceRole

The entry point retrieves the following dynamic information:

- InstanceStatus
- Logins
- OpenMode
- LogMode
- ShutdownPending
- DatabaseStatus
- Shared Pool Percent free
- Buffer Hits Percent

You can add additional attributes by adding sql statements to the file /opt/VRTSagents/ha/bin/Oracle/resinfo.sql. For example:

```
select 'static:HostName:'||host_name from v$instance;
select 'dynamic:ShutdownPending:'||shutdown_pending from
v$instance;
```

The format of the selected record must be as follows:

```
attribute_type:userkey_name:userkey_value
```

The variable *attribute_type* can take the value static and/or dynamic.

Action entry point for SF Oracle RAC agent for Oracle

The Veritas Cluster Server agent for Oracle supports the Action entry point, which enables you to perform predefined actions on a resource.

To perform an action on a resource, type the following command:

```
# hares -action res token [-actionargs arg1 ...] \
[-sys system] [-clus cluster]
```

You can also add custom actions for the agent.

For further information, refer to the *Veritas Cluster Server Agent Developer's Guide*.

See Table H-24 on page 698.

Table H-23 describes the agent's predefined actions.

Table H-23 Predefined agent actions

Action	Description
VRTS_GetInstanceName	Retrieves the name of the configured instance. You can use this option for the Oracle and the Netlsnr resources.
VRTS_GetRunningServices	Retrieves the list of processes that the agent monitors. You can use this option for the Oracle and the Netlsnr resources.
DBRestrict	Changes the database session to enable the RESTRICTED mode.
DBUndoRestrict	Changes the database session to disable the RESTRICTED mode.
DBSuspend	Suspends a database.
DBResume	Resumes a suspended database.
DBTbspBackup	Backs up a tablespace; `actionargs` contains name of the tablespace to be backed up.

Table H-24 lists the virtual fire drill actions of the Veritas Cluster Server agent for Oracle lets you run infrastructure checks and fix specific errors.

Table H-24 Predefined virtual fire drill actions

Virtual fire drill action	Description
getid (Oracle agent)	Verifies that the Oracle Owner exists on the node.

Table H-24 Predefined virtual fire drill actions *(continued)*

Virtual fire drill action	Description
home.vfd (Oracle agent)	Verifies the following: ■ ORACLE_HOME is mounted on the node and corresponding entry is in the fstab. If the ORACLE_HOME is not mounted, the action entry point checks if any other resource has already mounted ORACLE_HOME. ■ Pfile is provided and it exists on the node. ■ Password file from $ORACLE_HOME/dbs/orapw[SID] is present.
owner.vfd (Oracle agent)	Verifies the uid and gid of the Oracle Owner attribute. Checks if uid and gid of Owner attribute is the same on the node where the Oracle resource is currently ONLINE.
pfile.vfd (Oracle agent)	Checks for the presence of pfile or spfile on the local disk. If both pfile and spfile are not present, the agent function exits. If the Oracle resource is online in the cluster, the agent function logs a message that the spfile must be on the shared storage because the Oracle resource is online.
tnsadmin.vfd (Netlsnr agent)	Checks if listener.ora file is present. If the listener.ora file is not present, it checks if ORACLE_HOME is mounted and displays appropriate messages.

Resource type definition for the Oracle agent

The Oracle agent of the Veritas Cluster Server agent for Oracle is represented by the Oracle resource type in SF Oracle RAC.

```
type Oracle (
 static str AgentDirectory = "/opt/VRTSagents/ha/bin/Oracle"
 static keylist SupportedActions = { VRTS_GetInstanceName,
   VRTS_GetRunningServices, DBRestrict, DBUndoRestrict,
   DBResume, DBSuspend, DBTbspBackup, "home.vfd", "owner.vfd",
   "getid", "pfile.vfd" }
 static str ArgList[] = { Sid, Owner, Home, Pfile, StartUpOpt,
   ShutDownOpt, DBAUser, DBAPword,  EnvFile, AutoEndBkup,
   DetailMonitor, User, Pword, Table, MonScript, AgentDebug,
   Encoding, MonitorOption }
 static str IMFRegList[] = { Home, Owner, Sid, MonitorOption }
 str Sid
 str Owner
```

```
 str Home
 str Pfile
 str StartUpOpt = STARTUP_FORCE
 str ShutDownOpt = IMMEDIATE
 str DBAUser
 str DBAPword
 str EnvFile
 boolean AutoEndBkup = 1
 int DetailMonitor = 0
 str MonScript = "./bin/Oracle/SqlTest.pl"
 str User
 str Pword
 str Table
 boolean AgentDebug = 0
 str Encoding
 int MonitorOption = 0
 static boolean IntentionalOffline = 0
)
```

Attribute definition for the Oracle agent

Review the description of the Oracle agent attributes. The agent attributes are classified as required, optional, and internal.

Table H-25 lists the required attributes. You must assign values to the required attributes.

Table H-25 Required attributes for Oracle agent

Required attributes	Type and dimension	Definition
Sid	string-scalar	The variable $ORACLE_SID that represents the Oracle instance. The Sid is considered case-sensitive by the Oracle agent and by the Oracle database server.
Owner	string-scalar	The Oracle user who has privileges to start or stop the database instance. The agent also supports LDAP users as Oracle user.
Home	string-scalar	The $ORACLE_HOME path to Oracle binaries and configuration files. For example, you could specify the path as /opt/ora_home. **Note:** Do not append a slash (/) at the end of the path.

Table H-26 lists the optional attributes for Oracle agent. You can configure the optional attributes if necessary.

Table H-26 Optional attributes for Oracle agent

Optional Attributes	Type and Dimension	Definition
DBAUser	string-scalar	The database user who has sysdba privileges to start or stop the database.
DBAPword	string-scalar	Encrypted password for DBAUser. Encrypt passwords only when entering them using the command-line. Passwords must be encrypted using the SF Oracle RAC Encrypt utility.
StartUpOpt	string-scalar	Startup options for the Oracle instance. This attribute can take the following values: ■ STARTUP ■ STARTUP_FORCE ■ RESTRICTED ■ RECOVERDB ■ SRVCTLSTART ■ CUSTOM Default is STARTUP_FORCE.
ShutDownOpt	string-scalar	Shut down options for the Oracle instance. This attribute can take the following values: ■ IMMEDIATE ■ TRANSACTIONAL ■ SRVCTLSTOP ■ CUSTOM Default is IMMEDIATE.
EnvFile	string-scalar	The full path name of the file that is sourced by the entry point scripts. This file contains the environment variables set by the user for the Oracle database server environment such as LD_LIBRARY_PATH, NLS_DATE_FORMAT, and so on. The syntax for the contents of the file depends on the login shell of Owner. File must be readable by Owner. The file must not contain any prompts for user input.
Pfile	string-scalar	The name of the initialization parameter file with the complete path of the startup profile. You can also use the server parameter file. Create a one-line text initialization parameter file that contains only the SPFILE parameter. See the Oracle documentation for more information.

Table H-26 Optional attributes for Oracle agent *(continued)*

Optional Attributes	Type and Dimension	Definition
AutoEndBkup	integer-scalar	Setting the AutoEndBkup attribute to a non-zero value takes the datafiles in the database out of the backup mode, during Online. Default = 1
MonitorOption	integer-scalar	Monitor options for the Oracle instance. This attribute can take values 0 or 1. ■ 0—Process check monitoring (recommended) ■ 1—Health check monitoring The agent supports intelligent resource monitoring only when this attribute value is set to 0. Default = 0 See "Monitor options for the Oracle agent" on page 695.

Table H-26 Optional attributes for Oracle agent *(continued)*

Optional Attributes	Type and Dimension	Definition
IMF	integer-association	This resource-type level attribute determines whether the Oracle agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 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: ■ 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 oracle_imf_register agent function to register the resource with the AMF kernel 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.

Table H-26 Optional attributes for Oracle agent *(continued)*

Optional Attributes	Type and Dimension	Definition
DetailMonitor	integer-scalar	Determines whether or not detail monitoring is enabled. The attribute value 1 indicates that detail monitoring for Oracle is enabled. You must set the value of the LevelTwoMonitorFreq attribute to specify the frequency at which the agent must perform detailed monitoring. Default = 0
MonScript	string-scalar	Pathname to the script provided for detail monitoring. The default (basic monitoring) is to monitor the database PIDs only. **Note:** Detail monitoring is disabled if the value of the attribute MonScript is invalid or is set to an empty string. The pathname to the supplied detail monitor script is /opt/VRTSagents/ha/bin/Oracle/SqlTest.pl. MonScript also accepts a pathname relative to /opt/VRTSagents/ha. A relative pathname should start with "./", as in the path ./bin/Oracle/SqlTest.pl.
User	string-scalar	Internal database user. Connects to the database for detail monitoring.
LevelTwo MonitorFreq	integer-scalar	Specifies the frequency at which the agent for this resource type must perform second-level or detailed monitoring. You can also override the value of this attribute at resource-level. The value indicates the number of monitor cycles after which the agent will monitor Oracle in detail. For example, the value 5 indicates that the agent will monitor Oracle in detail every five online monitor intervals. If you manually upgraded to the SF Oracle RAC 5.1 SP1 agent, and if you had enabled detail monitoring in the previous version, then do the following: ■ Set the value of the LevelTwoMonitorFreq attribute to the same value of that of the DetailMonitor attribute. ■ Reset the value of the DetailMonitor attribute to 1 **Note:** If you set the AutoEndBkup attribute value to 0, then make sure that the LevelTwoMonitorFreq attribute value is 1 for detail monitoring. Default = 0
Pword	string-scalar	Encrypted password for internal database-user authentication. Encrypt passwords only when entering them using the command-line. Passwords must be encrypted using the SF Oracle RAC Encrypt utility.

Table H-26 Optional attributes for Oracle agent *(continued)*

Optional Attributes	Type and Dimension	Definition
Table	string-scalar	Table for update by `User/Pword`.
Encoding	string-scalar	Specifies operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. Default is "".
IntentionalOffline		This resource-type level attribute defines how VCS reacts when Oracle is intentionally stopped outside of VCS control. If you stop Oracle out of VCS control, the agent behavior is as follows: ■ 0—The Oracle agent registers a fault and initiates the failover of the service group. ■ 1—The Oracle agent takes the Oracle resource offline when Health check monitoring is enabled. If Health check monitoring is not enabled, the agent registers a fault and initiates the failover of the service group. **Note:** If you want to use the intentional offline functionality of the agent, you must set the value of the MonitorOption attribute as 1 to enable Health check monitoring. See the *Veritas Cluster Server Administrator's Guide*.
AgentDebug	boolean-scalar	Additional debug messages are logged when this flag is set. Default = 0

Table H-27 lists the internal attribute for Oracle agent. This attribute is for internal use only. Symantec recommends not to modify the value of this attribute.

Table H-27 Internal attributes for Oracle agent

Optional Attributes	Type and Dimension	Definition
AgentDirectory	static-string	Specifies the location of binaries, scripts, and other files related to the Oracle agent. Default is /opt/VRTSagents/ha/bin/Oracle.

Netlsnr agent functions

The Netlsnr agent is IMF-aware.

The listener is a server process that listens to incoming client connection requests and manages traffic to the database. The Netlsnr agent brings the listener services online, monitors their status, and takes them offline.

Table H-28 lists the Netlsnr agent functions.

Table H-28 Netlsnr agent functions

Agent operation	Description
Online	Starts the listener process by using the following command: `lsnrctl start $LISTENER`
Offline	Stops the listener process by using the following command: `lsnrctl stop $LISTENER` If the listener is configured with a password, the agent uses the password to stop the listener.
Monitor	Verifies the status of the listener process. The Netlsnr agent provides two levels of monitoring, basic and detail: ■ In the basic monitoring mode, the agent scans the process table for the `tnslsnr` process to verify that the listener process is running. ■ In the detail monitoring mode, the agent uses the `lsnrctl status $LISTENER` command to verify the status of the Listener process. (Default)
netlsnr_imf_init	Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for Netlsnr agent. This function runs when the agent starts up.
netlsnr_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.
netlsnr_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).
Clean	Scans the process table for `tnslsnr $LISTENER` and kills it.
Action	Performs the predefined actions on a resource. See "Action entry point for SF Oracle RAC agent for Oracle" on page 697.

Resource type definition for the Netlsnr agent

The Netlsnr agent of the Veritas Cluster Server agent for Oracle is represented by the Netlsnr resource type in SF Oracle RAC.

```
type Netlsnr (
 static str AgentDirectory = "/opt/VRTSagents/ha/bin/Netlsnr"
 static keylist SupportedActions = { VRTS_GetInstanceName,
   VRTS_GetRunningServices, "tnsadmin.vfd" }
 static str ArgList[] = { Owner, Home, TnsAdmin, Listener,
   EnvFile, MonScript, LsnrPwd, AgentDebug, Encoding }
 static str IMFRegList[] = { Home, Owner, Listener }
 str Owner
 str Home
 str TnsAdmin
 str Listener
 str EnvFile
 str MonScript = "./bin/Netlsnr/LsnrTest.pl"
 str LsnrPwd
 boolean AgentDebug = 0
 str Encoding
 static boolean IntentionalOffline = 0
)
```

Attribute definition for the Netlsnr agent

Review the description of the Netlsnr agent attributes. The agent attributes are classified as required, optional, and internal.

Table H-29 lists the required attributes for Netlsnr agent. You must assign values to the required attributes.

Table H-29 Required attributes for Netlsnr agent

Required attributes	Type and dimension	Definition
Owner	string-scalar	The Oracle user who has privileges to start or stop the listener process. The agent also supports LDAP users as Oracle user.
Home	string-scalar	The $ORACLE_HOME path to Oracle binaries and configuration files. For example, you could specify the path as /opt/ora_home. Do not append a slash (/) at the end of the path.

Table H-30 lists the optional attributes for Netlsnr agent. You can configure the optional attributes if necessary.

Table H-30 Optional attributes for Netlsnr agent

Optional attributes	Type and dimension	Definition
TnsAdmin	string-scalar	The $TNS_ADMIN path to directory in which the Listener configuration file resides (listener.ora). Default is /var/opt/oracle.
Listener	string-scalar	Name of Listener. The name for Listener is considered case-insensitive by the Netlsnr agent and the Oracle database server. Default is LISTENER.
LsnrPwd	string-scalar	The SF Oracle RAC encrypted password used to stop and monitor the listener. This password is set in the Listener configuration file. Encrypt passwords only when entering them using the command-line. Passwords must be encrypted using the SF Oracle RAC Encrypt utility.
EnvFile	string-scalar	Specifies the full path name of the file that is sourced by the entry point scripts. This file contains the environment variables set by the user for the Oracle listener environment such as LD_LIBRARY_PATH and so on. The syntax for the contents of the file depends on the login shell of Owner. This file must readable by Owner. The file must not contain any prompts for user input.

Table H-30 Optional attributes for Netlsnr agent *(continued)*

Optional attributes	Type and dimension	Definition
IMF	integer-association	This resource-type level attribute determines whether the Netlsnr agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 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 attribute to a non-zero value in some cases where the agent requires to perform poll-based resource monitoring in addition to the intelligent resource monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: ■ 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 netlsnr_imf_register agent function to register the resource with the AMF kernel 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.

Table H-30 Optional attributes for Netlsnr agent *(continued)*

Optional attributes	Type and dimension	Definition
MonScript	string-scalar	Pathname to the script provided for detail monitoring. By default, the detail monitoring is enabled to monitor the listener process. **Note:** If the value of the attribute MonScript is set to an empty string, the agent disables detail monitoring. The pathname to the supplied detail monitoring script is /opt/VRTSagents/ha/bin/Netlsnr/LsnrTest.pl. MonScript also accepts a pathname relative to /opt/VRTSagents/ha. A relative pathname should start with "./", as in the path ./bin/Netlsnr/LsnrTest.pl.
LevelTwo MonitorFreq	integer-scalar	Specifies the frequency at which the agent for this resource type must perform second-level or detailed monitoring. If you enabled detail monitoring, then set the value of the LevelTwoMonitorFreq attribute. Default = 0
Encoding	string-scalar	Specifies operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. Default is "".
IntentionalOffline		For future use. Do not change the value of this attribute. Default = 0
AgentDebug	boolean	Additional debug messages are logged when this flag is set. Default = 0

Table H-31 lists the internal attribute for Netlsnr agent. This attribute is for internal use only. Symantec recommends not to modify the value of this attribute.

Table H-31 Internal attributes for Netlsnr agent

Optional Attributes	Type and Dimension	Definition
AgentDirectory	static-string	Specifies the location of binaries, scripts, and other files related to the Netlsnr agent. Default is /opt/VRTSagents/ha/bin/Netlsnr.

ASMDG agent functions

The ASMDG agent mounts the ASM disk groups that the Oracle databases use, monitors the status, unmounts the ASM disk groups.

You must have specified the disk group names in the DiskGroups attribute of the ASMDG agent.

Table H-32 lists the ASMDG agent operations.

Table H-32 ASMDG agent operations

Agent operation	Description
Online	Mounts the specified Oracle ASM disk groups to an ASM instance by using the following SQL command: `alter diskgroup dg_name1, dg_name2 mount`
Offline	Unmounts the specified Oracle ASM disk groups from an ASM instance by using the following SQL command: `alter diskgroup dg_name1, dg_name2 dismount` **Note:** The following Oracle message appears in the VCS log when an ASM instance with no ASM disk groups mounted is shut down: ORA-15100: invalid or missing diskgroup name
Monitor	Verifies the status of the specified ASM disk groups. The disk groups can be in one of the following states: ■ mounted ■ dismounted ■ unknown ■ broken ■ connected If multiple ASM disk groups are configured for a resource, then the ASMDG agent returns the resource state considering the status of all the specified ASM disk groups.
Clean	Forcibly unmounts the Oracle ASM disk groups by using the following SQL command: `alter diskgroup dg_name1, dg_name2 dismount force`

Resource type definition for the ASMDG agent

The ASMDG agent of the Veritas Cluster Server agent for Oracle is represented by the ASMDG resource type in SF Oracle RAC.

```
type ASMDG (
 static str AgentDirectory = "/opt/VRTSagents/ha/bin/ASMDG"
 static str ArgList[] = { Sid, Owner, Home, DBAUser,
   DBAPword, DiskGroups, EnvFile, Encoding }
 str Sid
 str Owner
 str Home
 str DBAUser
 str DBAPword
 keylist DiskGroups
 str EnvFile
 str Encoding
)
```

Attribute definition for the ASMDG agent

Review the description of the ASMDG agent attributes. The agent attributes are classified as required, optional, and internal.

Table H-33 lists the required attributes. You must assign values to the required attributes.

Table H-33 Required attributes for ASMDG agent

Required attributes	Type and dimension	Definition
DiskGroups	keylist	The ASM disk groups, where you store the Oracle database files.
Sid	string-scalar	The variable $ORACLE_SID that represents the ASM instance.
Owner	string-scalar	The Oracle user who has privileges to mount or unmount the ASM disk group. The agent also supports LDAP users as Oracle user.
Home	string-scalar	The $ORACLE_HOME path to Oracle ASM binaries and configuration files. For example, you could specify the path as /opt/ora_home. **Note:** Do not append a slash (/) at the end of the path.

Table H-34 lists the optional attributes for ASMDG agent. You can configure the optional attributes if necessary.

Table H-34 Optional attributes for ASMDG agent

Optional Attributes	Type and Dimension	Definition
DBAUser	string-scalar	The ASM user who has sysasm privileges to start or stop the ASM instance. You can create ASM users for Oracle 11g R1 and later.
DBAPword	string-scalar	Encrypted password for DBAUser. Encrypt passwords only when entering them using the command-line. Passwords must be encrypted using the SF Oracle RAC Encrypt utility.
EnvFile	string-scalar	The full path name of the file that is sourced by the entry point scripts. This file contains the environment variables set by the user for the Oracle database server environment such as LD_LIBRARY_PATH, NLS_DATE_FORMAT, and so on. The syntax for the contents of the file depends on the login shell of Owner. File must be readable by Owner. The file must not contain any prompts for user input.
Encoding	string-scalar	Specifies operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. Default is "".

Table H-35 lists the internal attribute for ASMDG agent. This attribute is for internal use only. Symantec recommends not to modify the value of this attribute.

Table H-35 Internal attributes for ASMDG agent

Optional Attributes	Type and Dimension	Definition
AgentDirectory	static-string	Specifies the location of binaries, scripts, and other files related to the ASMDG agent. Default is /opt/VRTSagents/ha/bin/ASMDG.

CRSResource agent

The `CRSResource` agent provides an alternative mechanism for monitoring the Oracle database in the absence of the VCS Oracle agent. It checks the status of the Oracle Clusterware resources, which include the Oracle database instance, the listener, and the virtual IP address (VIP). The agent supports multiple database configurations and ensures that the Oracle database is online and available to an application when it starts.

Functions of the CRSResource agent

Table H-36 describes the functions of the CRSResource agent.

Table H-36 CRSResource agent entry points

Entry point	Description
Monitor	Checks the status of the following Oracle Clusterware resources: ■ Oracle database ■ Virtual IP address ■ Listener The monitor script checks the status of the resources every 60 seconds.
Online	A dummy entry point that uses a delay interval to ensure that the Oracle Clusterware resources come online before the monitor operation begins.

States of the CRSResource agent

Table H-37 lists the states of the CRSResource agent.

Table H-37 States of the CRSResource agent

State	Description
Online	Indicates that the Oracle database, VIP, and listener are running.
Faulted	Indicates that the Oracle database, VIP, and listener are not running or are faulted.
Unknown	Indicates the inability to determine the state of the resource due to incorrect attributes settings or other configuration issues.

Attributes of the CRSResource agent

Table H-38 Attributes of the CRSResource agent

Attribute	Dimension	Description
ResType	string-scalar	Indicates the type of the Oracle Clusterware resource. The types of resources are as follows: ■ DB ■ VIP ■ Listener
DBHome	string-scalar	The path to ORACLE_HOME containing the Oracle binaries and configuration files. For example, you could specify the path as /app/oracle/orahome. **Note:** Do not append a slash (/) at the end of the path.
CRSHome	string-scalar	The path to CRS_HOME containing the Oracle Clusterware binaries.
DBName	string-scalar	The name of the database on which the services are configured. This attribute is optional if you are configuring CRSResource to monitor VIP or listener.
SID	string-scalar	The name of the Oracle instance in the variable $ORACLE_SID. The SID is case-sensitive. This attribute is optional if you are configuring CRSResource to monitor VIP or listener.

Table H-38 Attributes of the CRSResource agent *(continued)*

Attribute	Dimension	Description
Owner	string-scalar	The name of the user for the Oracle database. This attribute is optional if you are configuring CRSResource to monitor VIP or listener.

VCS service group dependencies with the CRSResource agent

In a service group configuration with the CRSResource agent, Oracle Clusterware controls the database. An online local firm dependency exists between the groups—Application group, Oracle Clusterware group, and the CVM group.

Figure H-4 shows a schematic illustration of the service group dependencies.

Figure H-4 Service group dependencies with CRSResource agent

In the configuration:

- When the system starts, the CVM group brings up the volume and mount points for the databases. The Oracle Clusterware group brings up the OCR and voting disk, configures the private IP address for Oracle Clusterware, and starts Oracle Clusterware. Oracle Clusterware starts the database and the application is brought online. CRSResource comes online when the Oracle Clusterware resources (database/VIP/listener) are started by Oracle Clusterware.

  Note: When the system starts, all volumes and mount points MUST be online for the dependent service groups to be online.

- The oradata_mnt and oradata_voldg resources are configured as non-critical resources (critical=0) for managing failure scenarios.
  See "How CRSResource agent handles failures" on page 718.
- When CRSResource faults for any of the Oracle Clusterware resources, the application is brought offline.

The limitations of this configuration are as follows:

- The CFSMount and CVMVolDg resources can not be set as critical resources in the group.
  If the mount points and volume disk groups for all the databases are configured as critical in a single service group, then failure of any of them results in the whole group being FAULTED or brought offline. To ensure that a resource failure does not affect other resources in the group, the attribute Critical is set to zero for the CFSMount and CVMVolDg resources.
  However, if any of the database mounts fail to come online or a volume does not start, the whole service group fails to come online.
- CRSResource reports as FAULTED until Oracle Clusterware brings up the database instance, VIP, and listener. Even after Oracle Clusterware starts the database instance, VIP and listener, CRSResource remains in the FAULTED state for the OfflineMonitorInterval period. The status of CRSResource cannot be changed.

How CRSResource agent handles failures

The CRSResource agent ensures that faults in the resources of an application do not adversely impact other applications running on the system. To isolate failures, the oradata_mnt and oradata_voldg resources are configured as non-critical resources (critical=0). This ensures that storage issues in either of these resources do not affect the other databases and the dependent application continues to be online.

Note: The resources are considered non-critical only for the purpose of managing failure scenarios.

Figure H-5 illustrates a failure scenario.

Figure H-5 How CRSResource agent handles failures

Fault configurations with CRSResource agent

This section discusses scenarios that cause CRSResource to report FAULTED.

Scenario 1: CRSResource fault at system startup

1. The CVM group brings online the volume and mount points for the databases when the system starts.
2. The Oracle Clusterware group brings up the OCR and voting disk, configures the private IP address for Oracle Clusterware and starts Oracle Clusterware.

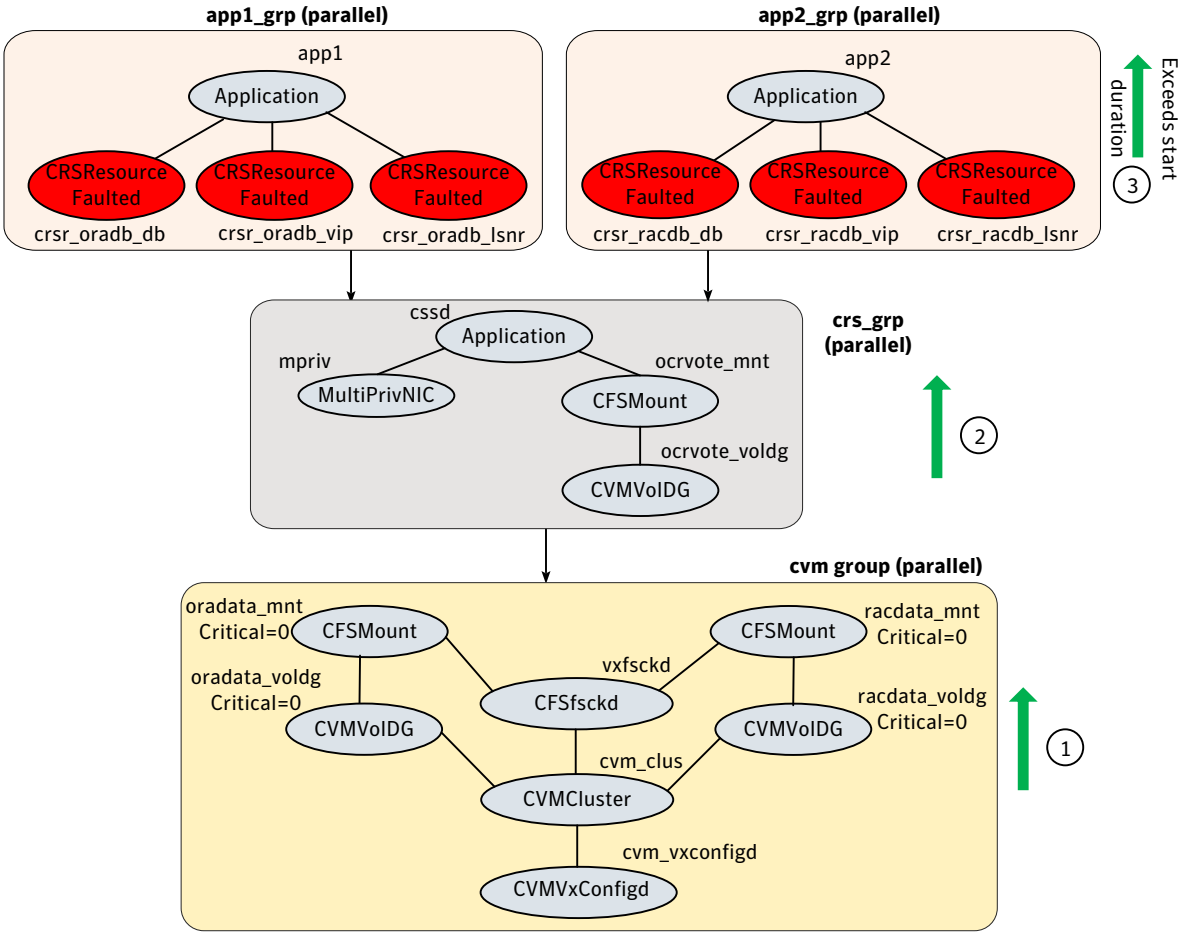
Oracle Clusterware is unable to bring the database or other resources online within the start duration configured in the agent.

3. The agent starts the monitoring operation after the set duration.

   If the Oracle Clusterware resources are not brought online yet, the CRSResource appears faulted.

Figure H-6 illustrates the scenario.

Figure H-6 CRSResource fault at system startup



Scenario 2: CRSResource fault when resource is brought offline

Any or all of the Oracle Clusterware resources (database, listener, or VIP) are brought offline due to a fault or for administrative purposes.

CRSResource reports FAULTED until Oracle Clusterware brings the resources online.

Resource type definition for the CRSResource agent

The following extract from the `CRSResource.cf` file describes the type definition for the CRSResource agent.

```
type CRSResource (
     static int MonitorTimeout = 300
     static int OfflineMonitorInterval = 60
     static str ArgList[] = { ResType, DBHome, CRSHome, DBName, SID, Owner
     static str Operations = None
     str ResType
     str DBHome
     str CRSHome
     str DBName
     str SID
     str Owner
)
```

Sample configuration for the CRSResource agent

The following sample configuration describes the DB, VIP, and Listener resource configurations for the CRSResource agent.

```
CRSResource crsr_oradb_db (
    ResType = DB
    DBHome = "/app/oracle/orahome"
    CRSHome = "/app/crshome"
    DBName = oradb
    SID @galaxy = oradb1
    SID @nebula = oradb2
    Owner = oracle
    )
CRSResource crsr_oradb_vip (
    ResType = VIP
    DBHome = "/app/oracle/orahome"
    CRSHome = "/app/crshome"
    )
```

```
CRSResource crsr_oradb_lsnr (
    ResType = Listener
    DBHome = "/app/oracle/orahome"
    CRSHome = "/app/crshome"
    )
```

Appendix I

SF Oracle RAC deployment scenarios

This appendix includes the following topics:

- SF Oracle RAC cluster with VCS IPC and PrivNIC agent
- SF Oracle RAC cluster with UDP IPC and PrivNIC agent
- SF Oracle RAC cluster for multiple databases with UDP IPC and MultiPrivNIC agent
- SF Oracle RAC cluster with isolated Oracle traffic and MultiPrivNIC agent
- SF Oracle RAC cluster with NIC bonding, VCS IPC and PrivNIC agent
- SF Oracle RAC cluster with NIC bonding, UDP IPC, and PrivNIC agent
- Configuration diagrams for setting up server-based I/O fencing
- Deploying Storage Foundation for Databases (SFDB) tools in a Storage Foundation for Oracle RAC environment

SF Oracle RAC cluster with VCS IPC and PrivNIC agent

This section illustrates the recommended configuration for the following scenario:

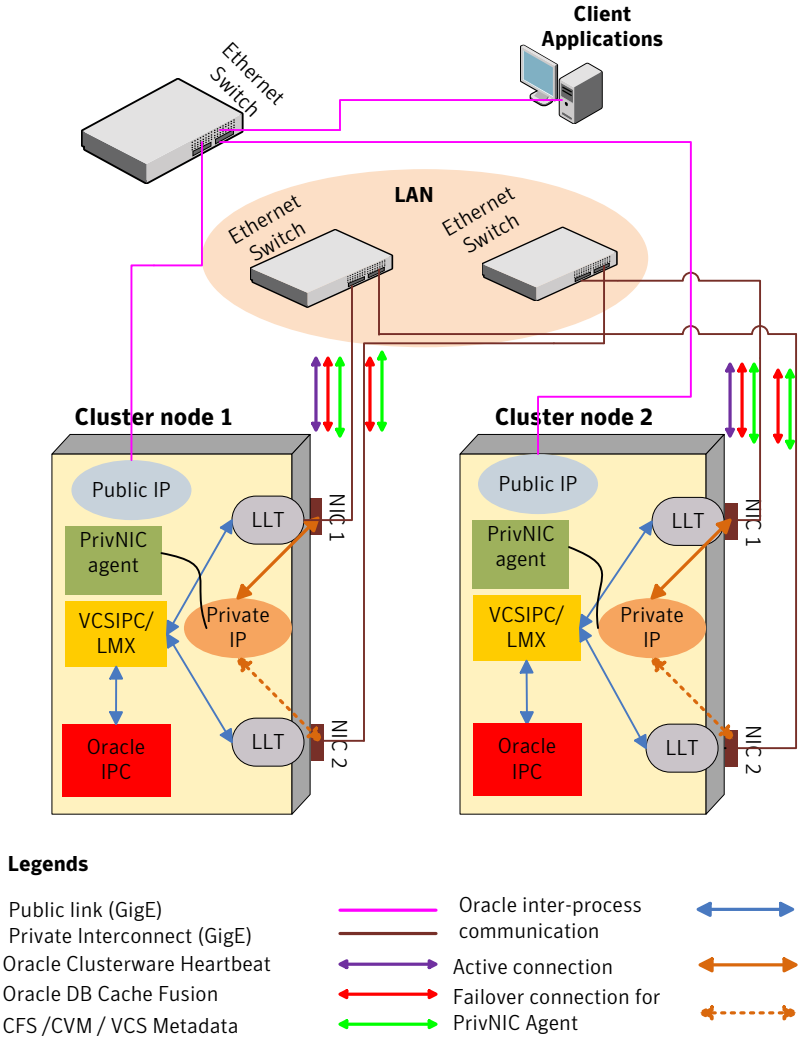
Deployment scenario	Oracle RAC 10g database cache fusion traffic is distributed over multiple LLT links using VCS IPC over LMX/LLT.
Recommendation	Use the PrivNIC agent.
Sample main.cf configuration file	The following sample main.cf file describes the configuration: `/etc/VRTSvcs/conf/sample_rac/sfrac01_main.cf`

In the illustrated configuration:

- Oracle uses VCS IPC over LMX/LLT for cache fusion.
- One private network IP address is used for Oracle Clusterware communication that takes place over one of the LLT private interconnect links.
- The CFS/CVM/VCS metadata and the Oracle database cache fusion traffic travels through LLT over the two physical links that are configured as LLT links.
- In the event of a NIC failure or link failure, the PrivNIC agent fails over the private network IP address from the failed link to the available LLT link. When the link is restored, the IP address is failed back to the original link.

Figure I-1 illustrates the logical view of a two-node SF Oracle RAC cluster with VCS IPC and PrivNIC agent (Oracle RAC 10g).

Figure I-1 SF Oracle RAC cluster with VCS IPC and PrivNIC agent (Oracle RAC 10g)



SF Oracle RAC cluster with UDP IPC and PrivNIC agent

This section illustrates the recommended configuration for the following scenario:

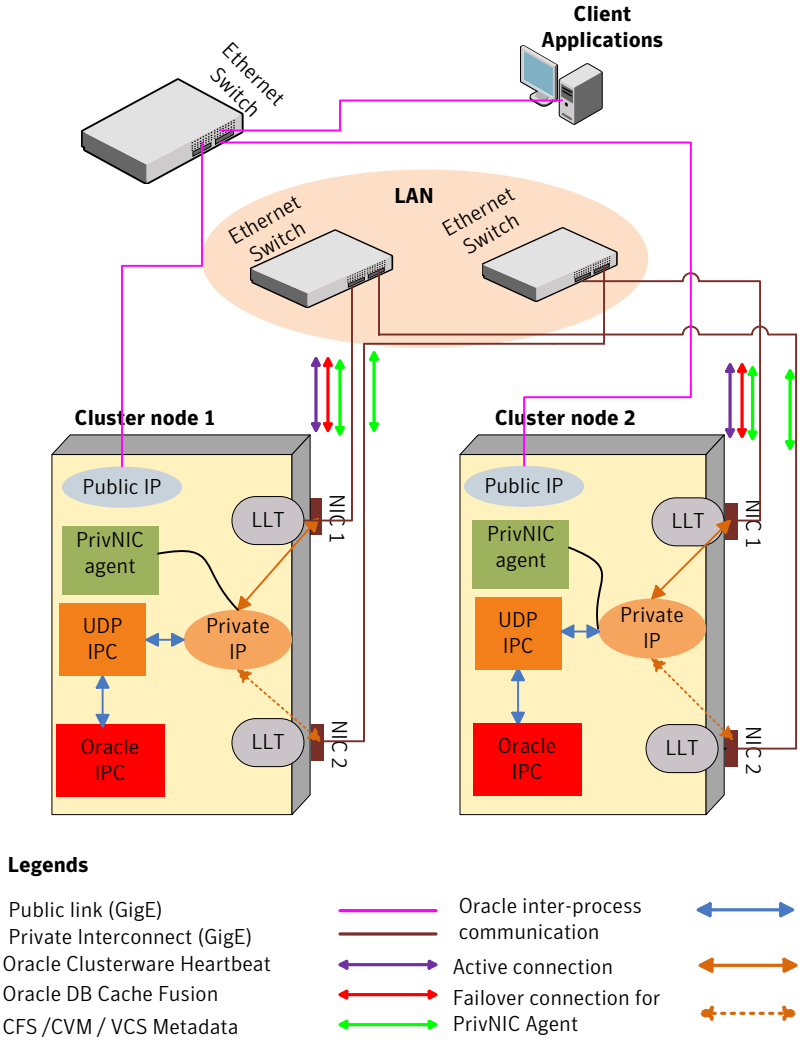
Deployment scenario	Oracle RAC configured with UDP IPC for database cache fusion.
Recommendation	Use the PrivNIC agent.
Sample main.cf configuration file	The following sample main.cf file describes the configuration: `/etc/VRTSvcs/conf/sample_rac/sfrac02_main.cf`

In the illustrated configuration:

- A common IP address is used for Oracle Clusterware communication and Oracle database cache fusion.
- Oracle Clusterware communication and Oracle database cache fusion traffic flows over one of the LLT private interconnect links.
- The CFS/CVM/VCS metadata travels through LLT over the two physical links that are configured as LLT links.
- In the event of a link failure, the PrivNIC agent fails over the private network IP address from the failed link to the available LLT link. When the link is restored, the IP address is failed back to the original link.

Figure I-2 illustrates the logical view of a two-node SF Oracle RAC cluster with UDP IPC and PrivNIC agent.

Figure I-2 SF Oracle RAC cluster with UDP IPC and PrivNIC agent



SF Oracle RAC cluster for multiple databases with UDP IPC and MultiPrivNIC agent

This section illustrates the recommended configuration for the following scenario:

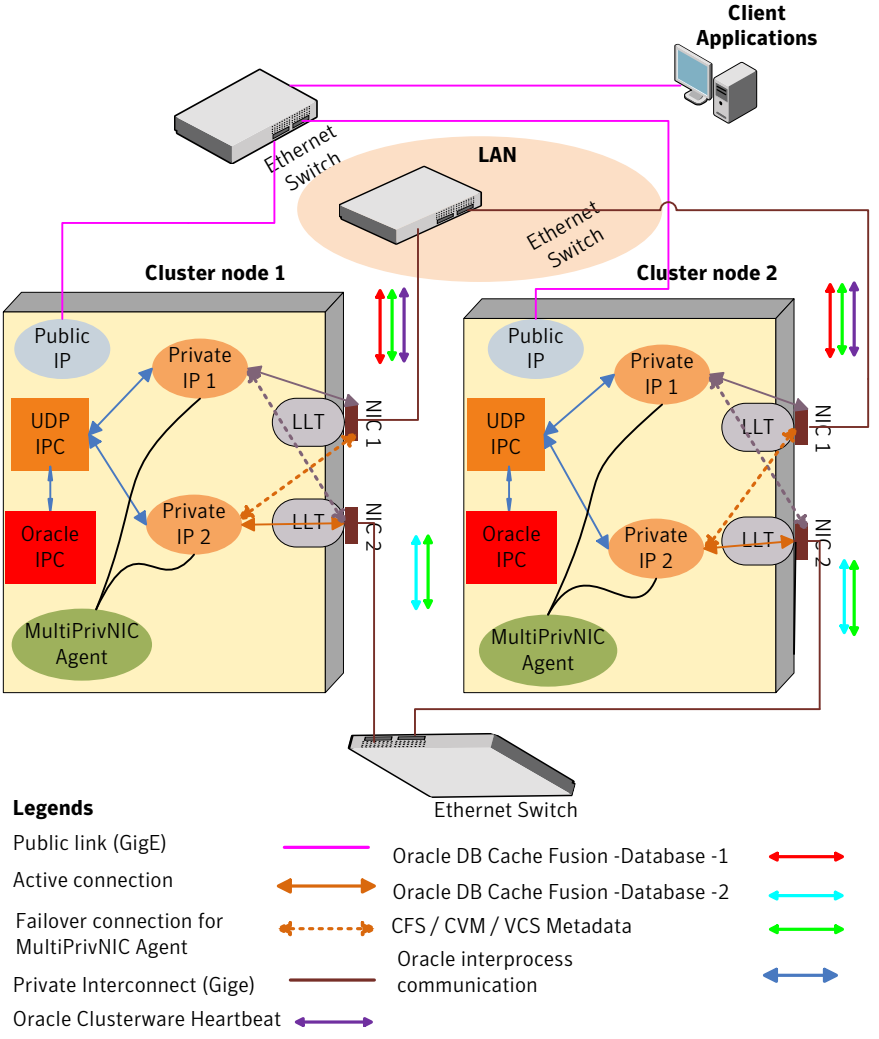
Deployment scenario	Oracle RAC is configured with UDP IPC for database cache fusion.
Recommendation	Use the MultiPrivNIC agent.
Sample main.cf configuration file	The following sample main.cf file describes the configuration: `/etc/VRTSvcs/conf/sample_rac/sfrac03_main.cf`

In the illustrated configuration:

- One private IP address is used for each database for database cache fusion. One of the private IP addresses used for the database cache fusion is shared by Oracle Clusterware communication.
  The CFS/CVM/VCS metadata also travels through these links.
- In the event of a link failure, the MultiPrivNIC agent fails over the private network IP address from the failed link to the available LLT link. When the link is restored, the IP address is failed back to the original link.

Figure I-3 illustrates the logical view of a two-node SF Oracle RAC cluster for multiple databases with UDP IPC and MultiPrivNIC agent.

Figure I-3 SF Oracle RAC cluster for multiple databases with UDP IPC and MultiPrivNIC agent



SF Oracle RAC cluster with isolated Oracle traffic and MultiPrivNIC agent

This section illustrates the recommended configuration for the following scenario:

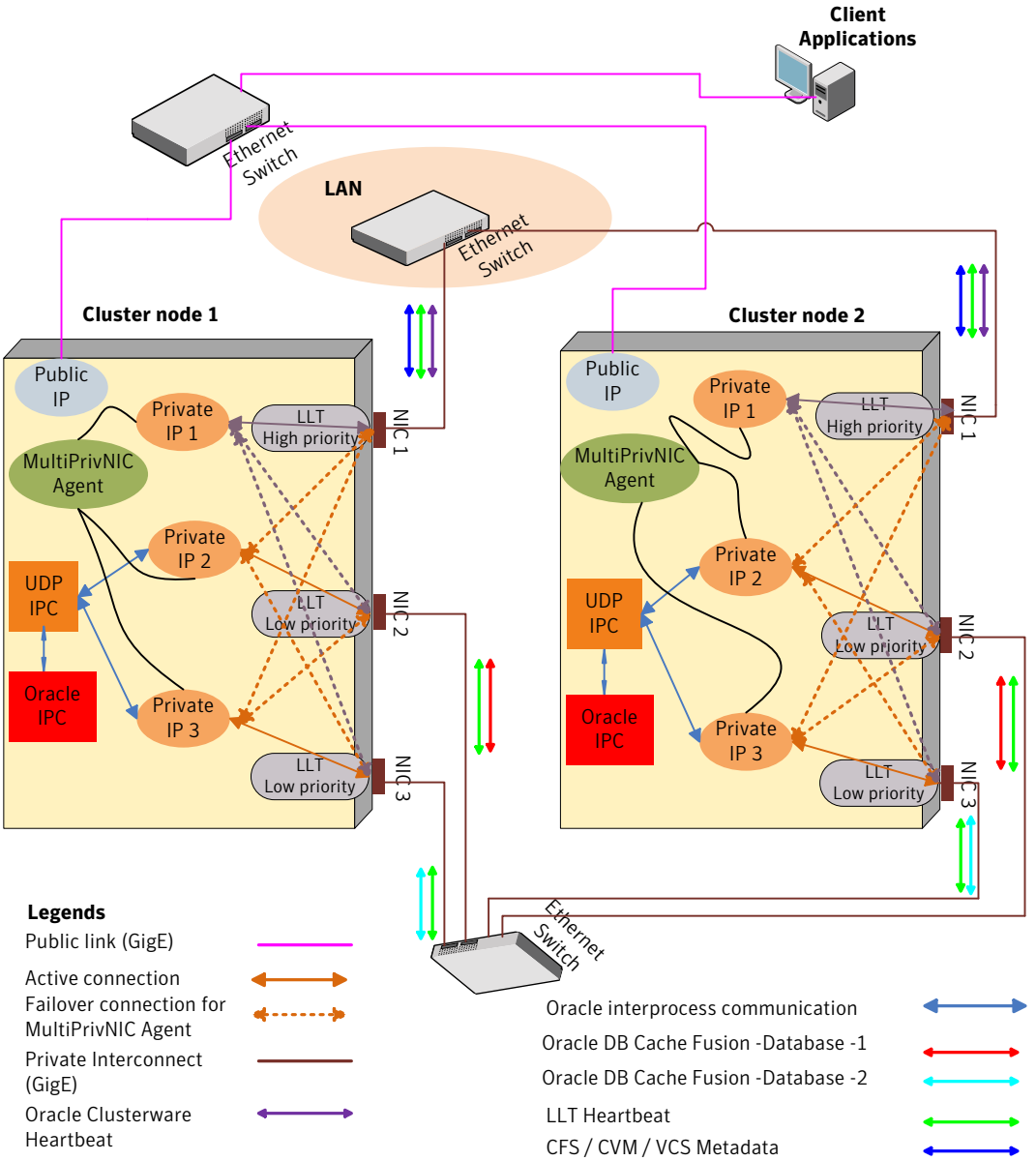
Deployment scenario	Oracle RAC database cache fusion traffic is isolated from the CFS/CVM/VCS metadata.
Recommendation	Use the MultiPrivNIC agent.
Sample main.cf configuration file	The following sample main.cf file describes the configuration: `/etc/VRTSvcs/conf/sample_rac/sfrac06_main.cf`

In the illustrated configuration:

- The private network IP address used for database cache fusion is configured over a dedicated link for each database. These links are configured as low-priority LLT links.
- The private network IP address used for Oracle Clusterware communication is configured over a high-priority LLT link. This link is also used for the CFS/CVM/VCS metadata transfer.
- In the event of a link failure, the MultiPrivNIC agent fails over the private network IP address from the failed link to the available LLT link. When the link is restored, the IP address is failed back to the original link.

Figure I-4 illustrates the logical view of a two-node SF Oracle RAC cluster with Oracle traffic isolated from VCS / CVM / CFS traffic.

Figure I-4 SF Oracle RAC cluster with isolated Oracle traffic and MultiPrivNIC agent



SF Oracle RAC cluster with NIC bonding, VCS IPC and PrivNIC agent

This section illustrates the recommended configuration for the following scenario:

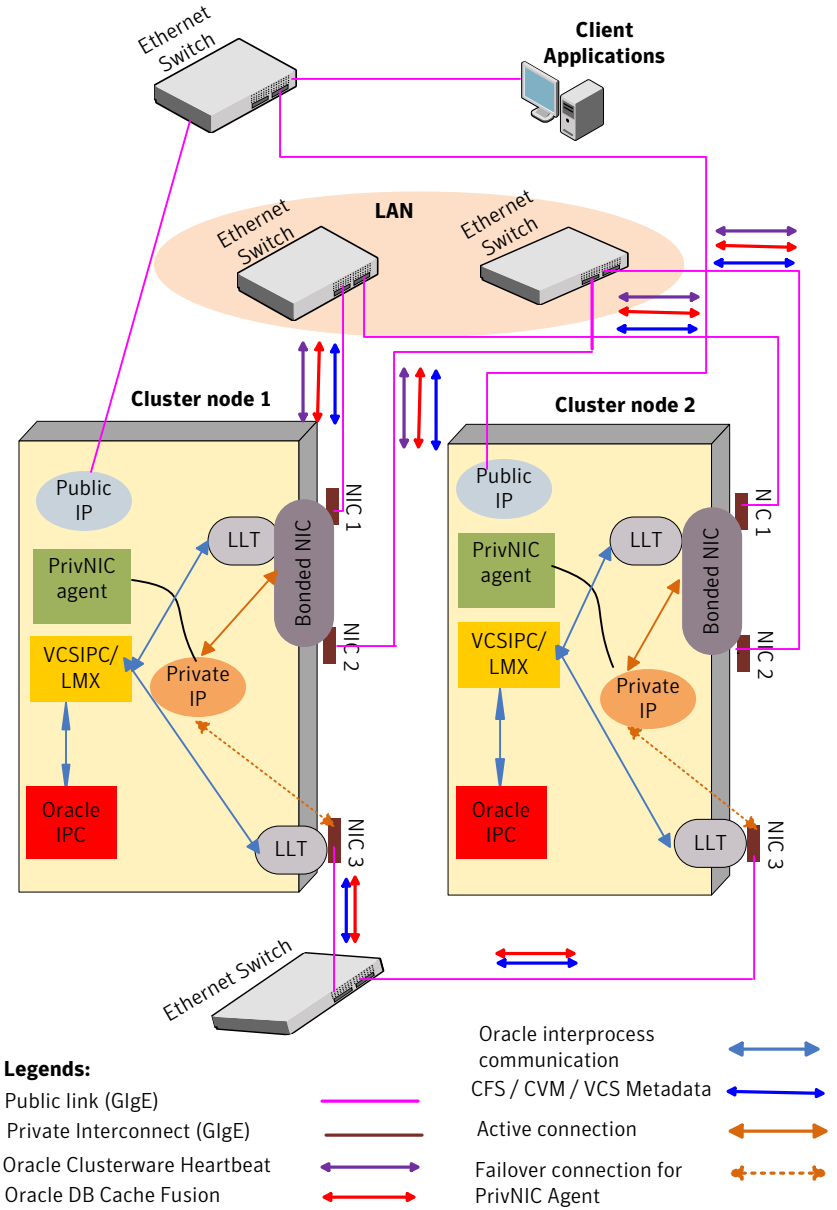
Deployment scenario	A bonded NIC interface is used along with another NIC interface to distribute Oracle RAC 10g database cache fusion traffic using VCS IPC over LMX/LLT.
Recommendation	Use the PrivNIC agent.
Sample main.cf configuration file	The following sample main.cf file describes the configuration: `/etc/VRTSvcs/conf/sample_rac/sfrac01_main.cf` **Note:** You must replace the lan1 interface in the sample file with the bonded NIC interface you use in the scenario and lan2 in the sample file with the NIC3 interface in the scenario.

In the illustrated configuration:

- Oracle uses VCS IPC over LMX/LLT for cache fusion.
- One common private network IP address is used for Oracle database cache fusion and Oracle Clusterware communication that takes place over the bonded NIC interface, configured as an LLT link.
- The Oracle Clusterware communication takes place over the other LLT private interconnect link.
- The Oracle database cache fusion as well as the CFS/CVM/VCS metadata travels through LLT over the three physical links.
- In the event of a bonded NIC interface failure, the PrivNIC agent fails over the private network IP address from the failed link to the other available LLT link. When the link is restored, the IP address is failed back to the original link.

Figure I-5 illustrates the logical view of a two-node SF Oracle RAC cluster with NIC bonding, VCS IPC, and PrivNIC agent (Oracle RAC 10g).

Figure I-5 SF Oracle RAC cluster with NIC bonding, VCS IPC and PrivNIC agent (Oracle RAC 10g)



SF Oracle RAC cluster with NIC bonding, UDP IPC, and PrivNIC agent

This section illustrates the recommended configuration for the following scenario:

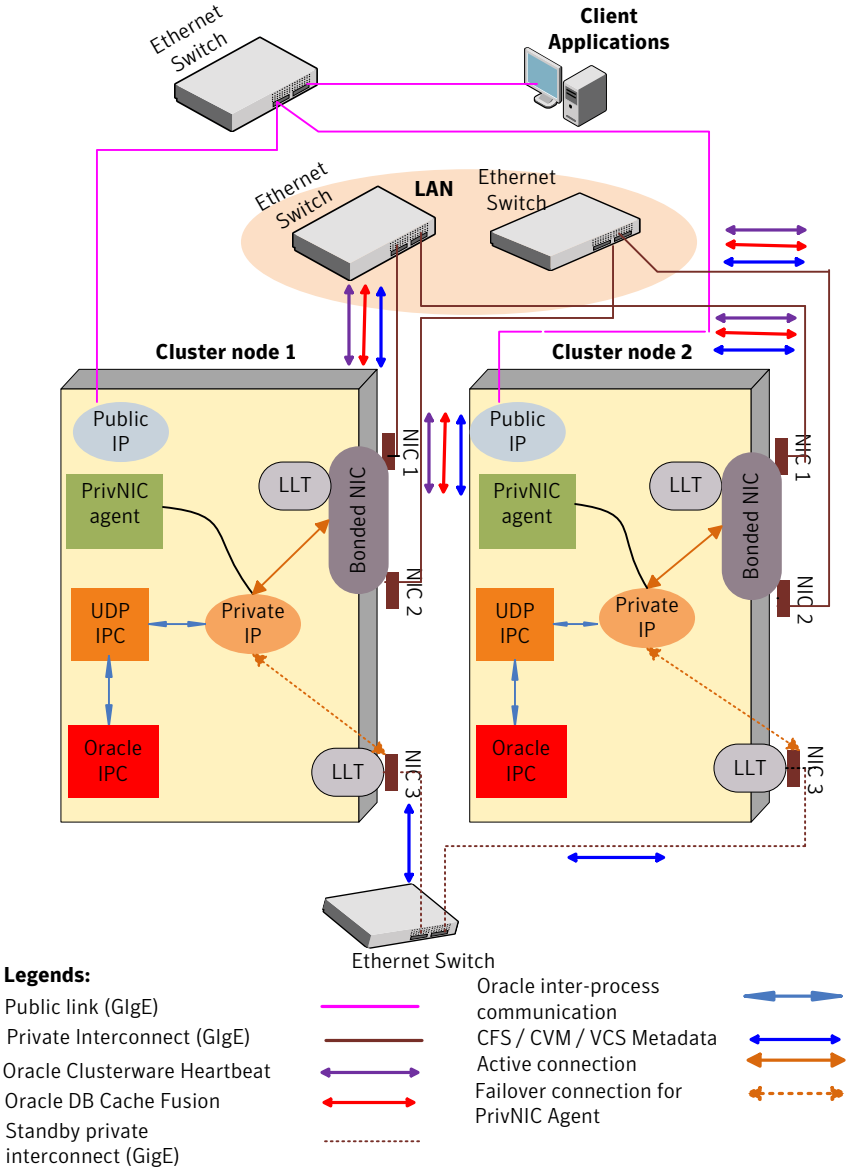
Deployment scenario	Oracle RAC with UDP IPC is configured to use a bonded NIC interface for distribution of Oracle database cache fusion traffic. A second link is configured as a standby link.
Recommendation	Use the PrivNIC agent.
Sample main.cf configuration file	The following sample main.cf file describes the configuration: `/etc/VRTSvcs/conf/sample_rac/sfrac02_main.cf` **Note:** You must replace the lan1 interface in the sample file with the bonded NIC interface you use in the scenario and lan2 in the sample file with the NIC3 interface in the scenario.

In the illustrated configuration:

- A common IP address is used for Oracle Clusterware communication and Oracle database cache fusion that is distributed over two underlying physical links of the bonded NIC interface. The bonded NIC interface is configured as a single LLT link.
- The CFS/CVM/VCS metadata also travels through the bonded link.
- In the event of a bonded link failure, the PrivNIC agent fails over the private network IP address from the failed link to the available standby LLT link. When the link is restored, the IP address is failed back to the original link.

Figure I-6 illustrates the logical view of a two-node SF Oracle RAC cluster with NIC bonding, UDP IPC, and PrivNIC agent.

Figure I-6 SF Oracle RAC cluster with NIC bonding, UDP IPC, and PrivNIC agent



Configuration diagrams for setting up server-based I/O fencing

The following CP server configuration diagrams can be used as guides when setting up CP server within your configuration:

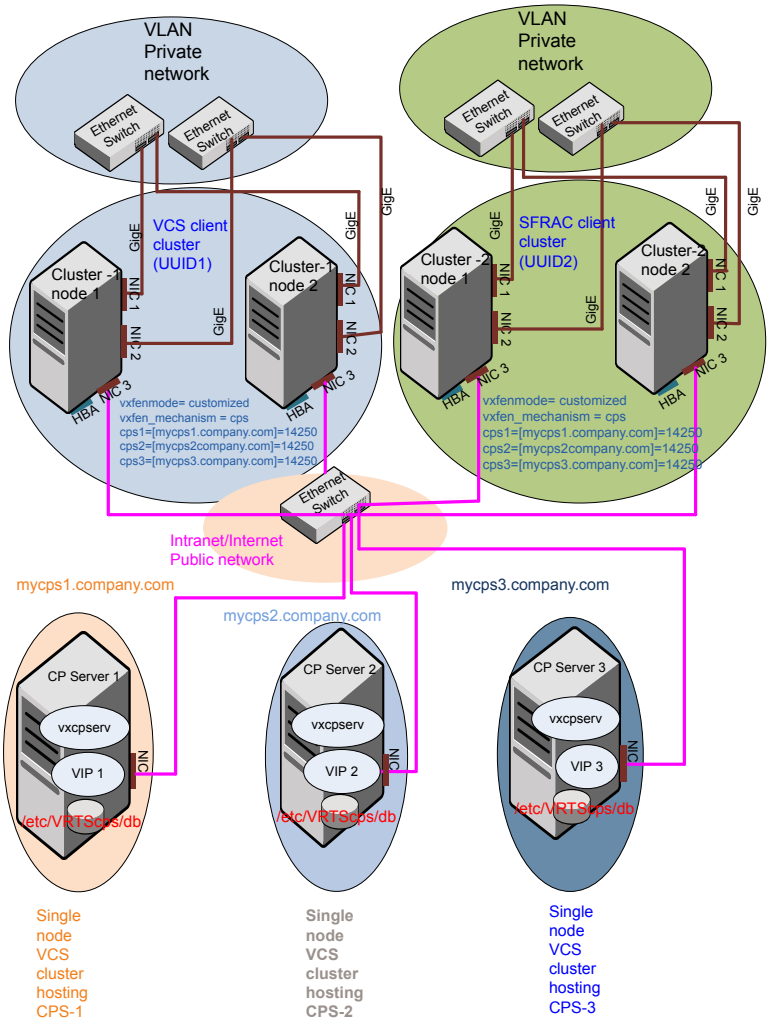
- Two unique client clusters that are served by 3 CP servers:
  See Figure I-7 on page 737.
- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:
- Two node campus cluster that is served be remote CP server and 2 SCSI-3 disks:
- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:

Two unique client clusters served by 3 CP servers

Figure I-7 displays a configuration where two unique client clusters are being served by 3 CP servers (coordination points). Each client cluster has its own unique user ID (UUID1 and UUID2).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

Figure I-7 Two unique client clusters served by 3 CP servers



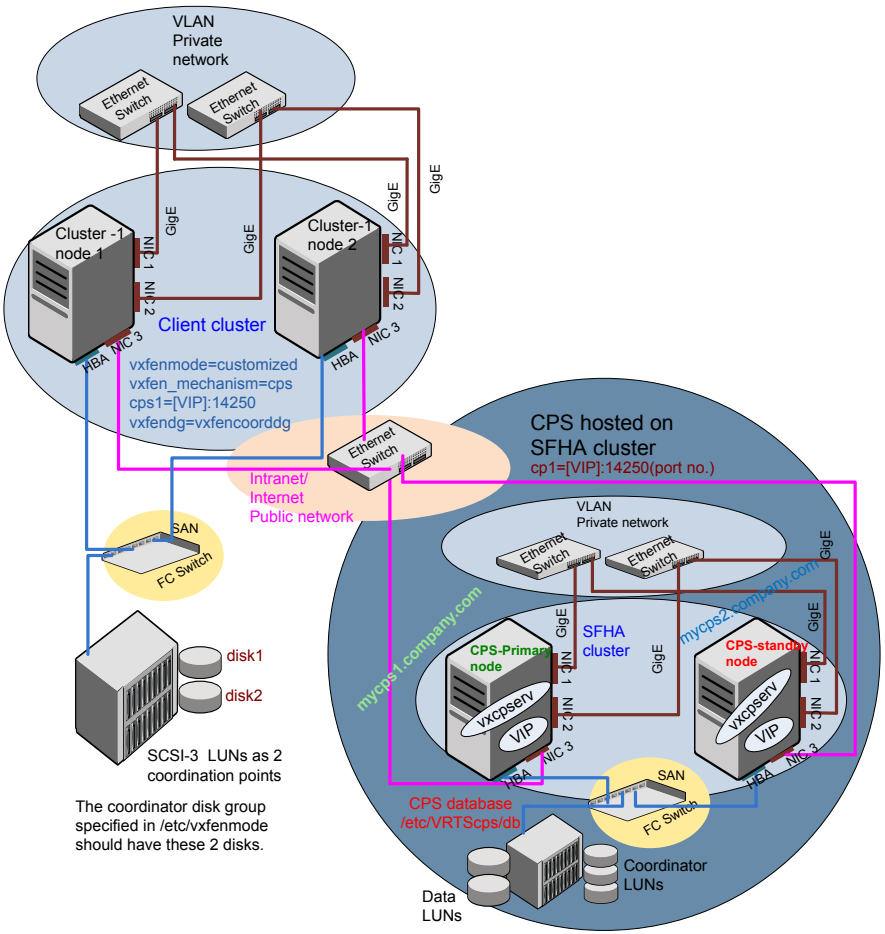
Client cluster served by highly available CPS and 2 SCSI-3 disks

Figure I-8 displays a configuration where a client cluster is served by one highly available CP server and 2 local SCSI-3 LUNs (disks).

In the `vxfenmode` file on the client nodes, `vxfenmode` is set to customized with vxfen mechanism set to `cps`.

The two SCSI-3 disks are part of the disk group vxfencoorddg. The third coordination point is a CP server hosted on an SFHA cluster, with its own shared database and coordinator disks.

Figure I-8 Client cluster served by highly available CP server and 2 SCSI-3 disks



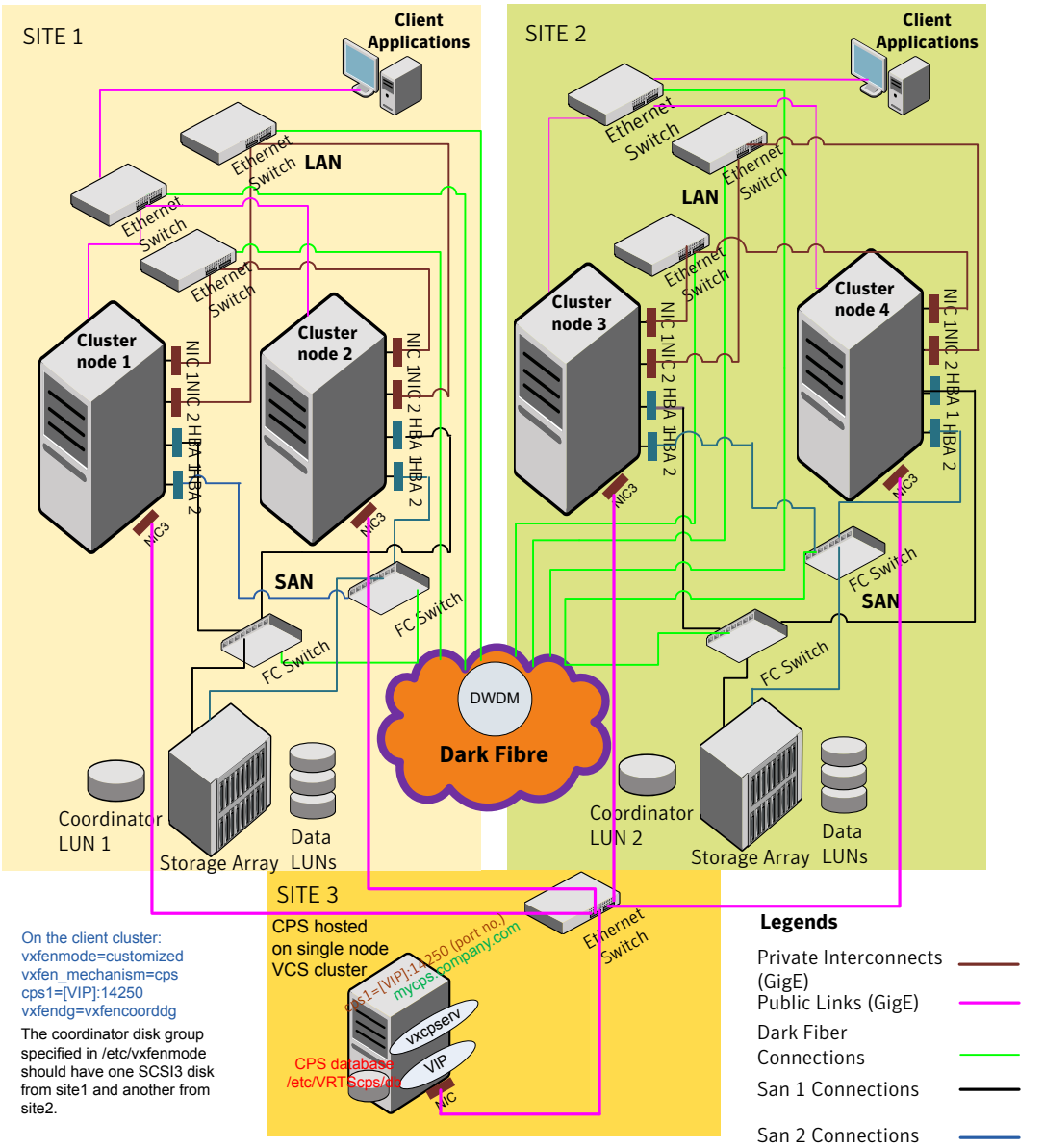
Two node campus cluster served by remote CP server and 2 SCSI-3 disks

Figure I-9 displays a configuration where a two node campus cluster is being served by one remote CP server and 2 local SCSI-3 LUN (disks).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

The two SCSI-3 disks (one from each site) are part of disk group vxfencoorddg. The third coordination point is a CP server on a single node VCS cluster.

Figure I-9 Two node campus cluster served by remote CP server and 2 SCSI-3



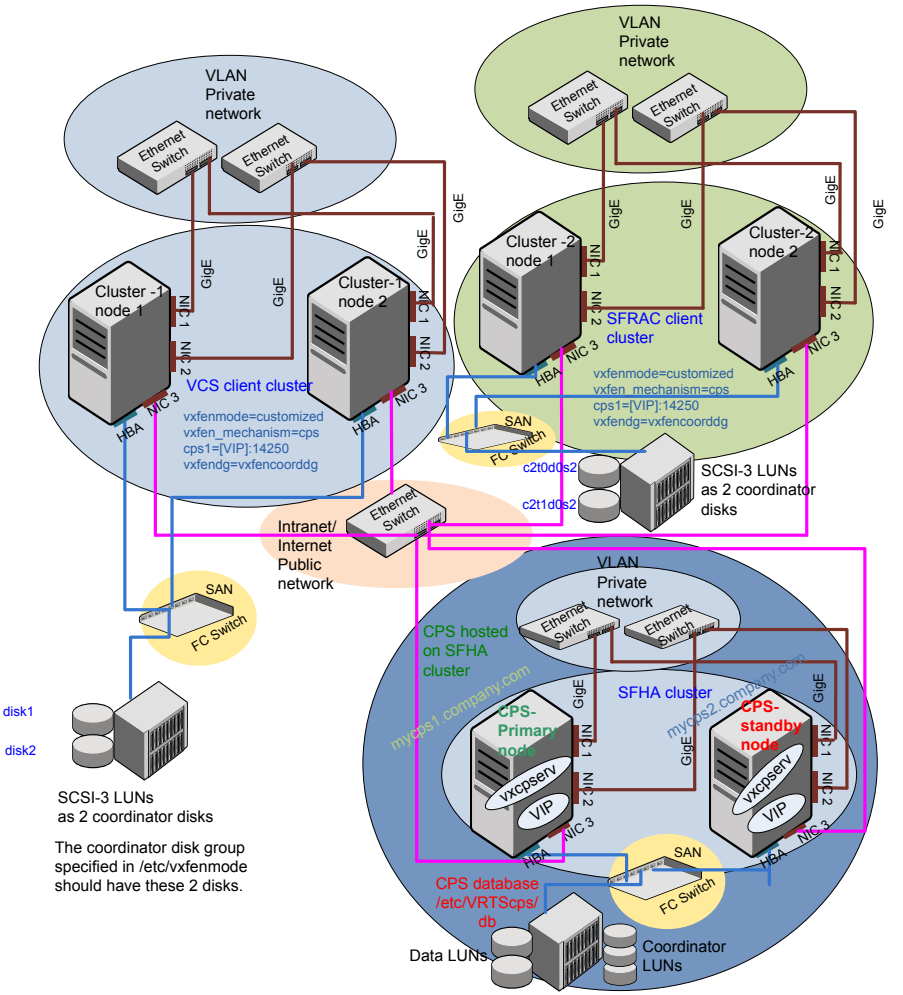
Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

Figure I-10 displays a configuration where multiple client clusters are being served by one highly available CP server and 2 local SCSI-3 LUNS (disks).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

The two SCSI-3 disks are are part of the disk group vxfencoorddg. The third coordination point is a CP server, hosted on an SFHA cluster, with its own shared database and coordinator disks.

Figure I-10 Multiple client clusters served by highly available CP server and 2 SCSI-3 disks



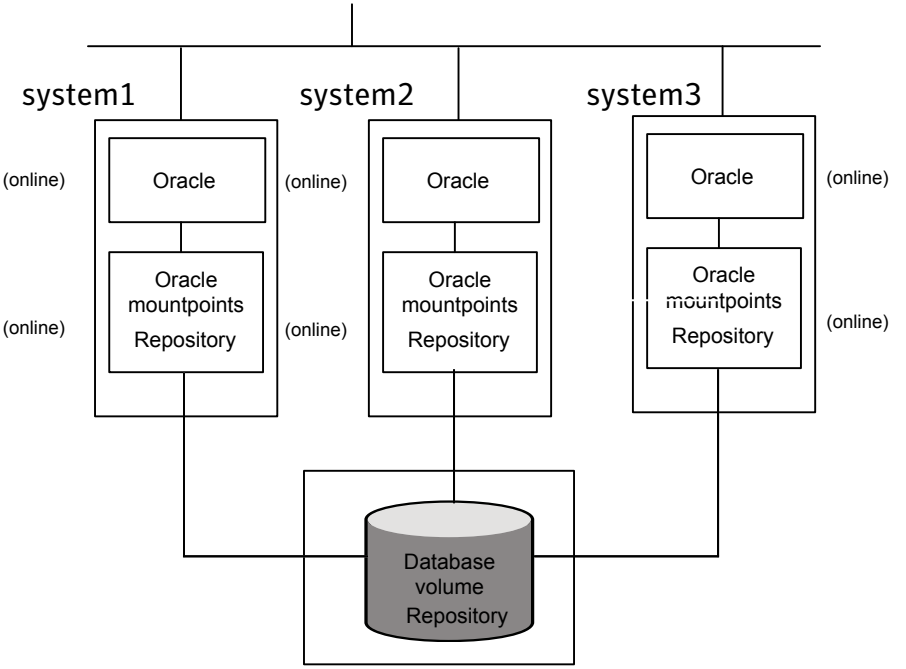
Deploying Storage Foundation for Databases (SFDB) tools in a Storage Foundation for Oracle RAC environment

If you are deploying the SFDB tools with Storage Foundation for Oracle RAC (multiple instance Oracle) your setup configuration will reflect the following conditions:

- A highly available parallel cluster with a multiple instances of Oracle is set up on galaxy and nebula with SF for Oracle RAC.
- The database is online on galaxy, nebula, and mercury.
- The datafiles are mounted and shared on galaxy, nebula, and mercury.
- The SFDB tools is mounted and shared on galaxy, nebula, and mercury.
- You can run the SFDB tools commands on galaxy, nebula, and mercury.
- Clustered ODM is supported for this configuration.

In the figure below the repository directory resides in the Oracle mount points.

Figure I-11 Deploying the database repository with Storage Foundation



For an SF Oracle RAC configuration, the systems are online in parallel and do not use failover mechanisms within the cluster.

Glossary

Agent	A process that starts, stops, and monitors all configured resources of a type, and reports their status to VCS.
Authentication Broker	The Veritas Security Services component that serves, one level beneath the root broker, as an intermediate registration authority and a certification authority. The authentication broker can authenticate clients, such as users or services, and grant them a certificate that will become part of the Veritas credential. An authentication broker cannot, however, authenticate other brokers. That task must be performed by the root broker.
Cluster	A cluster is one or more computers that are linked together for the purpose of multiprocessing and high availability. The term is used synonymously with VCS cluster, meaning one or more computers that are part of the same GAB membership.
CVM (cluster volume manager)	The cluster functionality of Veritas Volume Manager.
Disaster Recovery	Administrators with clusters in physically disparate areas can set the policy for migrating applications from one location to another if clusters in one geographic area become unavailable due to an unforeseen event. Disaster recovery requires heartbeating and replication.
disk array	A collection of disks logically arranged into an object. Arrays tend to provide benefits such as redundancy or improved performance.
DMP (Dynamic Multi-Pathing)	A feature designed to provide greater reliability and performance by using path failover and load balancing for multiported disk arrays connected to host systems through multiple paths. DMP detects the various paths to a disk using a mechanism that is specific to each supported array type. DMP can also differentiate between different enclosures of a supported array type that are connected to the same host system.
SmartTier	A feature with which administrators of multi-volume VxFS file systems can manage the placement of files on individual volumes in a volume set by defining placement policies that control both initial file location and the circumstances under which existing files are relocated. These placement policies cause the files to which they apply to be created and extended on specific subsets of a file system's volume set, known as placement classes. The files are relocated to volumes in other placement

	classes when they meet specified naming, timing, access rate, and storage capacity-related conditions.
Failover	A failover occurs when a service group faults and is migrated to another system.
GAB (Group Atomic Broadcast)	A communication mechanism of the VCS engine that manages cluster membership, monitors heartbeat communication, and distributes information throughout the cluster.
HA (high availability)	The concept of configuring the product to be highly available against system failure on a clustered network using Veritas Cluster Server (VCS).
IP address	An identifier for a computer or other device on a TCP/IP network, written as four eight-bit numbers separated by periods. Messages and other data are routed on the network according to their destination IP addresses. See also virtual IP address
Jeopardy	A node is in jeopardy when it is missing one of the two required heartbeat connections. When a node is running with one heartbeat only (in jeopardy), VCS does not restart the applications on a new node. This action of disabling failover is a safety mechanism that prevents data corruption.
latency	For file systems, this typically refers to the amount of time it takes a given file system operation to return to the user.
LLT (Low Latency Transport)	A communication mechanism of the VCS engine that provides kernel-to-kernel communications and monitors network communications.
logical volume	A simple volume that resides on an extended partition on a basic disk and is limited to the space within the extended partitions. A logical volume can be formatted and assigned a drive letter, and it can be subdivided into logical drives. See also LUN
LUN	A LUN, or logical unit, can either correspond to a single physical disk, or to a collection of disks that are exported as a single logical entity, or virtual disk, by a device driver or by an intelligent disk array's hardware. VxVM and other software modules may be capable of automatically discovering the special characteristics of LUNs, or you can use disk tags to define new storage attributes. Disk tags are administered by using the `vxdisk` command or the graphical user interface.
main.cf	The file in which the cluster configuration is stored.
mirroring	A form of storage redundancy in which two or more identical copies of data are maintained on separate volumes. (Each duplicate copy is known as a mirror.) Also RAID Level 1.
Node	The physical host or system on which applications and service groups reside. When systems are linked by VCS, they become nodes in a cluster.

resources	Individual components that work together to provide application services to the public network. A resource may be a physical component such as a disk group or network interface card, a software component such as a database server or a Web server, or a configuration component such as an IP address or mounted file system.
Resource Dependency	A dependency between resources is indicated by the keyword "requires" between two resource names. This indicates the second resource (the child) must be online before the first resource (the parent) can be brought online. Conversely, the parent must be offline before the child can be taken offline. Also, faults of the children are propagated to the parent.
Resource Types	Each resource in a cluster is identified by a unique name and classified according to its type. VCS includes a set of pre-defined resource types for storage, networking, and application services.
root broker	The first authentication broker, which has a self-signed certificate. The root broker has a single private domain that holds only the names of brokers that shall be considered valid.
SAN (storage area network)	A networking paradigm that provides easily reconfigurable connectivity between any subset of computers, disk storage and interconnecting hardware such as switches, hubs and bridges.
Service Group	A service group is a collection of resources working together to provide application services to clients. It typically includes multiple resources, hardware- and software-based, working together to provide a single service.
Service Group Dependency	A service group dependency provides a mechanism by which two service groups can be linked by a dependency rule, similar to the way resources are linked.
Shared Storage	Storage devices that are connected to and used by two or more systems.
shared volume	A volume that belongs to a shared disk group and is open on more than one node at the same time.
SNMP Notification	Simple Network Management Protocol (SNMP) developed to manage nodes on an IP network.
State	The current activity status of a resource, group or system. Resource states are given relative to both systems.
Storage Checkpoint	A facility that provides a consistent and stable view of a file system or database image and keeps track of modified data blocks since the last Storage Checkpoint.
System	The physical system on which applications and service groups reside. When a system is linked by VCS, it becomes a node in a cluster. See Node
types.cf	A file that describes standard resource types to the VCS engine; specifically, the data required to control a specific resource.

VCS (Veritas Cluster Server)	An open systems clustering solution designed to eliminate planned and unplanned downtime, simplify server consolidation, and allow the effective management of a wide range of applications in multiplatform environments.
Virtual IP Address	A unique IP address associated with the cluster. It may be brought up on any system in the cluster, along with the other resources of the service group. This address, also known as the IP alias, should not be confused with the base IP address, which is the IP address that corresponds to the host name of a system.
VxFS (Veritas File System)	A component of the Veritas Storage Foundation product suite that provides high performance and online management capabilities to facilitate the creation and maintenance of file systems. A file system is a collection of directories organized into a structure that enables you to locate and store files.
VxVM (Veritas Volume Manager)	A Symantec product installed on storage clients that enables management of physical disks as logical devices. It enhances data storage management by controlling space allocation, performance, data availability, device installation, and system monitoring of private and shared systems.
VVR (Veritas Volume Replicator)	A data replication tool designed to contribute to an effective disaster recovery plan.

Index

Symbols

$CRS_HOME
    setting up 308
$ORACLE_HOME
    setting up 308

A

adding
    users 134
agent operations
    Netlsnr agent 705
    Oracle agent 693
agents
    about 657
    CFSfsckd 676
    CFSMount 670, 676
    CSSD 690
    CVMCluster 659
    CVMVolDg 666
    CVMVxconfigd 661
    log files 362
    MultiPrivNIC 685
    of VCS 658
    of VCS for Oracle 658
    PrivNIC 679
ASM
    about 639
    configuring with CVM
        about 642
        configuring disk group 646
        creating shared raw volumes 647
        installing ASM 643
    main.cf 651
    SF Oracle RAC configuration 640
    unlinking ODM 645
    verifying setup 648
ASMDG agent
    attribute definitions 712
    resource type 711
ASMDG agent attributes
    AgentDirectory 712
ASMDG agent attributes *(continued)*
    DBAPword 712
    DBAUser 712
    DiskGroups 712
    Encoding 712
    EnvFile 712
    Home 712
    Owner 712
    Sid 712
attribute definitions
    ASMDG agent 712
    Netlsnr agent 707
    Oracle agent 700
attributes
    about agent attributes 658
    CFSMount agent 671, 676
    CVMCluster agent 660
    CVMVolDg agent 660, 668
    CVMVxconfigd agent 662
    MultiPrivNIC agent 686
    PrivNIC agent
        optional 682
        required 680
    UseFence 157
Automatic Storage Management. *See* ASM

B

basic monitoring 695
    health check 695
    process 695

C

cables
    cross-over Ethernet 433
CFS
    creating databases 655
    stopping applications 551
    unmounting file systems 551
CFSfsckd agent 676
    attributes 676

CFSMount agent 670, 676
attributes 671
entry points 671
sample configuration 675
type definition 675
CFSTypes.cf 675
cluster
removing a node from 474
verifying operation 198
cluster configuration 125
Cluster File System. *See* CFS
Cluster Manager 37
Cluster Volume Manager. *See* CVM
clusters
basic setup 38
four-node illustration 38
commands
gcoconfig 505
hastatus 198
hasys 199
lltconfig 606
lltstat 195
vradmin 520
vxassist 513, 515, 655
vxdisksetup (initializing disks) 147
vxedit 655
vxvol 513, 655
configuration
required information
for CVM 587
for global clusters 589
for I/O fencing 586
for secure clusters 587
for VCS 585
for VVR 589
configuration files
removing 561
See also main.cf samples
configuring
remsh 635
ssh 635–636
Configuring global clusters
for SF Oracle RAC 498
configuring VCS
adding users 134
event notification 134, 136
global clusters 138
secure mode 130
coordinator disks
setting up 155
CP server database 33
CP server user privileges 33
CSSD agent 690
attributes 691
CVM
configuration worksheet 596
CVMTypes.cf file 660
installation worksheet 596–597
required information
for configuration 587
upgrading protocol version 262
CVMCluster agent 659
attributes 660
entry points 659
sample configuration 661
type definition 660
CVMTypes.cf
definition, CVMCluster agent 660
definition, CVMVolDg agent 670
definition, CVMVxconfigd agent 666
CVMVolDg agent 666
attributes 668
entry points 667
sample configuration 670
type definition 670
CVMVxconfigd agent 661
attributes 662
CVMTypes.cf 666
entry points 662
sample configuration 666
type definition 666

D

databases
creating 653
creating tablespaces
on CFS 655
on raw volumes 654
dbca
description 653
detail monitoring 695
disks
adding and initializing 147
coordinator 155
testing with vxfentsthdw 149
verifying node access 150

E

environment variables
    MANPATH 83
Ethernet controllers 433

F

files. *See* configuration files

G

GAB
    port memberships 197
GAB ports 197
gabtab file
    verifying after installation 606
gcoconfig command 505
Global Cluster Option (GCO)
    overview 43
global clusters
    about 35
    configuration 138
        using VVR 505
    configuration examples 523
    configuring VCS service groups 505
    illustration of dependencies 521
    migration 535–536
    overview 498
    replicating database volumes 521
    required information
        for configuration 589
    requirements 496
groups
    log owner 522
    RVG 523

H

hastatus -summary command 198
hasys -display command 199
health check APIs 695
health check monitoring 695
hubs
    independent 433

I

I/O fencing
    checking disks 149
    required information
        for configuration 586
I/O fencing *(continued)*
    setting up 155
    shared storage 149
installation
    of Oracle Clusterware 331
    of Oracle Grid Infrastructure 331
    of Oracle RAC 275
    preparation 581
installation worksheets 581
installing
    Root Broker 101
installsfrac
    installing Clusterware 331
    installing Oracle Grid Infrastructure 331
    installing Oracle RAC 278
    installing SF Oracle RAC 89
    upgrading SF Oracle RAC 216

J

Java Console 37

L

links
    private network 606
LLT
    interconnects 84
    verifying 195
lltconfig command 606
llthosts file
    verifying after installation 606
lltstat command 195
llttab file
    verifying after installation 606

M

main.cf
    after SF Oracle RAC installation 605
main.cf files 628
main.cf samples
    for CSSD resource 693
MANPATH environment variable 83
media speed 84
    optimizing 83
migration, of Oracle 363
monitoring
    basic 695
    detail 695

MultiPrivNIC
for UDP 304
MultiPrivNIC agent 685
attributes 686
entry point 685
type definition 689
MultiPrivNIC.cf 689
sample configuration 689

N

Netlsnr agent
attribute definitions 707
operations 705
resource type 707
Netlsnr agent attributes
AgentDebug 707
AgentDirectory 707
EnvFile 707
Home 707
Listener 707
LsnrPwd 707
MonScript 707
Owner 707
TnsAdmin 707
nodes
adding Oracle RAC nodes
configuring GAB 440
configuring LLT 440
configuring VCSMM 440
configuring VXFEN 440
starting Volume Manager 439
preparing Oracle RAC nodes
configuring CVM 448
configuring private IP addresses 460
preparing $CRS_HOME 462
preparing $ORACLE_HOME 462
removing Oracle RAC 11g nodes
editing VCS configuration files 475
GAB configuration 476
LLT configuration 475
modifying VCS configuration 476
removing Oracle RAC nodes
Oracle procedure 474
removing Oracle RACnodes
workflow 473
nodes, removing 473

O

OCR
creating
on raw volumes 288
creating file system
using CLI 289
operations
Netlsnr agent 705
Oracle agent 693
optimizing
media speed 83
options
SF Oracle RAC configuration 123
Oracle
agent log file 362
creating databases 654–655
stopping instances 548
supported versions 52
Oracle 11g
migration from Oracle RAC 10g
installing Oracle RAC 10g 365
post-upgrade tasks 366
Oracle 11g Release 2
migration from Oracle RAC 10g
of existing database 366
pre-upgrade tasks 364
Oracle 11gRelease 2
migration from Oracle 9i 2
pre-upgrade tasks 365
Oracle agent
attribute definitions 700
operations 693
resource type 699
Oracle agent attributes
AgentDebug 700
AgentDirectory 700
AutoEndBkup 700
DBAPword 700
DBAUser 700
DetailMonitor 700
EnvFile 700
Home 700
IMF 700
MonitorOption 700
MonScript 700
Owner 700
Pfile 700
Pword 700
ShutDownOpt 700

Oracle agent attributes *(continued)*
Sid 700
StartUpOpt 700
Table 700
User 700
Oracle Grid Infrastructure
installing 331
Oracle RAC
database replication 519
installation
installing database 338
workflow 329
manual installation
installing database binaries 340
installing Oracle Clusterware 334
installing Oracle Grid Infrastructure 334
post-installation
adding UDP IP addresses 354
pre-installation
creating OCR 288
creating Oracle disk groups 282
creating Oracle users and groups 279
creating voting disk volumes 288
identifying public virtual IP addresses 277
setting system parameters 278
setting up Oracle user equivalence 323
setting up storage 57
starting installsfrac 278
workflow 275
Oracle RAC 11g
agent log file 362
configuring service groups
preventing automatic starting of database 355
installation
configuring service groups 356
setting environment variables 331
verifying 341
post-installation
adding patches 345
creating database 353
relinking SF Oracle RAC libraries 350
pre-installation
configuring MultiPrivNIC 304
preparing $CRS_HOME 308
preparing $ORACLE_HOME 308
setting environment variables 331
Oracle RAC 11g Clusterware
creating file system 311, 462
Oracle RAC 11g Clusterware *(continued)*
verifying installation 341
Oracle RAC 11g Release 1 Clusterware
creating file system 315, 467

P

patches
adding 345
patchsets
adding 345
PATH variable
VCS commands 194
ports
GAB 197
primary site
creating SRL volume 512
setting up 499
setting up replication objects 513
VCS configuration 526, 529
PrivNIC agent 679
attributes 680
entry point 680
sample configuration 684
type definition 684
PrivNIC.cf 684
process monitoring 695

R

raw volumes
creating
Oracle DBCA procedure 647
remote shell 636
removing a node from a cluster 474
remsh
configuration 635
replication
automatic synchronization 520
configuring on both sites 504
full synchronization with Checkpoint 520
modifying VCS configuration 522
options 497
setting up primary site 499
setting up secondary site 501
supported hardware 496
supported software 496
supported technologies 496
using VVR 512
verifying status 521

resource type
ASMDG 711
Netlsnr 707
Oracle 699
resources
CVMVolDg 523
RVGSharedPri 523
response file
about 371
syntax 374
Root Broker 36
installing 101

S

SCSI-3 persistent reservations
verifying 155
secondary site
configuring replication 515
creating SRL volume 515
setting up 501
setting up disk groups 517
setting up RLINKs 516
secure clusters
adding users 588
required information
for configuration 587
secure shell 636
service groups
configuring 356
VCS, for global clusters 505
setting umask, before installing 81
SF Oracle RAC
about 27
coordinator disks 155
high-level view 38
illustration of global cluster dependencies 521
takeover 536
SF Oracle RAC configuration
about 123
configuring clusters 125
creating configuration files 139
of components 124
options 123
preparation
worksheets 581
starting processes 139
verifying 197
SF Oracle RAC installation
pre-installation tasks
mounting product disc 82
setting MANPATH 83
setting umask 81
setting up shared storage 82
synchronizing time settings 81
verifying systems 84
preinstallation information 45
preparation
worksheets 581
requirements
hardware 46
software 52
using installsfrac 89
verifying
cluster operations 194
GAB operations 194
LLT operations 194
SF Oracle RAC uninstallation
preparation
stopping applications, CFS 551
stopping applications, VxFS 553
stopping Oracle instances 548
stopping VCS 552
uninstalling 551
unmounting CFS file systems 551
unmounting VxFS file systems 553
removing configuration files 561
removing depots 560
using uninstallsfrac program 560
workflow 545
SF Oracle RAC upgrade
post-upgrade tasks
relinking Oracle RAC libraries 258
upgrading CVM protocol version 262
upgrading disk group version 262
preparation 208
restoring configuration files 217
stopping cluster resources 208
stopping Oracle RAC 208
upgrading licenses 237
using installsfrac 216
shared storage
setting up 82
SMTP email notification 134
SNMP trap notification 136
ssh
configuration 635

ssh *(continued)*
configuring 636
Symantec Product Authentication Service 36, 101, 130
synchronizing time settings, before installing 81
system communication using remote shell
secure shell 636
system state attribute value 198

U

uninstallation
of SF Oracle RAC 555
uninstallsfrac program
removing depots 560
users
creating 279
for &ProductNameShort;, adding 588

V

VCS
agent log file 362
command directory path variable 194
configuration, for database volume replication 521
configuring service groups 505
notifications 35
required information
for configuration 585
stopping 552
VCS configuration
for replication 522
VCS Global cluster option. *See* GCO
VCS notifications
SMTP notification 35
SNMP notification 35
Veritas File System
stopping applications 553
unmounting 553
Veritas Operations Manager 36
Veritas Volume Replicator. *See* VVR
virtual fire drill 698
voting disk
creating
on raw volumes 288
voting disks
creating file system
using CLI 289
vradmin command 520
VVR
about 35
configuration examples 523
configuration worksheet 596
configuring global clusters 505
configuring on both sites 504
database volume replication
configuring VCS 521
defining heartbeat cluster objects 506
defining remote clusters 506
global cluster overview 511
installation worksheet 596–597
Oracle RAC database replication 519
primary site
creating SRL volume 512
setting up replication objects 513
replication
using automatic synchronization 520
using full synchronization with Checkpoint 520
replication agents 497
required information
for configuration 589
secondary site
configuring replication 515
creating SRL volume 515
setting up disk groups 517
setting up RLINKs 516
setting up primary site 499
setting up replication 512
setting up secondary site 501
types of replication 497
VCS configuration
CVMoIDG resource 523
log owner group 522
Oracle RAC database service group 523
primary site 526
RVG group 523
RVGSharedPri resource 523
secondary site 529
verifying replication 521
vxassist command 513, 515, 655
vxdisksetup command 147
VxFS. *See* Veritas File System
vxvol command 513, 655

W

worksheets
for &ProductNameShort; 582

worksheets *(continued)*
for CVM 596
for replication
SRDF 597
VVR 596
for VVR 596